Jurnalul Oficial al Uniunii Europene

L 333

Anul 65

Ediția în limba română **Legislație**

27 decembrie 2022

Cuprins

[1] Text cu relevanță pentru SEE.

RO

Actele ale căror titluri sunt tipărite cu caractere drepte sunt acte de gestionare curentă adoptate în cadrul politicii agricole și care au, în general, o perioadă de valabilitate limitată.

Titlurile celorlalte acte sunt tipărite cu caractere aldine și sunt precedate de un asterisc.

I

(Acte legislative)

REGULAMENTE

REGULAMENTUL (UE) 2022/2554 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 14 decembrie 2022

privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Băncii Centrale Europene ([1]),

având în vedere avizul Comitetului Economic și Social European ([2]),

hotărând în conformitate cu procedura legislativă ordinară ([3]),

întrucât:

(1) În era digitală, tehnologia informației și a comunicațiilor (TIC) sprijină sistemele complexe utilizate pentru activitățile de zi cu zi. Aceasta susține activitatea economiilor noastre în sectoare-cheie, inclusiv în sectorul financiar, și îmbunătățește funcționarea pieței interne. Creșterea gradului de digitalizare și de interconectare amplifică, de asemenea, riscurile TIC, ceea ce face ca societatea în ansamblu – și sistemul financiar, în special – să fie mai vulnerabilă la amenințările cibernetice sau la perturbările din domeniul TIC. Deși utilizarea extensivă a sistemelor TIC și gradul ridicat de digitalizare și conectivitate sunt în prezent caracteristicile de bază ale activităților entităților financiare din Uniune, reziliența digitală a acestora trebuie încă să fie mai bine abordată și integrată în cadrele lor operaționale mai ample.

(2) În ultimele decenii, utilizarea TIC a dobândit un rol esențial în furnizarea serviciilor financiare, ajungând în prezent să aibă o importanță critică în ceea ce privește operarea funcțiilor zilnice uzuale ale tuturor entităților financiare. Astăzi, digitalizarea acoperă, de exemplu, plățile, care au trecut tot mai mult de la metodele bazate pe numerar și pe suportul de hârtie la utilizarea soluțiilor digitale, precum și compensarea și decontarea titlurilor de valoare, tranzacționarea electronică și algoritmică, operațiunile de creditare și de finanțare, creditarea de la persoană la persoană, ratingul de credit, gestionarea creanțelor și operațiunile de tip back-office. Sectorul asigurărilor a fost, de

([1]) JO C 343, 26.8.2021, p. 1.
([2]) JO C 155, 30.4.2021, p. 38.
([3]) Poziția Parlamentului European din 10 noiembrie 2022 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 28 noiembrie 2022.

asemenea, transformat prin utilizarea TIC, de la apariția intermediarilor de asigurări care își oferă serviciile online folosind InsurTech, până la subscrierea de asigurări folosind mijloace digitale. Finanțele nu numai că au devenit în mare parte digitale în întregul sector, ci digitalizarea a aprofundat, de asemenea, interconexiunile și dependențele din interiorul sectorului financiar, precum și relaționarea cu furnizorii terți de infrastructură și servicii.

(3) Comitetul european pentru risc sistemic (CERS) a reafirmat într-un raport din 2020 care abordează riscul cibernetic sistemic modul în care nivelul ridicat existent de interconectare dintre entitățile financiare, piețele financiare și infrastructurile pieței financiare și, în special, interdependențele dintre sistemele lor TIC ar putea constitui o vulnerabilitate sistemică, deoarece incidentele cibernetice localizate s-ar putea răspândi rapid de la oricare dintre cele aproximativ 22 000 de entități financiare ale Uniunii la întregul sistem financiar, nestingherite de limitele geografice. Breșele grave de securitate a TIC care au loc în sectorul financiar nu afectează doar entitățile financiare luate separat. Acestea facilitează, de asemenea, propagarea vulnerabilităților localizate la nivelul canalelor de transmisie financiară și pot avea consecințe negative asupra stabilității sistemului financiar al Uniunii, cum ar fi generarea de retrageri masive de lichiditate și o pierdere generală a încrederii în piețele financiare.

(4) În ultimii ani, riscurile TIC au atras atenția responsabililor de elaborarea politicilor, a organismelor de reglementare și a organismelor de standardizare de la nivel național și internațional, precum și de la nivelul Uniunii, într-o încercare de a spori reziliența digitală, a stabili standarde și a coordona activitatea de reglementare sau de supraveghere. La nivel internațional, Comitetul de la Basel pentru supraveghere bancară, Comitetul pentru plăți și infrastructuri de piață, Consiliul pentru Stabilitate Financiară, Institutul pentru Stabilitate Financiară, precum și G7 și G20 urmăresc să furnizeze autorităților competente și operatorilor pe piață din diferite jurisdicții instrumente care să consolideze reziliența sistemelor lor financiare. Această activitate a fost determinată, de asemenea, de necesitatea de a lua în considerare în mod corespunzător riscurile TIC în contextul unui sistem financiar global foarte interconectat și de a urmări o mai mare coerență a bunelor practici relevante.

(5) În pofida existenței unor inițiative de politică și legislative specifice la nivel național și la nivelul Uniunii, riscurile TIC reprezintă în continuare o provocare la adresa rezilienței operaționale, a performanței și a stabilității sistemului financiar al Uniunii. Reformele care au urmat crizei financiare din 2008 au consolidat în primul rând reziliența financiară a sectorului financiar al Uniunii și au vizat protejarea competitivității și a stabilității Uniunii din punct de vedere economic, prudențial și al comportamentului pe piață. Deși securitatea TIC și reziliența digitală fac parte din riscul operațional, acestea s-au aflat mai puțin în centrul agendei de reglementare în urma crizei financiare și s-au dezvoltat doar în anumite domenii ale politicii și ale cadrului de reglementare al serviciilor financiare din Uniune sau numai în câteva state membre.

(6) În Comunicarea sa din 8 martie 2018 intitulată „Planul de acțiune privind FinTech: pentru un sector financiar european mai competitiv și mai inovator”, Comisia a evidențiat importanța capitală a creșterii rezilienței sectorului financiar al Uniunii, inclusiv din punct de vedere operațional, pentru a asigura siguranța tehnologică și buna sa funcționare, recuperarea rapidă în urma unor breșe și incidente legate de TIC, permițând în cele din urmă furnizarea eficace și fără probleme a serviciilor financiare în întreaga Uniune, inclusiv în situații de criză, și menținând totodată încrederea consumatorilor și a pieței.

(7) În aprilie 2019, Autoritatea europeană de supraveghere (Autoritatea bancară europeană, ABE), instituită prin Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([4]), Autoritatea europeană de supraveghere (Autoritatea europeană de asigurări și pensii ocupaționale, EIOPA), instituită prin Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ([5]), și Autoritatea europeană de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe, ESMA), instituită prin Regulamentul (UE) nr. 1095/2010 al Parlamentului

([4]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12).

([5]) Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană de asigurări și pensii ocupaționale), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/79/CE a Comisiei (JO L 331, 15.12.2010, p. 48).

European și al Consiliului ([6]) (cunoscute în mod colectiv drept „autoritățile europene de supraveghere" sau „AES"), au emis în comun un aviz tehnic solicitând o abordare coerentă a riscurilor TIC în domeniul financiar și recomandând consolidarea, în mod proporțional, a rezilienței operaționale digitale a sectorului serviciilor financiare prin intermediul unei inițiative sectoriale a Uniunii.

(8) Sectorul financiar al Uniunii este reglementat printr-un cadru unic de reglementare și este guvernat de un sistem european de supraveghere financiară. Cu toate acestea, dispozițiile privind reziliența operațională digitală și securitatea TIC nu sunt încă armonizate pe deplin sau în mod consecvent, în pofida faptului că reziliența operațională digitală este vitală pentru asigurarea stabilității financiare și a integrității pieței în era digitală și nu este mai puțin importantă decât, de exemplu, standardele comune prudențiale sau de conduită pe piață. Prin urmare, cadrul unic de reglementare și sistemul de supraveghere ar trebui să fie dezvoltate pentru a acoperi și reziliența operațională digitală, prin consolidarea mandatelor autorităților competente pentru a le permite să supravegheze gestionarea riscurilor TIC în sectorul financiar în vederea protejării integrității și eficienței pieței interne și pentru facilitarea funcționării organizate a acesteia.

(9) Disparitățile legislative și abordările naționale inegale în materie de reglementare sau de supraveghere cu privire la riscurile TIC generează obstacole în calea funcționării pieței interne a serviciilor financiare, împiedicând exercitarea fără probleme a libertății de stabilire și de prestare de servicii pentru entitățile financiare care desfășoară activități transfrontaliere. Concurența între entități financiare de același tip care operează în diferite state membre ar putea, de asemenea, să fie denaturată. Acest lucru este valabil în special în domeniile în care armonizarea la nivelul Uniunii a fost foarte limitată, cum ar fi testarea rezilienței operaționale digitale, sau a lipsit, cum ar fi monitorizarea riscurilor TIC generate de părți terțe. Disparitățile care decurg din evoluțiile preconizate la nivel național ar putea genera noi obstacole în calea funcționării pieței interne, în detrimentul participanților la piață și al stabilității financiare.

(10) Până în prezent, întrucât dispozițiile legate de riscurile TIC au fost abordate doar parțial la nivelul Uniunii, există lacune sau suprapuneri în domenii importante, cum ar fi raportarea incidentelor legate de TIC și testarea rezilienței operaționale digitale, precum și inconsecvențe ca urmare a apariției unor norme naționale divergente sau a aplicării ineficiente din punctul de vedere al costurilor a normelor care se suprapun. Acest lucru este în special în detrimentul domeniilor care utilizează intensiv TIC, precum sectorul financiar, deoarece riscurile legate de tehnologie nu au frontiere, iar sectorul financiar își desfășoară serviciile pe o bază transfrontalieră largă, în interiorul și în afara Uniunii. Entitățile financiare individuale care desfășoară activități transfrontaliere sau dețin mai multe autorizații (de exemplu, o entitate financiară poate avea o autorizație bancară, o autorizație de firmă de investiții și o autorizație de instituție de plată, fiecare dintre acestea fiind emisă de o altă autoritate competentă din unul sau mai multe state membre) se confruntă cu provocări operaționale în ceea ce privește abordarea riscurilor TIC și atenuarea efectelor negative ale incidentelor TIC pe cont propriu și într-un mod coerent și eficient din punctul de vedere al costurilor.

(11) Întrucât cadrul unic de reglementare nu a fost însoțit de un cadru cuprinzător privind riscurile TIC sau riscurile operaționale, este necesară armonizarea suplimentară a principalelor cerințe privind reziliența operațională digitală a tuturor entităților financiare. Dezvoltarea capacităților TIC și a rezilienței generale a entităților financiare, pe baza unor astfel de cerințe principale, în scopul de a rezista întreruperilor operaționale, ar contribui la menținerea stabilității și integrității piețelor financiare ale Uniunii și, astfel, la asigurarea unui nivel ridicat de protecție pentru investitorii și consumatorii din Uniune. Întrucât urmărește să contribuie la buna funcționare a pieței interne, prezentul regulament ar trebui să se bazeze pe dispozițiile articolului 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), astfel cum au fost interpretate în conformitate cu jurisprudența constantă a Curții de Justiție a Uniunii Europene (denumită în continuare „Curtea de Justiție").

(12) Prezentul regulament urmărește să consolideze și să actualizeze cerințele privind riscurile TIC ca parte a cerințelor privind riscurile operaționale care, până în prezent, au fost abordate separat în diferite acte juridice ale Uniunii. Deși au acoperit principalele categorii de riscuri financiare (de exemplu, riscul de credit, riscul de piață, riscul de credit al contrapărții și riscul de lichiditate, riscul de conduită pe piață), actele respective nu au abordat în mod cuprinzător, la momentul adoptării lor, toate componentele rezilienței operaționale. Atunci când au fost dezvoltate într-o mai mare măsură în actele juridice respective ale Uniunii, normele privind riscul operațional au favorizat, adesea, o abordare cantitativă tradițională a riscurilor (și anume, stabilirea unei cerințe de capital pentru a acoperi riscurile TIC), mai

([6]) Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei (JO L 331, 15.12.2010, p. 84).

degrabă decât norme calitative specifice pentru protecția, detectarea, limitarea, recuperarea și repararea capacităților în cazul unor incidente legate de TIC sau referitoare la capacitățile de raportare și de testare digitală. Actele respective erau menite, în principal, să acopere și să actualizeze norme esențiale privind supravegherea prudențială, integritatea pieței sau conduita pe piață. Prin consolidarea și actualizarea diferitelor norme privind riscurile TIC, toate dispozițiile care abordează riscul digital în sectorul financiar ar urma să fie reunite pentru prima dată, într-un mod coerent, într-un singur act legislativ. Prin urmare, prezentul regulament elimină lacunele sau remediază inconsecvențele din unele dintre actele juridice anterioare, inclusiv în ceea ce privește terminologia utilizată în acestea, și face trimiteri explicite la riscurile TIC prin intermediul unor norme specifice privind capacitățile de gestionare a riscurilor TIC, raportarea incidentelor, testarea rezilienței operaționale și monitorizarea riscurilor TIC generate de părți terțe. Astfel, prezentul regulament ar trebui, de asemenea, să crească gradul de conștientizare cu privire la riscurile TIC și să recunoască faptul că incidentele legate de TIC și o lipsă de reziliență operațională ar putea periclita soliditatea entităților financiare.

(13) Entitățile financiare ar trebui să aibă aceeași abordare și să respecte aceleași norme bazate pe principii cu privire la riscurile TIC, ținând cont de dimensiunea și profilul lor general de risc și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor. Consecvența contribuie la creșterea încrederii în sistemul financiar și la menținerea stabilității acestuia, în special în perioade de dependență ridicată de sisteme, platforme și infrastructuri TIC, ceea ce implică un risc digital sporit. Respectarea unei igiene cibernetice de bază ar trebui, de asemenea, să permită evitarea impunerii unor costuri semnificative asupra economiei, prin reducerea la minimum a impactului și a costurilor asociate perturbărilor TIC.

(14) Un regulament ajută la reducerea complexității reglementării, favorizează convergența supravegherii și sporește securitatea juridică, contribuind totodată la limitarea costurilor de asigurare a conformității, în special pentru entitățile financiare care desfășoară activități transfrontaliere, precum și la reducerea denaturărilor concurenței. Prin urmare, opțiunea pentru un regulament în vederea instituirii unui cadru comun pentru reziliența operațională digitală a entităților financiare reprezintă cel mai adecvat mod de a garanta o aplicare omogenă și coerentă a tuturor componentelor gestionării riscurilor TIC de către sectorul financiar al Uniunii.

(15) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([7]) a fost primul cadru de reglementare orizontal în materie de securitate cibernetică adoptat la nivelul Uniunii, care se aplică și în cazul a trei tipuri de entități financiare, și anume instituțiile de credit, locurile de tranzacționare și contrapărțile centrale. Totuși, întrucât Directiva (UE) 2016/1148 a stabilit un mecanism de identificare la nivel național a operatorilor de servicii esențiale, doar anumite instituții de credit, locuri de tranzacționare și contrapărți centrale care au fost identificate de statele membre au fost, în practică, incluse în domeniul său de aplicare, trebuind, prin urmare, să respecte cerințele privind securitatea TIC și notificarea incidentelor prevăzute în aceasta. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([8]) stabilește un criteriu uniform pentru a determina entitățile care intră în domeniul său de aplicare (regula privind criteriul de dimensiune), menținând în același timp în domeniul său de aplicare cele trei tipuri de entități financiare.

(16) Cu toate acestea, întrucât prezentul regulament sporește nivelul de armonizare în ceea ce privește diferitele componente ale rezilienței digitale, prin introducerea unor cerințe privind gestionarea riscurilor TIC și raportarea incidentelor legate de TIC care sunt mai stricte în comparație cu cele prevăzute în dreptul actual al Uniunii privind serviciile financiare, acest nivel sporit constituie o armonizare sporită și în comparație cu cerințele prevăzute în Directiva (UE) 2022/2555. Prin urmare, prezentul regulament constituie *lex specialis* în raport cu Directiva (UE) 2022/2555. În același timp, este esențial să se mențină o legătură puternică între sectorul financiar și cadrul orizontal de securitate cibernetică al Uniunii, astfel cum este prevăzut în prezent în Directiva (UE) 2022/2555, pentru a asigura coerența cu strategiile de securitate cibernetică adoptate de statele membre și pentru a permite autorităților de supraveghere financiară să fie informate cu privire la incidentele cibernetice care afectează alte sectoare care intră sub incidența directivei respective.

([7]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

([8]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (a se vedea pagina 80 din prezentul Jurnal Oficial).

(17) În conformitate cu articolul 4 alineatul (2) din Tratatul privind Uniunea Europeană și fără a aduce atingere controlului jurisdicțional exercitat de Curtea de Justiție, prezentul regulament nu ar trebui să aducă atingere responsabilității statelor membre cu privire la funcțiile esențiale ale statului în ceea ce privește siguranța publică, apărarea și protejarea securității naționale, de exemplu în ceea ce privește furnizarea de informații care ar fi contrare protejării securității naționale.

(18) Pentru a facilita procesul de învățare transsectorială și pentru a valorifica în mod eficace experiențele altor sectoare în abordarea amenințărilor cibernetice, entitățile financiare menționate în Directiva (UE) 2022/2555 ar trebui să rămână parte a „ecosistemului" directivei respective [de exemplu, Grupul de cooperare și echipele de intervenție în caz de incidente de securitate informatică (echipe CSIRT)]. AES și autoritățile naționale competente ar trebui să poată participa la discuțiile de politică strategice și la lucrările tehnice ale Grupului de cooperare în temeiul directivei respective și să schimbe informații, precum și să coopereze în continuare cu punctele unice de contact desemnate sau instituite în conformitate cu directiva respectivă. Autoritățile competente în temeiul prezentului regulament ar trebui, de asemenea, să se consulte și să coopereze cu echipele CSIRT. Autoritățile competente ar trebui, de asemenea, să fie în măsură să solicite consultanță tehnică din partea autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 și să stabilească acorduri de cooperare menite să asigure mecanisme eficace și rapide de coordonare a răspunsului.

(19) Având în vedere legăturile puternice dintre reziliența digitală și reziliența fizică a entităților financiare, este necesară o abordare coerentă în ceea ce privește reziliența entităților critice în prezentul regulament și în Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului ([9]). Având în vedere că reziliența fizică a entităților financiare este abordată în mod cuprinzător de obligațiile de gestionare a riscurilor TIC și de raportare care fac obiectul prezentului regulament, obligațiile prevăzute în capitolele III și IV din Directiva (UE) 2022/2557 nu ar trebui să se aplice entităților financiare care intră în domeniul de aplicare al directivei respective.

(20) Furnizorii de servicii de cloud computing sunt o categorie de infrastructuri digitale care intră sub incidența Directivei (UE) 2022/2555. Cadrul de supraveghere al Uniunii (denumit în continuare „cadrul de supraveghere") instituit prin prezentul regulament se aplică tuturor furnizorilor terți esențiali de servicii TIC, inclusiv furnizorilor de servicii de cloud computing care furnizează servicii TIC entităților financiare, și ar trebui să fie considerat complementar supravegherii în temeiul Directivei (UE) 2022/2555. În plus, cadrul de supraveghere instituit prin prezentul regulament ar trebui să acopere furnizorii de servicii de cloud computing în absența unui cadru orizontal al Uniunii care să instituie o autoritate de supraveghere digitală.

(21) Pentru a păstra controlul deplin asupra riscurilor TIC, entitățile financiare trebuie să dispună de capacități cuprinzătoare care să permită o gestionare sănătoasă și eficace a riscurilor TIC, precum și de mecanisme și politici specifice pentru tratarea tuturor incidentelor legate de TIC și pentru raportarea incidentelor majore legate de TIC. De asemenea, entitățile financiare ar trebui să dispună de politici pentru testarea sistemelor, controalelor și proceselor TIC, precum și pentru gestionarea riscurilor TIC generate de părți terțe. Nivelul de referință al rezilienței operaționale digitale pentru entitățile financiare ar trebui să fie majorat, permițând totodată o aplicare proporțională a cerințelor pentru anumite entități financiare, în special pentru microîntreprinderi, precum și pentru entitățile financiare care fac obiectul unui cadru simplificat de gestionare a riscurilor TIC. Pentru a facilita o supraveghere eficientă a instituțiilor pentru furnizarea de pensii ocupaționale care să fie proporțională și să abordeze necesitatea de a reduce sarcinile administrative ale autorităților competente, mecanismele naționale de supraveghere relevante cu privire la astfel de entități financiare ar trebui să țină seama de dimensiunea și profilul general de risc al acestora, precum și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, chiar și atunci când pragurile relevante stabilite la articolul 5 din Directiva (UE) 2016/2341 a Parlamentului European și a Consiliului ([10]) sunt depășite. În special, activitățile de supraveghere ar trebui să se concentreze în primul rând asupra necesității de a aborda riscurile grave asociate gestionării riscurilor TIC ale unei anumite entități.

([9]) Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (a se vedea pagina 164 din prezentul Jurnal Oficial).

([10]) Directiva (UE) 2016/2341 a Parlamentului European și a Consiliului din 14 decembrie 2016 privind activitățile și supravegherea instituțiilor pentru furnizarea de pensii ocupaționale (IORP) (JO L 354, 23.12.2016, p. 37).

Autoritățile competente ar trebui, de asemenea, să mențină o abordare vigilentă, dar proporțională, în ceea ce privește supravegherea instituțiilor pentru furnizarea de pensii ocupaționale care, în conformitate cu articolul 31 din Directiva (UE) 2016/2341, externalizează către furnizorii de servicii o parte semnificativă a activității lor principale, cum ar fi gestionarea activelor, calculele actuariale, contabilitatea și gestionarea datelor.

(22) Pragurile de raportare a incidentelor legate de TIC și taxonomiile variază semnificativ la nivel național. Deși un numitor comun poate fi atins prin intermediul activităților relevante întreprinse de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) instituită prin Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului ([11]) și de Grupul de cooperare în temeiul Directivei (UE) 2022/2555, încă există sau pot apărea abordări divergente privind stabilirea pragurilor și folosirea taxonomiilor pentru restul entităților financiare. Din cauza divergențelor respective, există cerințe multiple pe care entitățile financiare trebuie să le respecte, în special atunci când își desfășoară activitatea în mai multe state membre și când fac parte dintr-un grup financiar. În plus, astfel de divergențe pot împiedica crearea unor noi mecanisme uniforme sau centralizate ale Uniunii, care să accelereze procesul de raportare și să sprijine un schimb de informații rapid și fără probleme între autoritățile competente, care este esențial pentru abordarea riscurilor TIC în cazul unor atacuri la scară largă cu potențiale consecințe sistemice.

(23) Pentru a reduce sarcina administrativă și eventualele obligații de raportare redundante pentru anumite entități financiare, cerința de raportare a incidentelor în temeiul Directivei (UE) 2015/2366 a Parlamentului European și a Consiliului ([12]) ar trebui să înceteze să se aplice furnizorilor de servicii de plată care intră în domeniul de aplicare al prezentului regulament. În consecință, instituțiile de credit, instituțiile emitente de monedă electronică, instituțiile de plată și prestatorii de servicii de informare cu privire la conturi, astfel cum se menționează la articolul 33 alineatul (1) din directiva respectivă, ar trebui, de la data aplicării prezentului regulament, să raporteze în temeiul prezentului regulament toate incidentele operaționale sau de securitate legate de plăți care au fost raportate anterior în temeiul directivei respective, indiferent dacă astfel de incidente sunt legate de TIC sau nu.

(24) Pentru a permite autorităților competente să îndeplinească roluri de supraveghere prin obținerea unei imagini de ansamblu complete asupra naturii, frecvenței, importanței și impactului incidentelor legate de TIC și pentru a consolida schimbul de informații între autoritățile publice relevante, inclusiv autoritățile de aplicare a legii și autoritățile de rezoluție, prezentul regulament ar trebui să prevadă un regim solid de raportare a incidentelor legate de TIC, ale cărui cerințe relevante să remedieze lacunele actuale din dreptul privind serviciile financiare și să elimine suprapunerile și dublările existente, pentru a reduce costurile. Este esențial să se armonizeze regimul de raportare a incidentelor legate de TIC prin impunerea obligației ca toate entitățile financiare să raporteze autorităților lor competente printr-un cadru unic simplificat, astfel cum este prevăzut în prezentul regulament. În plus, AES ar trebui să fie împuternicite să detalieze într-o mai mare măsură elementele relevante pentru cadrul de raportare a incidentelor legate de TIC, cum ar fi taxonomia, intervalele de timp, seturile de date, modelele și pragurile aplicabile. Pentru a asigura coerența deplină cu Directiva (UE) 2022/2555, entităților financiare ar trebui să li se permită, în mod voluntar, să notifice autorității competente relevante amenințările cibernetice semnificative, atunci când consideră că amenințarea cibernetică este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți.

(25) În anumite subsectoare financiare au fost elaborate cerințe de testare a rezilienței operaționale digitale care stabilesc cadre de reglementare care nu sunt întotdeauna pe deplin aliniate. Acest lucru conduce la o eventuală duplicare a costurilor pentru entitățile financiare transfrontaliere și face ca recunoașterea reciprocă a rezultatelor testării rezilienței operaționale digitale să devină complexă, ceea ce, la rândul său, poate fragmenta piața internă.

([11]) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

([12]) Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE (JO L 337, 23.12.2015, p. 35).

(26) În plus, în cazul în care nu este necesară testarea TIC, vulnerabilitățile rămân nedetectate și conduc la expunerea unei entități financiare la riscuri TIC și, în cele din urmă, creează un risc mai mare pentru stabilitatea și integritatea sectorului financiar. Fără intervenția Uniunii, testarea rezilienței operaționale digitale ar continua să fie inconsecventă și nu ar exista un sistem de recunoaștere reciprocă a rezultatelor testelor TIC între diferite jurisdicții. În plus, întrucât este puțin probabil ca alte subsectoare financiare să adopte sistemele de testare la o scară semnificativă, acestea nu s-ar bucura de beneficiile potențiale ale unui cadru de testare, în ceea ce privește dezvăluirea vulnerabilităților și a riscurilor TIC, și testarea capacităților de apărare și a continuității activității, ceea ce contribuie la creșterea încrederii consumatorilor, a furnizorilor și a partenerilor de afaceri. Pentru a remedia aceste suprapuneri, divergențe și lacune, este necesar să se stabilească norme pentru un sistem de testare coordonat, facilitând astfel recunoașterea reciprocă a testelor avansate pentru entitățile financiare care îndeplinesc criteriile stabilite în prezentul regulament.

(27) Dependența entităților financiare de folosirea serviciilor TIC este determinată parțial de nevoia lor de a se adapta la o economie globală digitală competitivă emergentă, de a spori eficiența activității lor și de a răspunde cererii consumatorilor. Natura și amploarea unei astfel de dependențe au fost în continuă evoluție în ultimii ani, conducând la o reducere a costurilor în ceea ce privește intermedierea financiară, permițând dezvoltarea și scalabilitatea activităților financiare și oferind în același timp o gamă largă de instrumente TIC pentru gestionarea proceselor interne complexe.

(28) Utilizarea amplă a serviciilor TIC este demonstrată prin acorduri contractuale complexe, în cadrul cărora entitățile financiare se confruntă adesea cu dificultăți în ceea ce privește negocierea unor condiții contractuale care să fie adaptate la standardele prudențiale sau la alte cerințe de reglementare pe care trebuie să le respecte, sau, pe de altă parte, în exercitarea unor drepturi specifice, cum ar fi drepturile de acces sau de audit, chiar și atunci când acestea din urmă sunt consacrate în acordurile contractuale. În plus, multe dintre respectivele acorduri contractuale nu oferă garanții suficiente care să permită monitorizarea completă a proceselor de subcontractare, privând astfel entitatea financiară de capacitatea sa de a evalua aceste riscuri asociate. În plus, întrucât furnizorii terți de servicii TIC oferă adesea servicii standardizate diferitelor tipuri de clienți, astfel de acorduri contractuale nu răspund întotdeauna în mod adecvat nevoilor individuale sau specifice ale actorilor din sectorul financiar.

(29) Chiar dacă dreptul Uniunii privind serviciile financiare conține anumite norme generale privind externalizarea, monitorizarea dimensiunii contractuale nu este pe deplin ancorată în dreptul Uniunii. În absența unor standarde ale Uniunii clare și specifice care să se aplice acordurilor contractuale încheiate cu furnizorii terți de servicii TIC, sursa externă a riscurilor TIC nu este abordată în mod cuprinzător. Prin urmare, este necesar să se stabilească anumite principii-cheie care să orienteze gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe, care sunt deosebit de importante atunci când entitățile financiare recurg la furnizori terți de servicii TIC care să sprijine îndeplinirea funcțiilor critice sau importante ale entităților financiare. Aceste principii ar trebui să fie însoțite de un set de drepturi contractuale de bază în legătură cu mai multe elemente legate de executarea și încetarea acordurilor contractuale, cu scopul de a oferi anumite garanții minime care să consolideze capacitatea entităților financiare de a monitoriza în mod eficace toate riscurile TIC care apar la nivelul furnizorilor terți de servicii TIC. Aceste principii sunt complementare legislației sectoriale aplicabile externalizării.

(30) În prezent, este evidentă o anumită lipsă de omogenitate și convergență în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe și a dependențelor TIC față de terți. În pofida eforturilor de abordare a externalizării, cum ar fi Ghidul ABE din 2019 privind externalizarea și Orientările ESMA din 2021 privind externalizarea către furnizorii de servicii de cloud, problema mai amplă a contracarării riscului sistemic care poate fi declanșat de expunerea sectorului financiar la un număr limitat de furnizori terți esențiali de servicii TIC nu este abordată în mod suficient de dreptul Uniunii. Lipsa reglementărilor la nivelul Uniunii este agravată de absența unor norme naționale privind mandatele și instrumentele care să permită autorităților de supraveghere financiară să dobândească o bună înțelegere a dependențelor TIC față de terți și să monitorizeze în mod adecvat riscurile care decurg din concentrarea dependențelor TIC față de terți.

(31) Ținând seama de riscurile sistemice potențiale implicate de practicile de externalizare sporite și de concentrarea serviciilor TIC furnizate de părți terțe și având în vedere insuficiența capacității mecanismelor naționale de a oferi autorităților de supraveghere financiară instrumente adecvate pentru cuantificarea, calificarea și remedierea consecințelor riscurilor TIC care apar la nivelul furnizorilor terți esențiali de servicii TIC, este necesar să se instituie un cadru adecvat de supraveghere, care să permită o monitorizare continuă a activităților furnizorilor terți de servicii TIC care sunt furnizori terți esențiali de servicii TIC pentru entitățile financiare, asigurând în același timp păstrarea confidențialității și a securității clienților, alții decât entitățile financiare. Deși furnizarea de servicii TIC intragrup implică riscuri și beneficii specifice, aceasta nu ar trebui considerată în mod automat mai puțin riscantă decât furnizarea de servicii TIC de către furnizorii din afara unui grup financiar și, prin urmare, ar trebui să facă obiectul aceluiași cadru de reglementare. Cu toate acestea, atunci când serviciile TIC sunt furnizate în interiorul aceluiași grup financiar, entitățile financiare ar putea avea un nivel mai ridicat de control asupra furnizorilor intragrup, de care ar trebui să se țină seama în evaluarea globală a riscurilor.

(32) Având în vedere că riscurile TIC devin din ce în ce mai complexe și mai sofisticate, măsurile adecvate pentru detectarea și prevenirea riscurilor TIC depind în mare măsură de schimbul periodic între entitățile financiare de informații privind amenințările și vulnerabilitatea. Schimbul de informații contribuie la crearea unui grad sporit de conștientizare cu privire la amenințările cibernetice. La rândul său, acest lucru sporește capacitatea entităților financiare de a preveni ca amenințările cibernetice să devină incidente reale legate de TIC și permite entităților financiare să limiteze mai eficient impactul incidentelor legate de TIC și să se redreseze mai rapid. În absența unor orientări la nivelul Uniunii, mai mulți factori par să fi împiedicat astfel de schimburi de informații, în special incertitudinea cu privire la compatibilitatea cu normele privind protecția datelor, cu normele antitrust și cu cele privind răspunderea.

(33) În plus, incertitudinile cu privire la tipul de informații care pot fi partajate cu alți participanți pe piață sau cu autorități care nu au atribuții de supraveghere (precum ENISA, pentru contribuții analitice sau Europolul, în scopul asigurării respectării legii) conduc la nedivulgarea de informații utile. Prin urmare, amploarea și calitatea schimbului de informații rămân în prezent limitate și fragmentate, schimburile relevante fiind realizate în cea mai mare parte la nivel local (prin inițiative naționale) și fără acorduri consecvente de schimburi de informații la nivelul Uniunii, adaptate nevoilor unui sistem financiar integrat. Prin urmare, este important să se consolideze aceste canale de comunicare.

(34) Entitățile financiare ar trebui să fie încurajate să facă schimb de informații și date operative privind amenințările cibernetice și să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, în vederea consolidării capacităților lor de a evalua, a monitoriza, a apăra împotriva amenințărilor cibernetice și a răspunde în mod adecvat la acestea, prin participarea la acorduri privind schimbul de informații. Prin urmare, este necesar să se favorizeze apariția la nivelul Uniunii a unor mecanisme pentru acorduri voluntare privind schimbul de informații care, atunci când au loc în medii de încredere, ar ajuta comunitatea industriei financiare să prevină amenințările cibernetice și să răspundă în mod colectiv la acestea prin limitarea rapidă a răspândirii riscurilor TIC și prin împiedicarea unei contaminări potențiale prin canalele financiare. Aceste mecanisme ar trebui să respecte normele Uniunii aplicabile în domeniul concurenței din Comunicarea Comisiei din 14 ianuarie 2011 intitulată „Orientări privind aplicabilitatea articolului 101 din Tratatul privind funcționarea Uniunii Europene acordurilor de cooperare orizontală”, precum și normele Uniunii în materie de protecție a datelor, în special Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([13]). Acestea ar trebui să funcționeze pe baza utilizării unuia sau a mai multor temeiuri juridice prevăzute la articolul 6 din regulamentul respectiv, cum ar fi în contextul prelucrării datelor cu caracter personal care este necesară în scopul interesului legitim urmărit de operator sau de o parte terță, astfel cum se menționează la articolul 6 alineatul (1) litera (f) din regulamentul respectiv, precum și în contextul prelucrării datelor cu caracter personal care este necesară pentru îndeplinirea unei obligații legale care îi revine operatorului, necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, astfel cum se menționează la articolul 6 alineatul (1) literele (c) și, respectiv, (e) din regulamentul respectiv.

([13]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

(35) Pentru a menține un nivel ridicat de reziliență operațională digitală pentru întregul sector financiar și, în același timp, pentru a ține pasul cu evoluțiile tehnologice, prezentul regulament ar trebui să abordeze riscurile care decurg din toate tipurile de servicii TIC. În acest scop, definiția serviciilor TIC în contextul prezentului regulament ar trebui înțeleasă în sens larg, incluzând serviciile digitale și de date furnizate în mod continuu prin intermediul sistemelor TIC unuia sau mai multor utilizatori interni sau externi. Această definiție ar trebui, de exemplu, să includă așa-numitele servicii „over the top", care se încadrează în categoria serviciilor de comunicații electronice. Definiția ar trebui să excludă numai categoria limitată de servicii tradiționale de telefonie analogică care pot fi calificate drept servicii ale rețelei publice comutate de telefonie (PSTN), servicii care utilizează linii terestre, servicii de telefonie istorice (POTS) sau servicii de linii telefonice fixe.

(36) În pofida acoperirii largi prevăzute de prezentul regulament, aplicarea normelor privind reziliența operațională digitală ar trebui să țină seama de diferențele semnificative dintre entitățile financiare din punctul de vedere al dimensiunii lor **și** al profilului general de risc. Ca principiu general, atunci când se distribuie resurse și capacități către punerea în aplicare a cadrului de gestionare a riscurilor TIC, entitățile financiare ar trebui să asigure un echilibru corespunzător între nevoile lor în materie de TIC și dimensiunea și profilul lor general de risc, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, în timp ce autoritățile competente ar trebui să continue să evalueze și să revizuiască abordarea acestei distribuiri.

(37) Prestatorii de servicii de informare cu privire la conturi, menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366, sunt incluși în mod explicit în domeniul de aplicare al prezentului regulament, ținând seama de natura specifică a activităților lor și de riscurile care decurg din acestea. În plus, instituțiile emitente de monedă electronică și instituțiile de plată care sunt exceptate în temeiul articolului 9 alineatul (1) din Directiva 2009/110/CE a Parlamentului European și a Consiliului ([14]) și al articolului 32 alineatul (1) din Directiva (UE) 2015/2366 sunt incluse în domeniul de aplicare al prezentului regulament chiar dacă nu au fost autorizate, în conformitate cu Directiva 2009/110/CE, să emită monedă electronică sau dacă nu au fost autorizate, în conformitate cu Directiva (UE) 2015/2366, să furnizeze și să presteze servicii de plată. Cu toate acestea, oficiile poștale care efectuează operațiuni de virament, menționate la articolul 2 alineatul (5) punctul 3 din Directiva 2013/36/UE a Parlamentului European și a Consiliului ([15]), sunt excluse din domeniul de aplicare al prezentului regulament. Autoritatea competentă pentru instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366, instituțiile emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE și prestatorii de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366 ar trebui să fie autoritatea competentă desemnată în conformitate cu articolul 22 din Directiva (UE) 2015/2366.

(38) Întrucât entitățile financiare mai mari s-ar putea bucura de resurse mai ample și pot mobiliza rapid fonduri pentru a dezvolta structuri de guvernanță și a institui diverse strategii corporative, numai entitățile financiare care nu sunt microîntreprinderi în sensul prezentului regulament ar trebui să aibă obligația de a institui mecanisme de guvernanță mai complexe. Astfel de entități sunt mai bine echipate, în special, pentru a institui funcții de gestionare dedicate supravegherii acordurilor cu furnizorii terți de servicii TIC sau gestionării crizelor, pentru a-și organiza gestionarea riscurilor TIC în conformitate cu modelul celor trei linii de apărare sau pentru a institui un model intern de gestionare și control al riscurilor și pentru a supune cadrul lor de gestionare a riscurilor TIC auditurilor interne.

(39) Unele entități financiare beneficiază de derogări sau fac obiectul unui cadru de reglementare foarte puțin strict în temeiul legislației sectoriale relevante a Uniunii. Printre aceste entități financiare se numără administratorii de fonduri de investiții alternative menționați la articolul 3 alineatul (2) din Directiva 2011/61/UE a Parlamentului European și a Consiliului ([16]), întreprinderile de asigurare și de reasigurare menționate la articolul 4 din Directiva 2009/138/CE a Parlamentului European și a Consiliului ([17]) și instituțiile pentru furnizarea de pensii ocupaționale

([14]) Directiva 2009/110/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 privind accesul la activitate, desfășurarea și supravegherea prudențială a activității instituțiilor emitente de monedă electronică, de modificare a Directivelor 2005/60/CE și 2006/48/CE și de abrogare a Directivei 2000/46/CE (JO L 267, 10.10.2009, p. 7).

([15]) Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

([16]) Directiva 2011/61/UE a Parlamentului European și a Consiliului din 8 iunie 2011 privind administratorii fondurilor de investiții alternative și de modificare a Directivelor 2003/41/CE și 2009/65/CE și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 1095/2010 (JO L 174, 1.7.2011, p. 1).

([17]) Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II), (JO L 335, 17.12.2009, p. 1).

care gestionează sisteme de pensii care împreună nu au mai mult de 15 membri în total. Având în vedere aceste derogări, includerea unor astfel de entități financiare în domeniul de aplicare al prezentului regulament ar fi disproporționată. În plus, prezentul regulament recunoaște particularitățile structurii pieței de intermediere de asigurări, astfel încât intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare care pot fi calificați drept microîntreprinderi sau drept întreprinderi mici sau mijlocii nu ar trebui să facă obiectul prezentului regulament.

(40) Întrucât entitățile menționate la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE sunt excluse din domeniul de aplicare al directivei respective, statele membre ar trebui, prin urmare, să poată alege să excepteze de la aplicarea prezentului regulament astfel de entități situate pe teritoriile lor respective.

(41) În mod similar, pentru a alinia prezentul regulament la domeniul de aplicare al Directivei 2014/65/UE a Parlamentului European și a Consiliului ([18]), este, de asemenea, oportun să se excludă din domeniul de aplicare al prezentului regulament persoanele fizice și juridice menționate la articolele 2 și 3 din directiva respectivă care sunt autorizate să presteze servicii de investiții fără a trebui să obțină o autorizație în temeiul Directivei 2014/65/UE. Cu toate acestea, articolul 2 din Directiva 2014/65/UE exclude, de asemenea, din domeniul de aplicare al directivei respective entități care pot fi calificate drept entități financiare în sensul prezentului regulament, cum ar fi depozitarii centrali de titluri de valoare, organismele de plasament colectiv sau întreprinderile de asigurare și de reasigurare. Excluderea din domeniul de aplicare al prezentului regulament a persoanelor și entităților menționate la articolele 2 și 3 din directiva respectivă nu ar trebui să includă depozitarii centrali de titluri de valoare, organismele de plasament colectiv sau întreprinderile de asigurare și de reasigurare.

(42) În temeiul legislației sectoriale a Uniunii, unele entități financiare fac obiectul unor cerințe sau exceptări mai puțin stricte din motive legate de dimensiunea lor sau de serviciile pe care le furnizează. Categoria respectivă de entități financiare include firmele de investiții mici și neinterconectate, instituțiile mici pentru furnizarea de pensii ocupaționale care pot fi excluse din domeniul de aplicare al Directivei (UE) 2016/2341 în condițiile prevăzute la articolul 5 din directiva respectivă de către statul membru în cauză și care gestionează sisteme de pensii care împreună nu au mai mult de 100 de membri în total, precum și instituțiile exceptate în temeiul Directivei 2013/36/UE. Prin urmare, în conformitate cu principiul proporționalității și pentru a păstra spiritul legislației sectoriale a Uniunii, este, de asemenea, oportun ca aceste entități financiare să facă obiectul unui cadru simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament. Caracterul proporțional al cadrului de gestionare a riscurilor TIC care acoperă aceste entități financiare nu ar trebui să fie modificat de standardele tehnice de reglementare care urmează să fie elaborate de AES. În plus, în conformitate cu principiul proporționalității, este oportun, de asemenea, ca instituțiile de plată menționate la articolul 32 alineatul (1) din Directiva (UE) 2015/2366 și instituțiile emitente de monedă electronică menționate la articolul 9 din Directiva 2009/110/CE care sunt exceptate în conformitate cu dreptul intern de transpunere a respectivelor acte juridice ale Uniunii să facă obiectul unui cadru simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament, în timp ce instituțiile de plată și instituțiile emitente de monedă electronică care nu au fost exceptate în conformitate cu dreptul intern de transpunere a legislației sectoriale a Uniunii ar trebui să respecte cadrul general stabilit de prezentul regulament.

(43) În mod similar, entitățile financiare care pot fi calificate drept microîntreprinderi sau care fac obiectul cadrului simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament nu ar trebui să fie obligate să stabilească un rol de monitorizare a acordurilor încheiate cu furnizori terți de servicii TIC cu privire la utilizarea serviciilor TIC; sau să desemneze un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante; să atribuie unei funcții de control responsabilitatea pentru gestionarea și supravegherea riscurilor TIC și să asigure un nivel adecvat de independență acestei funcții de control pentru a evita conflictele de interese; să documenteze și să revizuiască cel puțin o dată pe an cadrul de gestionare a riscurilor TIC; să asigure realizarea unui audit intern periodic cu privire la cadrul de gestionare a riscurilor TIC; să efectueze evaluări aprofundate în urma unor schimbări majore în infrastructurile și procesele lor de rețea și ale sistemului informatic; să efectueze în mod regulat analize de risc privind sistemele TIC moștenite; să supună punerea în aplicare a planurilor de răspuns și de recuperare în domeniul TIC unor audituri interne independente; să aibă o funcție de gestionare a crizelor, să extindă testarea planurilor privind continuarea activității și a planurilor de răspuns și de recuperare pentru a integra în aceasta scenariile de transfer între infrastructura TIC primară și instalațiile redundante; să raporteze autorităților competente, la cererea acestora, o estimare a costurilor și

([18]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).

pierderilor anuale agregate cauzate de incidentele majore legate de TIC; să mențină capacități TIC redundante; să comunice autorităților naționale competente modificările puse în aplicare în urma verificărilor ulterioare incidentelor legate de TIC; să monitorizeze în permanență evoluțiile tehnologice relevante, să instituie un program cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC prevăzut în prezentul regulament sau să adopte și să revizuiască periodic o strategie privind riscurile TIC generate de părți terțe. În plus, microîntreprinderilor ar trebui să li se solicite să evalueze necesitatea menținerii unor astfel de capacități TIC redundante numai pe baza profilului lor de risc. Microîntreprinderile ar trebui să beneficieze de un regim mai flexibil în ceea ce privește programele de testare a rezilienței operaționale digitale. Atunci când analizează tipul și frecvența testelor care urmează să fie efectuate, acestea ar trebui să asigure un echilibru corespunzător între obiectivul de a menține un nivel ridicat de reziliență operațională digitală, resursele disponibile și profilul general de risc al acestora. Microîntreprinderile și entitățile financiare care fac obiectul cadrului simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament ar trebui să fie exceptate de la obligația de a efectua testări avansate ale instrumentelor, sistemelor și proceselor TIC pe baza testelor de penetrare bazate pe amenințări (TLPT), întrucât numai entitățile financiare care îndeplinesc criteriile stabilite în prezentul regulament ar trebui să fie obligate să efectueze astfel de teste. Având în vedere capacitățile lor limitate, microîntreprinderile ar trebui să poată conveni cu furnizorul terț de servicii TIC să delege drepturile de acces, inspecție și audit ale entității financiare unei părți terțe independente, care urmează să fie desemnată de furnizorul terț de servicii TIC, cu condiția ca entitatea financiară să poată solicita în orice moment toate informațiile și garanțiile relevante cu privire la performanța furnizorului terț de servicii TIC de la partea terță independentă respectivă.

(44) Întrucât numai acele entități financiare care au fost identificate în scopul testării avansate a rezilienței digitale ar trebui să aibă obligația de a efectua teste de penetrare bazate pe amenințări, procesele administrative și costurile financiare implicate de efectuarea unor astfel de teste ar trebui să fie suportate de către un procent mic de entități financiare.

(45) Pentru a asigura alinierea deplină și coerența globală între strategiile de afaceri ale entităților financiare, pe de o parte, și gestionarea riscurilor TIC, pe de altă parte, organele de conducere ale entităților financiare ar trebui să aibă obligația de a îndeplini un rol activ și esențial în orientarea și adaptarea cadrului de gestionare a riscurilor TIC și a strategiei globale privind reziliența operațională digitală. Abordarea care urmează să fie adoptată de organele de conducere nu ar trebui să se concentreze numai pe mijloacele de asigurare a rezilienței sistemelor TIC, ci ar trebui să acopere, de asemenea, persoanele și procesele printr-un set de politici care cultivă, la fiecare nivel corporativ și pentru întregul personal, un sentiment puternic de conștientizare cu privire la riscurile cibernetice și un angajament de a respecta o igienă cibernetică strictă la toate nivelurile. Cea mai importantă responsabilitate a organului de conducere în gestionarea riscurilor TIC ale unei entități financiare ar trebui să constea într-un principiu general al acestei abordări cuprinzătoare, transpus în continuare în implicarea constantă a organului de conducere în monitorizarea gestionării riscurilor TIC.

(46) În plus, principiul responsabilității depline și finale a organului de conducere pentru gestionarea riscurilor TIC ale entității financiare este în strânsă legătură cu necesitatea de a asigura un nivel de investiții legate de TIC și un buget general pentru entitatea financiară care i-ar permite acesteia să atingă un nivel ridicat de reziliență operațională digitală.

(47) Inspirat de bunele practici, de orientările, recomandările și abordările relevante emise la nivel internațional, național și sectorial privind gestionarea riscului cibernetic, prezentul regulament promovează un set de principii care facilitează structura globală a gestionării riscurilor TIC. Prin urmare, atât timp cât principalele capacități pe care entitățile financiare le instituie abordează diversele funcții în gestionarea riscurilor TIC (identificare, protecție și prevenire, detectare, răspuns și recuperare, învățare și evoluție și comunicare) stabilite în prezentul regulament, entitățile financiare ar trebui să aibă în continuare libertatea de a utiliza modele de gestionare a riscurilor TIC diferit formulate sau clasificate.

(48) Pentru a ține pasul cu un peisaj în evoluție al amenințărilor cibernetice, entitățile financiare ar trebui să mențină sisteme TIC actualizate, care să fie fiabile și capabile nu numai de a garanta prelucrarea datelor necesară pentru executarea serviciilor lor, ci și de a asigura o reziliență tehnologică suficientă care să le permită să trateze în mod adecvat nevoile de prelucrare suplimentare cauzate de condiții de criză a pieței sau de alte situații adverse.

(49) Sunt necesare planuri eficace de continuitate a activității și recuperare pentru a permite entităților financiare să soluționeze cu promptitudine și rapiditate incidentele legate de TIC, în special atacurile cibernetice, prin limitarea daunelor și acordând prioritate reluării activităților și acțiunilor de recuperare în conformitate cu politicile lor privind copiile de rezervă. Cu toate acestea, o astfel de reluare a activității nu ar trebui în niciun caz să pună în pericol integritatea și securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor.

(50) Deși prezentul regulament permite entităților financiare să-și stabilească obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, într-un mod flexibil și, prin urmare, să stabilească astfel de obiective ținând seama pe deplin de natura și de importanța funcțiilor relevante și de orice nevoi funcționale specifice, o evaluare a impactului global potențial asupra eficienței pieței ar trebui să fie obligatorie atunci când entitățile financiare stabilesc astfel de obiective.

(51) Propagatorii atacurilor cibernetice tind să urmărească câștiguri financiare direct la sursă, expunând astfel entitățile financiare la consecințe semnificative. Pentru a preveni pierderea integrității sistemelor TIC sau indisponibilitatea acestora și, prin urmare, pentru a evita încălcarea securității datelor și deteriorarea infrastructurii fizice TIC, raportarea incidentelor majore legate de TIC de către entitățile financiare ar trebui să fie îmbunătățită și raționalizată în mod semnificativ. Raportarea incidentelor legate de TIC ar trebui armonizată prin introducerea unei cerințe pentru toate entitățile financiare de a raporta direct autorităților lor competente relevante. În cazul în care o entitate financiară face obiectul supravegherii de către mai multe autorități naționale competente, statele membre ar trebui să desemneze o singură autoritate competentă ca destinatar al unei astfel de raportări. Instituțiile de credit clasificate drept semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013 al Consiliului ([19]) ar trebui să transmită aceste raportări autorităților naționale competente, care ar trebui să transmită ulterior raportul Băncii Centrale Europene (BCE).

(52) Raportarea directă ar trebui să permită autorităților de supraveghere financiară să aibă acces imediat la informații cu privire la incidentele majore legate de TIC. Autoritățile de supraveghere financiară ar trebui, la rândul lor, să transmită detaliile incidentelor majore legate de TIC autorităților nefinanciare publice [cum ar fi autoritățile competente și punctele unice de contact în temeiul Directivei (UE) 2022/2555, autoritățile naționale de protecție a datelor și autoritățile de aplicare a legii în cazul incidentelor majore legate de TIC de natură penală] pentru a spori gradul de conștientizare a acestor autorități cu privire la astfel de incidente și, în cazul echipelor CSIRT, pentru a facilita asistența promptă care poate fi acordată entităților financiare, după caz. În plus, statele membre ar trebui să poată stabili că entitățile financiare sunt cele care ar trebui să furnizeze astfel de informații autorităților publice din afara domeniului serviciilor financiare. Respectivele fluxuri de informații ar trebui să le permită entităților financiare să beneficieze rapid de orice contribuție tehnică relevantă, de consiliere cu privire la măsurile corective și de măsurile subsecvente luate de aceste autorități. Informațiile privind incidentele majore legate de TIC ar trebui canalizate reciproc: autoritățile de supraveghere financiară ar trebui să ofere entității financiare tot feedbackul sau toate orientările necesare, în timp ce AES ar trebui să partajeze date anonimizate privind amenințările cibernetice și vulnerabilitățile legate de un incident, pentru a contribui la o apărare colectivă mai amplă.

(53) Deși toate entitățile financiare ar trebui să aibă obligația de a efectua raportarea incidentelor, nu se preconizează că această cerință le va afecta pe toate în aceeași măsură. Într-adevăr, pragurile de semnificație relevante, precum și termenele de raportare ar trebui să fie ajustate în mod corespunzător, în contextul actelor delegate bazate pe standardele tehnice de reglementare care urmează să fie elaborate de AES, pentru a acoperi numai incidentele majore legate de TIC. În plus, la stabilirea termenelor pentru obligațiile de raportare ar trebui să se țină seama de particularitățile entităților financiare.

(54) Prezentul regulament ar trebui să impună instituțiilor de credit, instituțiilor de plată, prestatorilor de servicii de informare cu privire la conturi și instituțiilor emitente de monedă electronică să raporteze toate incidentele operaționale sau de securitate legate de plăți – raportate anterior în temeiul Directivei (UE) 2015/2366 – indiferent de natura incidentului, legată sau nu de TIC.

([19]) Regulamentul (UE) nr. 1024/2013 al Consiliului din 15 octombrie 2013 de conferire a unor atribuții specifice Băncii Centrale Europene în ceea ce privește politicile legate de supravegherea prudențială a instituțiilor de credit (JO L 287, 29.10.2013, p. 63).

(55) AES ar trebui să aibă sarcina de a evalua fezabilitatea și condițiile unei posibile centralizări a rapoartelor privind incidentele legate de TIC la nivelul Uniunii. O astfel de centralizare ar putea consta într-o platformă unică a UE pentru raportarea incidentelor majore legate de TIC, care fie să primească direct rapoartele relevante și să notifice automat autoritățile naționale competente, fie doar să centralizeze rapoartele relevante transmise de autoritățile naționale competente, îndeplinind astfel un rol de coordonare. AES ar trebui să aibă sarcina de a pregăti, în consultare cu BCE și ENISA, un raport comun în care să analizeze fezabilitatea instituirii unei platforme unice la nivelul UE.

(56) Pentru a atinge un nivel ridicat de reziliență operațională digitală și în conformitate atât cu standardele internaționale relevante (de exemplu, elementele fundamentale ale G7 pentru testele de penetrare bazate pe amenințări), cât și cu cadrele aplicate în Uniune, cum ar fi TIBER-UE, entitățile financiare ar trebui să își testeze periodic sistemele TIC și personalul care are responsabilități legate de TIC în ceea ce privește eficacitatea capacităților lor de prevenire, detectare, răspuns și recuperare, pentru a descoperi și a aborda potențialele vulnerabilități TIC. Pentru a reflecta diferențele existente între diferitele subsectoare financiare și în interiorul acestora în ceea ce privește nivelul de pregătire în materie de securitate cibernetică al entităților financiare, testarea ar trebui să includă o gamă largă de instrumente și acțiuni, de la evaluarea cerințelor de bază (de exemplu, evaluări și examinări ale vulnerabilităților, analize ale surselor deschise, evaluări ale securității rețelelor, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță sau teste de la un capăt la altul) până la testări mai avansate cu ajutorul TLPT. Astfel de testări mai avansate ar trebui să fie obligatorii numai pentru entitățile financiare care sunt suficient de mature din perspectiva TIC pentru a le efectua în mod rezonabil. Prin urmare, testarea rezilienței operaționale digitale impusă prin prezentul regulament ar trebui să fie mai riguroasă pentru entitățile financiare care îndeplinesc criteriile stabilite în prezentul regulament (de exemplu, instituțiile de credit mari, sistemice și cu o TIC matură, bursele de valori, depozitarii centrali de titluri de valoare și contrapărțile centrale) decât pentru alte entități financiare. În același timp, testarea rezilienței operaționale digitale prin intermediul TLPT ar trebui să fie mai relevantă pentru entitățile financiare care operează în subsectoare ale serviciilor financiare esențiale și care joacă un rol sistemic (de exemplu, plăți, servicii bancare și compensări și decontări) și mai puțin relevantă pentru alte subsectoare (de exemplu, administratorii de active și agențiile de rating de credit).

(57) Entitățile financiare implicate în activități transfrontaliere și care își exercită libertatea de stabilire sau de prestare de servicii în Uniune ar trebui să respecte un singur set de cerințe de testare avansată (de exemplu, TLPT) în statul membru de origine, care ar trebui să includă infrastructurile TIC din toate jurisdicțiile în care grupul financiar transfrontalier își desfășoară activitatea pe teritoriul Uniunii, permițând astfel acestor grupuri financiare transfrontaliere să suporte costurile de testare legate de TIC într-o singură jurisdicție.

(58) Pentru a fructifica expertiza deja dobândită de anumite autorități competente, în special în ceea ce privește punerea în aplicare a cadrului TIBER-UE, prezentul regulament ar trebui să permită statelor membre să desemneze o singură autoritate publică responsabilă în sectorul financiar, la nivel național, pentru toate aspectele legate de TLPT, sau autorităților competente să delege, în absența unei astfel de desemnări, exercitarea sarcinilor legate de TLPT unei alte autorități financiare naționale competente.

(59) Întrucât prezentul regulament nu impune entităților financiare să acopere toate funcțiile critice sau importante în cadrul unui singur test de penetrare bazat pe amenințări, entitățile financiare ar trebui să aibă libertatea de a stabili care funcții critice sau importante și câte astfel de funcții ar trebui incluse în sfera unui astfel de test.

(60) Testarea grupată în sensul prezentului regulament – care implică participarea mai multor entități financiare la un TLPT și pentru care un furnizor terț de servicii TIC poate încheia în mod direct acorduri contractuale cu o entitate externă de testare – ar trebui să fie permisă numai în cazul în care se preconizează în mod rezonabil că vor fi afectate în mod negativ calitatea sau securitatea serviciilor furnizate de furnizorul terț de servicii TIC clienților care sunt entități care nu intră în domeniul de aplicare al prezentului regulament, sau confidențialitatea datelor referitoare la astfel de servicii. Testarea grupată ar trebui, de asemenea, să facă obiectul unor garanții (conducerea de către o entitate financiară desemnată, calibrarea numărului de entități financiare participante) pentru a asigura un exercițiu de testare riguros pentru entitățile financiare implicate care îndeplinesc obiectivele TLPT în temeiul prezentului regulament.

(61) Pentru a profita de resursele interne disponibile la nivel corporativ, prezentul regulament ar trebui să permită utilizarea unor entități interne de testare în scopul efectuării TLPT, cu condiția să existe aprobarea autorității de supraveghere, să nu existe conflicte de interese și să existe o alternare periodică între utilizarea entităților interne și a celor externe de testare (la fiecare trei teste), solicitând, în același timp, ca furnizorul de informații privind amenințările din TLPT să fie întotdeauna extern entității financiare. Responsabilitatea pentru desfășurarea TLPT ar trebui să revină în totalitate entității financiare. Atestările furnizate de autorități ar trebui să fie exclusiv în scopul recunoașterii reciproce și nu ar trebui să împiedice nicio acțiune ulterioară necesară pentru a aborda riscurile TIC la care este expusă entitatea financiară și nici nu ar trebui să fie considerate drept o validare de către autoritățile de supraveghere a capacităților unei entități financiare de gestionare și atenuare a riscurilor TIC.

(62) Pentru a asigura o monitorizare solidă a riscurilor TIC generate de părți terțe în sectorul financiar, este necesar să se stabilească un set de norme bazate pe principii care să ghideze entitățile financiare atunci când monitorizează riscurile care apar în contextul funcțiilor externalizate către furnizorii terți de servicii TIC, în special cu privire la serviciile TIC care sprijină funcții critice sau importante, precum și, la un nivel mai general, în contextul tuturor dependențelor față de furnizorii terți de servicii TIC.

(63) Pentru a aborda complexitatea diferitelor surse de riscuri TIC, ținând seama, în același timp, de multitudinea și diversitatea furnizorilor de soluții tehnologice care permit furnizarea fără probleme a serviciilor financiare, prezentul regulament ar trebui să acopere o gamă largă de furnizori terți de servicii TIC, inclusiv furnizori de servicii de cloud computing, software, servicii de analiză a datelor și furnizori de servicii de centre de date. În mod similar, întrucât entitățile financiare ar trebui să identifice și să gestioneze în mod eficace și coerent toate tipurile de riscuri, inclusiv în contextul serviciilor TIC achiziționate în cadrul unui grup financiar, ar trebui să se clarifice faptul că întreprinderile care fac parte dintr-un grup financiar și furnizează servicii TIC în principal societății-mamă sau filialelor ori sucursalelor societății-mamă a acestora, precum și entitățile financiare care furnizează servicii TIC altor entități financiare ar trebui, de asemenea, să fie considerate furnizori terți de servicii TIC în temeiul prezentului regulament. În cele din urmă, având în vedere evoluția pieței serviciilor de plată, care devine din ce în ce mai dependentă de soluții tehnice complexe și având în vedere tipurile emergente de servicii de plată și soluțiile legate de plăți, participanții la ecosistemul serviciilor de plată, la furnizarea de activități de procesare a plăților sau la exploatarea infrastructurilor de plată ar trebui, de asemenea, să fie considerați drept furnizori terți de servicii TIC în temeiul prezentului regulament, cu excepția băncilor centrale atunci când operează sisteme de plată sau de decontare a titlurilor de valoare, precum și a autorităților publice atunci când furnizează servicii legate de TIC în contextul îndeplinirii funcțiilor statului.

(64) O entitate financiară ar trebui să rămână în orice moment pe deplin responsabilă de respectarea obligațiilor sale prevăzute în prezentul regulament. Entitățile financiare ar trebui să aplice o abordare proporțională în ceea ce privește monitorizarea riscurilor care apar la nivelul furnizorilor terți de servicii TIC, ținând seama în mod corespunzător de natura, amploarea, complexitatea și importanța dependențelor lor legate de TIC, de caracterul critic sau de importanța serviciilor, proceselor sau funcțiilor care fac obiectul acordurilor contractuale și, în cele din urmă, în baza unei evaluări atente a oricărui impact potențial asupra continuității și calității serviciilor financiare la nivel individual și la nivel de grup, după caz.

(65) Desfășurarea unei astfel de monitorizări ar trebui să urmeze o abordare strategică a riscurilor TIC generate de părți terțe, formalizată prin adoptarea de către organul de conducere al entității financiare a unei strategii dedicate privind riscurile TIC generate de părți terțe, bazate pe o verificare continuă a tuturor acestor dependențe față de furnizorii terți de servicii TIC. Pentru a spori gradul de conștientizare în materie de supraveghere cu privire la dependențele față de furnizorii terți de servicii TIC și în vederea sprijinirii suplimentare a activității în contextul cadrului de supraveghere instituit prin prezentul regulament, toate entitățile financiare ar trebui să aibă obligația de a menține un registru de informații cu privire la toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC. Autoritățile de supraveghere financiară ar trebui să fie în măsură să solicite registrul complet sau să solicite secțiuni specifice din acesta și, astfel, să obțină informații esențiale pentru a înțelege mai bine dependențele în materie de TIC ale entităților financiare.

(66) O analiză precontractuală aprofundată ar trebui să stea la baza încheierii formale a acordurilor contractuale, în special prin axarea pe elemente precum caracterul critic sau importanța serviciilor sprijinite de contractul TIC avut în vedere, aprobările necesare din partea autorităților de supraveghere sau alte condiții, posibilul risc de concentrare implicat, precum și aplicând toate diligențele necesare în procesul de selecție și evaluare a furnizorilor terți de servicii TIC și prin evaluarea potențialelor conflicte de interese. În ceea ce privește acordurile contractuale privind funcțiile critice sau importante, entitățile financiare ar trebui să ia în considerare utilizarea de către furnizorii terți de servicii TIC a celor mai recente și mai înalte standarde de securitate a informațiilor. Încetarea acordurilor contractuale ar putea fi determinată de cel puțin o serie de circumstanțe care indică deficiențe la nivelul furnizorului terț de servicii

TIC, în special încălcări semnificative ale legislației sau ale clauzelor contractuale, circumstanțe care indică o posibilă modificare a îndeplinirii funcțiilor prevăzute în acordurile contractuale, dovezi ale deficiențelor furnizorului terț de servicii TIC în gestionarea globală a riscurilor TIC sau circumstanțe care indică incapacitatea autorității competente relevante de a supraveghea în mod eficace entitatea financiară.

(67) Pentru a aborda impactul sistemic al riscului de concentrare a serviciilor TIC furnizate de către părți terțe, prezentul regulament promovează o soluție echilibrată prin adoptarea unei abordări flexibile și progresive cu privire la un astfel de risc de concentrare, deoarece impunerea unor plafoane rigide sau limitări stricte ar putea împiedica desfășurarea activității comerciale și ar putea restrânge libertatea contractuală. Entitățile financiare ar trebui să evalueze în detaliu acordurile contractuale preconizate pentru a identifica probabilitatea apariției unui astfel de risc, inclusiv prin intermediul unor analize aprofundate ale acordurilor de subcontractare, în special atunci când sunt încheiate cu furnizori terți de servicii TIC stabiliți într-o țară terță. În această etapă și în vederea găsirii unui echilibru între necesitatea de a menține libertatea contractuală și cea de a garanta stabilitatea financiară, nu se consideră adecvat să se stabilească norme privind plafoane și limite stricte pentru expunerile la furnizorii terți de servicii TIC. În ceea ce privește cadrul de supraveghere, un supraveghetor principal numit în temeiul prezentului regulament ar trebui, în ceea ce privește furnizorii terți esențiali de servicii TIC, să acorde o atenție deosebită înțelegerii depline a amplorii interdependențelor și descoperirii cazurilor specifice în care un grad ridicat de concentrare a furnizorilor terți esențiali de servicii TIC din Uniune este susceptibil să exercite o presiune asupra stabilității și integrității sistemului financiar al Uniunii și să mențină un dialog cu furnizorii terți esențiali de servicii TIC, în cazurile în care acest risc specific este identificat.

(68) Pentru a evalua și monitoriza în mod regulat capacitatea unui furnizor terț de servicii TIC de a furniza servicii în condiții de siguranță unei entități financiare fără efecte negative asupra rezilienței operaționale digitale a unei entități financiare, ar trebui armonizate mai multe elemente contractuale esențiale cu furnizorii terți de servicii TIC. O astfel de armonizare ar trebui să acopere domeniile minime care sunt esențiale pentru a permite o monitorizare completă de către entitatea financiară a riscurilor care ar putea fi generate de furnizorul terț de servicii TIC, din perspectiva necesității unei entități financiare de a-și asigura reziliența digitală, deoarece aceasta depinde în mare măsură de stabilitatea, funcționalitatea, disponibilitatea și securitatea serviciilor TIC primite.

(69) La renegocierea acordurilor contractuale pentru a urmări alinierea la cerințele prezentului regulament, entitățile financiare și furnizorii terți de servicii TIC ar trebui să se asigure că acoperă principalele dispoziții contractuale prevăzute în prezentul regulament.

(70) Definiția „funcției critice sau importante” prevăzută în prezentul regulament ar trebui să includă „funcțiile critice” astfel cum sunt definite la articolul 2 alineatul (1) punctul 35 din Directiva 2014/59/UE a Parlamentului European și a Consiliului ([20]). În consecință, funcțiile considerate critice în temeiul Directivei 2014/59/UE sunt incluse în definiția funcțiilor critice în sensul prezentului regulament.

(71) Independent de caracterul critic sau de importanța funcției sprijinite de serviciile TIC, acordurile contractuale ar trebui, în special, să prevadă specificații cu privire la descrierile complete ale funcțiilor și serviciilor, a locurilor în care sunt furnizate astfel de funcții și în care urmează să fie prelucrate datele, precum și o indicare a descrierilor la nivelul serviciilor. Alte elemente esențiale pentru a permite unei entități financiare să monitorizeze riscurile TIC generate de părți terțe sunt: dispozițiile contractuale care specifică modul în care accesibilitatea, disponibilitatea, integritatea, securitatea și protecția datelor cu caracter personal sunt asigurate de furnizorul terț de servicii TIC, dispozițiile care stabilesc garanțiile relevante pentru a permite accesul, recuperarea și restituirea datelor în caz de insolvență, rezoluție sau întrerupere a operațiunilor comerciale ale furnizorului terț de servicii TIC, precum și dispozițiile care impun furnizorului terț de servicii TIC să ofere asistență în cazul unor incidente TIC în legătură cu serviciile furnizate, fără costuri suplimentare sau la un cost stabilit ex ante; dispozițiile privind obligația furnizorului

([20]) Directiva 2014/59/UE a Parlamentului European și a Consiliului din 15 mai 2014 de instituire a unui cadru pentru redresarea și rezoluția instituțiilor de credit și a firmelor de investiții și de modificare a Directivei 82/891/CEE a Consiliului și a Directivelor 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE și 2013/36/UE și a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 648/2012 ale Parlamentului European și ale Consiliului (JO L 173, 12.6.2014, p. 190).

terț de servicii TIC de a coopera pe deplin cu autoritățile competente și cu autoritățile de rezoluție ale entității financiare și dispozițiile privind drepturile de încetare și perioade minime de preaviz aferente încetării acordurilor contractuale, în conformitate cu așteptările autorităților competente și ale autorităților de rezoluție.

(72) În plus față de aceste dispoziții contractuale și pentru a se asigura că entitățile financiare păstrează controlul deplin asupra tuturor evoluțiilor care au loc la nivelul terților și care le pot afecta securitatea TIC, contractele pentru furnizarea de servicii TIC care sprijină funcții critice sau importante ar trebui, de asemenea, să prevadă următoarele: specificarea descrierilor complete la nivelul serviciilor, cu obiective de performanță cantitative și calitative precise, pentru a permite, fără întârzieri nejustificate, luarea de măsuri corective adecvate atunci când nivelurile convenite ale serviciilor nu sunt atinse; perioadele de preaviz și obligațiile de raportare relevante ale furnizorului terț de servicii TIC în cazul unor evoluții cu un potențial impact semnificativ asupra capacității furnizorului terț de servicii TIC de a furniza în mod eficace serviciile TIC respective; o cerință impusă furnizorului terț de servicii TIC de a pune în aplicare și de a testa planuri pentru situații neprevăzute și de a dispune de măsuri, instrumente și politici de securitate TIC care să permită furnizarea în condiții de siguranță a serviciilor, precum și de a participa și de a coopera pe deplin la TLPT efectuat de entitatea financiară.

(73) Contractele pentru furnizarea de servicii TIC care sprijină funcții critice sau importante ar trebui să conțină, de asemenea, dispoziții care să permită drepturile de acces, de inspecție și de audit exercitate de entitatea financiară sau de o parte terță desemnată, precum și dreptul de a produce copii ca instrumente esențiale pentru monitorizarea continuă de către entitățile financiare a performanței furnizorului terț de servicii TIC, alături de deplina cooperare a furnizorului de servicii în timpul inspecțiilor. În mod similar, autoritatea competentă a entității financiare ar trebui să dispună de dreptul, pe baza unor preavize, de a inspecta și a audita furnizorul terț de servicii TIC, sub rezerva protecției informațiilor confidențiale.

(74) Astfel de acorduri contractuale ar trebui, de asemenea, să prevadă strategii de ieșire specifice pentru a asigura, în special, perioade de tranziție obligatorii în cursul cărora furnizorii terți de servicii TIC ar trebui să continue să furnizeze serviciile relevante în vederea reducerii riscului de perturbări la nivelul entității financiare sau pentru a permite acesteia din urmă să treacă efectiv la utilizarea altor furnizori terți de servicii TIC sau, alternativ, să treacă la utilizarea de soluții dezvoltate pe plan intern, în concordanță cu complexitatea serviciului TIC furnizat. În plus, entitățile financiare care intră în domeniul de aplicare al Directivei 2014/59/UE ar trebui să se asigure că contractele relevante pentru servicii TIC sunt solide și pe deplin executorii în cazul rezoluției respectivelor entități financiare. Prin urmare, în conformitate cu așteptările autorităților de rezoluție, entitățile financiare respective ar trebui să se asigure că contractele relevante pentru serviciile TIC sunt reziliente în ceea ce privește rezoluția. Atât timp cât își îndeplinesc în continuare obligațiile de plată, entitățile financiare respective ar trebui să se asigure, printre alte cerințe, că contractele relevante pentru servicii TIC conțin clauze de neîncetare, de nesuspendare și de nemodificare din motive de restructurare sau de rezoluție.

(75) În plus, utilizarea voluntară a clauzelor contractuale standard elaborate de autoritățile publice sau de instituțiile Uniunii, în special utilizarea clauzelor contractuale elaborate de Comisie pentru serviciile de cloud computing ar putea oferi un confort suplimentar entităților financiare și furnizorilor lor terți de servicii TIC, prin creșterea nivelului lor de securitate juridică cu privire la utilizarea serviciilor de cloud computing în sectorul financiar, în deplină conformitate cu cerințele și așteptările prevăzute în dreptul Uniunii privind serviciile financiare. Elaborarea unor clauze contractuale standard se bazează pe măsurile deja prevăzute în Planul de acțiune privind Fintech din 2018, care a anunțat intenția Comisiei de a încuraja și de a facilita elaborarea unor clauze contractuale standard pentru utilizarea externalizării serviciilor de cloud computing de către entitățile financiare, pe baza eforturilor depuse de părțile interesate transsectoriale în domeniul serviciilor de cloud computing, pe care Comisia le-a facilitat cu ajutorul implicării sectorului financiar.

(76) Cu scopul de a promova convergența și eficiența în ceea ce privește abordările în materie de supraveghere a riscurilor TIC generate de părți terțe în sectorul financiar, precum și de a consolida reziliența operațională digitală a entităților financiare care se bazează pe furnizori terți esențiali de servicii TIC pentru furnizarea serviciilor TIC care sprijină furnizarea de servicii financiare, contribuind astfel la menținerea stabilității sistemului financiar al Uniunii și a integrității pieței interne a serviciilor financiare, furnizorii terți esențiali de servicii TIC ar trebui să facă obiectul unui cadru de supraveghere al Uniunii. Deși instituirea cadrului de supraveghere este justificată de valoarea adăugată a luării de măsuri la nivelul Uniunii și de rolul inerent și particularitățile utilizării serviciilor TIC în furnizarea de

servicii financiare, ar trebui reamintit, în același timp, că această soluție pare adecvată numai în contextul prezentului regulament, care abordează în mod specific reziliența operațională digitală în sectorul financiar. Cu toate acestea, un astfel de cadru de supraveghere nu ar trebui considerat un nou model de supraveghere la nivelul Uniunii în domeniul serviciilor și activităților financiare.

(77) Cadrul de supraveghere ar trebui să se aplice numai furnizorilor terți esențiali de servicii TIC. Prin urmare, ar trebui să existe un mecanism de desemnare care să țină seama de dimensiunea și natura dependenței sectorului financiar de astfel de furnizori terți de servicii TIC. Mecanismul respectiv ar trebui să implice un set de criterii cantitative și calitative pentru a stabili parametrii critici ca bază pentru includerea în cadrul de supraveghere. Pentru a asigura acuratețea acestei evaluări și indiferent de structura corporativă a furnizorului terț de servicii TIC, astfel de criterii ar trebui, în cazul unui furnizor terț de servicii TIC care face parte dintr-un grup mai larg, să ia în considerare întreaga structură de grup a furnizorului terț de servicii TIC. Pe de o parte, furnizorii terți esențiali de servicii TIC care nu sunt desemnați în mod automat în temeiul aplicării criteriilor respective ar trebui să aibă posibilitatea de a opta să fie parte din cadrul de supraveghere în mod voluntar, pe de altă parte, furnizorii terți de servicii TIC care fac deja obiectul cadrelor mecanismului de supraveghere care sprijină îndeplinirea sarcinilor Sistemului European al Băncilor Centrale, astfel cum sunt menționate la articolul 127 alineatul (2) din TFUE, ar trebui să fie exceptați.

(78) În mod similar, entitățile financiare care furnizează servicii TIC altor entități financiare, deși aparțin categoriei furnizorilor terți de servicii TIC în temeiul prezentului regulament, ar trebui, de asemenea, să fie exceptate de la cadrul de supraveghere, deoarece fac deja obiectul mecanismelor de supraveghere instituite prin dreptul relevant al Uniunii privind serviciile financiare. După caz, autoritățile competente ar trebui să țină seama, în contextul activităților lor de supraveghere, de riscurile TIC pe care entitățile financiare care furnizează servicii TIC le prezintă pentru entitățile financiare. De asemenea, având în vedere mecanismele existente de monitorizare a riscurilor la nivel de grup, aceeași derogare ar trebui introdusă pentru furnizorii terți de servicii TIC care furnizează servicii în principal entităților din propriul grup. Furnizorii terți de servicii TIC care furnizează servicii TIC numai într-un stat membru entităților financiare care își desfășoară activitatea numai în statul membru respectiv ar trebui, de asemenea, să fie exceptați de la mecanismul de desemnare din cauza activităților lor limitate și a lipsei impactului transfrontalier.

(79) Transformarea digitală prin care trec serviciile financiare a generat un nivel fără precedent de utilizare a serviciilor TIC și de dependență de acestea. Întrucât a devenit imposibilă furnizarea de servicii financiare fără utilizarea serviciilor de cloud computing, a soluțiilor software și a serviciilor legate de date, ecosistemul financiar al Uniunii a devenit intrinsec codependent de anumite servicii TIC furnizate de furnizorii de servicii TIC. Unii dintre acești furnizori, inovatori în dezvoltarea și aplicarea tehnologiilor bazate pe TIC, joacă un rol semnificativ în furnizarea de servicii financiare sau au devenit integrați în lanțul valoric al serviciilor financiare. Prin urmare, aceștia au devenit esențiali pentru stabilitatea și integritatea sistemului financiar al Uniunii. Această dependență generalizată de serviciile oferite de furnizori terți esențiali de servicii TIC, combinată cu interdependența sistemelor informatice ale diferiților operatori de pe piață, creează un risc direct și potențial grav pentru sistemul de servicii financiare al Uniunii și pentru continuitatea furnizării de servicii financiare în cazul în care furnizorii terți esențiali de servicii TIC ar fi afectați de perturbări operaționale sau de incidente cibernetice majore. Incidentele cibernetice au o capacitate distinctă de a se multiplica și de a se răspândi în întreg sistemul financiar într-un ritm considerabil mai rapid decât alte tipuri de riscuri monitorizate în sectorul financiar și se pot extinde dincolo de sectoare și dincolo de frontierele geografice. Acestea au potențialul de a evolua într-o criză sistemică, în care încrederea în sistemul financiar a fost erodată din cauza perturbării funcțiilor de sprijinire a economiei reale sau a unor pierderi financiare substanțiale, atingând un nivel la care sistemul financiar nu este în măsură să reziste sau care necesită aplicarea unor măsuri de absorbție a șocurilor majore. Pentru a preveni apariția acestor scenarii și, astfel, punerea în pericol a stabilității financiare și a integrității Uniunii, este esențial să se asigure convergența practicilor de supraveghere legate de riscurile TIC generate de părți terțe în domeniul financiar, în special prin noi norme care să permită supravegherea de către Uniune a furnizorilor terți esențiali de servicii TIC.

(80) Cadrul de supraveghere depinde în mare măsură de gradul de colaborare dintre supraveghetorul principal și furnizorul terț esențial de servicii TIC care furnizează entităților financiare servicii care afectează furnizarea de servicii financiare. Supravegherea reușită se bazează, printre altele, pe capacitatea supraveghetorului principal de a efectua în mod eficace misiuni de monitorizare și inspecții pentru a evalua normele, controalele și procesele utilizate de furnizorii terți esențiali de servicii TIC, precum și pe capacitatea de a evalua impactul potențial cumulativ al activităților lor asupra stabilității financiare și a integrității sistemului financiar. În același timp, este esențial ca furnizorii terți esențiali de servicii TIC să urmeze recomandările supraveghetorului principal și să răspundă preocupărilor acestuia. Întrucât o lipsă de cooperare din partea unui furnizor terț esențial de servicii TIC care furnizează servicii care afectează furnizarea de servicii financiare, cum ar fi refuzul de a acorda acces la sediul său sau de a prezenta informații, ar priva, în cele din urmă, supraveghetorul principal de instrumentele sale esențiale de evaluare a riscurilor TIC generate de părți terțe și ar putea avea un impact negativ asupra stabilității financiare și a integrității sistemului financiar, este necesar să se prevadă, de asemenea, un regim de sancționare proporțional.

(81) În acest context, necesitatea ca supraveghetorul principal să impună penalități cu titlu cominatoriu pentru a obliga furnizorii terți esențiali de servicii TIC să respecte obligațiile în materie de transparență și de acces prevăzute în prezentul regulament nu ar trebui să fie pusă în pericol de dificultățile generate de executarea respectivelor penalități în legătură cu furnizorii terți esențiali de servicii TIC stabiliți într-o țară terță. Pentru a asigura caracterul executoriu al unor astfel de penalități și pentru a permite o punere în aplicare rapidă a procedurilor care susțin dreptul la apărare al furnizorilor terți esențiali de servicii TIC în contextul mecanismului de desemnare și al emiterii de recomandări, respectivii furnizorii terți esențiali de servicii TIC care furnizează entităților financiare servicii care afectează furnizarea de servicii financiare ar trebui să aibă obligația de a menține o prezență comercială adecvată în Uniune. Având în vedere natura supravegherii și absența unor mecanisme comparabile în alte jurisdicții, nu există mecanisme alternative adecvate care să asigure acest obiectiv prin intermediul unei cooperări eficace cu autoritățile de supraveghere financiară din țările terțe în ceea ce privește monitorizarea impactului riscurilor operaționale digitale prezentate de furnizorii terți de servicii TIC cu impact sistemic, care pot fi calificați drept furnizori terți esențiali de servicii TIC stabiliți într-o țară terță. Prin urmare, pentru a continua furnizarea de servicii TIC către entități financiare din Uniune, un furnizor terț de servicii TIC stabilit într-o țară terță care a fost desemnat ca fiind esențial în conformitate cu prezentul regulament ar trebui să întreprindă, în termen de 12 luni de la desemnarea sa, toate măsurile necesare pentru a asigura stabilirea sa în Uniune, prin înființarea unei filiale, astfel cum este definită în întregul acquis al Uniunii, și anume în Directiva 2013/34/UE a Parlamentului European și a Consiliului ([21]).

(82) Cerința de a înființa o filială în Uniune nu ar trebui să împiedice furnizorul terț esențial de servicii TIC să furnizeze servicii TIC și asistența tehnică aferentă de la instalații și infrastructuri situate în afara Uniunii. Prezentul regulament nu impune o obligație de localizare a datelor, deoarece nu impune stocarea sau prelucrarea datelor în Uniune.

(83) Furnizorii terți esențiali de servicii TIC ar trebui să fie în măsură să furnizeze servicii TIC oriunde în lume, nu neapărat sau nu numai de la sedii situate în Uniune. Activitățile de supraveghere ar trebui să se desfășoare mai întâi la sediile situate în Uniune și prin interacțiunea cu entități situate în Uniune, inclusiv cu filialele înființate de furnizori terți esențiali de servicii TIC în temeiul prezentului regulament. Cu toate acestea, astfel de acțiuni în cadrul Uniunii ar putea fi insuficiente pentru a permite supraveghetorului principal să își îndeplinească pe deplin și în mod eficace sarcinile care îi revin în temeiul prezentului regulament. Prin urmare, supraveghetorul principal ar trebui să fie, de asemenea, în măsură să își exercite competențele de supraveghere relevante în țări terțe. Exercitarea acestor competențe în țări terțe ar trebui să permită supraveghetorului principal să examineze instalațiile de la care serviciile TIC sau de asistență tehnică sunt efectiv furnizate sau gestionate de furnizorul terț esențial de servicii TIC și ar trebui să ofere supraveghetorului principal o înțelegere cuprinzătoare și operațională a gestionării riscurilor TIC de către furnizorul terț esențial de servicii TIC. Posibilitatea ca supraveghetorul principal, în calitate de agenție a Uniunii, să exercite competențe în afara teritoriului Uniunii ar trebui să fie încadrată în mod corespunzător de condițiile relevante, în special de consimțământul furnizorului terț esențial de servicii TIC în cauză. În mod similar, autoritățile relevante din țara terță ar trebui să fie informate cu privire la exercitarea, pe teritoriul lor, a activităților supraveghetorului principal și nu ar trebui să aibă obiecții la aceasta. Cu toate acestea, pentru a asigura punerea în aplicare eficace și fără a aduce atingere competențelor respective ale instituțiilor Uniunii și ale statelor membre,

([21]) Directiva 2013/34/UE a Parlamentului European și a Consiliului din 26 iunie 2013 privind situațiile financiare anuale, situațiile financiare consolidate și rapoartele conexe ale anumitor tipuri de întreprinderi, de modificare a Directivei 2006/43/CE a Parlamentului European și a Consiliului și de abrogare a Directivelor 78/660/CEE și 83/349/CEE ale Consiliului (JO L 182, 29.6.2013, p. 19).

aceste competențe trebuie, de asemenea, să fie pe deplin ancorate în încheierea acordurilor de cooperare administrativă cu autoritățile relevante din țara terță în cauză. Prin urmare, prezentul regulament ar trebui să permită AES să încheie acorduri de cooperare administrativă cu autoritățile relevante din țări terțe, care nu ar trebui să creeze obligații juridice în ceea ce privește Uniunea și statele sale membre.

(84) Pentru a facilita comunicarea cu supraveghetorul principal și pentru a asigura o reprezentare adecvată, furnizorii terți esențiali de servicii TIC care fac parte dintr-un grup ar trebui să desemneze o persoană juridică drept punct de coordonare.

(85) Cadrul de supraveghere nu ar trebui să aducă atingere competenței statelor membre de a derula propriile misiuni de supraveghere sau monitorizare cu privire la furnizorii terți de servicii TIC care nu sunt desemnați ca fiind esențiali în temeiul prezentului regulament, dar care sunt considerați importanți la nivel național.

(86) Pentru a valorifica arhitectura instituțională multistratificată în domeniul serviciilor financiare, Comitetul comun al AES ar trebui să asigure în continuare coordonarea transsectorială generală în ceea ce privește toate aspectele legate de riscurile TIC, în conformitate cu sarcinile sale privind securitatea cibernetică. Acesta ar trebui să fie sprijinit de un nou subcomitet (Forumul de supraveghere) care desfășoară activități pregătitoare atât pentru deciziile individuale adresate furnizorilor terți esențiali de servicii TIC, cât și pentru emiterea de recomandări colective, în special cu privire la analiza comparativă a programelor de supraveghere pentru furnizorii terți esențiali de servicii TIC, precum și pentru identificarea celor mai bune practici pentru abordarea aspectelor legate de riscul de concentrare a TIC.

(87) Pentru a se asigura că furnizorii terți esențiali de servicii TIC sunt supravegheați în mod adecvat și eficace la nivelul Uniunii, prezentul regulament prevede că oricare dintre cele trei AES ar putea fi desemnată drept supraveghetor principal. Atribuirea individuală a unui furnizor terț esențial de servicii TIC uneia dintre cele trei AES ar trebui să rezulte dintr-o evaluare a preponderenței entităților financiare care își desfășoară activitatea în sectoarele financiare pentru care AES respectivă are atribuții. Această abordare ar trebui să conducă la o repartizare echilibrată a sarcinilor și atribuțiilor între cele trei AES, în contextul exercitării funcțiilor de supraveghere, și ar trebui să utilizeze în mod optim resursele umane și expertiza tehnică disponibile în fiecare dintre cele trei AES.

(88) Supraveghetorilor principali ar trebui să li se acorde competențele necesare pentru a efectua investigații, pentru a desfășura inspecții la fața locului și în afara sediului la sediile și locațiile furnizorilor terți esențiali de servicii TIC și pentru a obține informații complete și actualizate. Aceste competențe ar trebui să îi permită supraveghetorului principal să obțină informații concrete cu privire la tipul, dimensiunea și impactul riscurilor TIC generate de părți terțe pentru entitățile financiare și, în cele din urmă, pentru sistemul financiar al Uniunii. Încredințarea rolului principal de supraveghere AES este o condiție prealabilă pentru înțelegerea și abordarea dimensiunii sistemice a riscurilor TIC în domeniul financiar. Impactul furnizorilor terți esențiali de servicii TIC asupra sectorului serviciilor financiare din Uniune și potențialele probleme cauzate de riscul asociat de concentrare a TIC impun adoptarea unei abordări colective la nivelul Uniunii. Efectuarea simultană a mai multor misiuni de audit și exercitarea simultană a mai multor drepturi de acces, efectuate separat de numeroase autorități competente, cu o coordonare redusă sau inexistentă între acestea, ar împiedica supraveghetorii financiari să obțină o imagine de ansamblu completă și cuprinzătoare a riscurilor TIC generate de părți terțe în Uniune, creând în același timp redundanță, sarcini și complexitate pentru furnizorii terți esențiali de servicii TIC în cazul în care aceștia ar face obiectul a numeroase cereri de monitorizare și inspecție.

(89) Având în vedere impactul semnificativ al desemnării lor ca fiind esențiali, prezentul regulament ar trebui să asigure respectarea drepturilor furnizorilor terți esențiali de servicii TIC pe tot parcursul punerii în aplicare a cadrului de supraveghere. Înainte de a fi desemnați drept esențiali, furnizorii respectivi ar trebui, de exemplu, să aibă dreptul să prezinte supraveghetorului principal o declarație motivată care să conțină orice informații relevante în scopul evaluării legate de desemnarea lor. Întrucât supraveghetorul principal ar trebui să fie împuternicit să prezinte recomandări cu privire la aspecte legate de riscurile TIC și la măsurile reparatorii adecvate, care includ competența de a se opune anumitor acorduri contractuale care afectează în ultimă instanță stabilitatea entității financiare sau a sistemului financiar; furnizorilor terți esențiali de servicii TIC ar trebui, de asemenea, să li se ofere posibilitatea de a furniza, înainte de finalizarea recomandărilor respective, explicații cu privire la impactul preconizat al soluțiilor avute în vedere în recomandări asupra clienților care sunt entități care nu intră în domeniul de aplicare al

prezentului regulament și să formuleze soluții pentru atenuarea riscurilor. Furnizorii terți esențiali de servicii TIC care nu sunt de acord cu recomandările ar trebui să prezinte o explicație motivată a intenției lor de a nu aproba recomandarea. În cazul în care nu se prezintă o astfel de explicație motivată sau explicația motivată este considerată insuficientă, supraveghetorul principal ar trebui să emită un anunț public care să descrie succint problema neconformității.

(90) Autoritățile competente ar trebui să includă în mod corespunzător sarcina de a verifica respectarea pe fond a recomandărilor emise de supraveghetorul principal în funcțiile lor cu privire la supravegherea prudențială a entităților financiare. Autoritățile competente ar trebui să poată solicita entităților financiare să ia măsuri suplimentare pentru a aborda riscurile identificate în recomandările supraveghetorului principal și ar trebui să emită, în timp util, notificări în acest sens. În cazul în care supraveghetorul principal adresează recomandări furnizorilor terți esențiali de servicii TIC care sunt supravegheați în temeiul Directivei (UE) 2022/2555, autoritățile competente ar trebui să poată consulta, în mod voluntar și înainte de a adopta măsuri suplimentare, autoritățile competente în temeiul directivei respective pentru a promova o abordare coordonată în ceea ce privește furnizorii terți esențiali de servicii TIC în cauză.

(91) Exercitarea supravegherii ar trebui să fie ghidată de trei principii operaționale menite să asigure: (a) o coordonare strânsă între AES în rolurile lor de supraveghetori principali, prin intermediul unei rețele de supraveghere comună (RSC), (b) coerența cu cadrul instituit prin Directiva (UE) 2022/2555 (printr-o consultare voluntară a organismelor în temeiul directivei respective pentru a evita duplicarea măsurilor care vizează furnizorii terți esențiali de servicii TIC) și (c) aplicarea diligenței pentru a reduce la minimum riscul potențial de perturbare a serviciilor furnizate de furnizorii terți esențiali de servicii TIC clienților care sunt entități exceptate din domeniul de aplicare al prezentului regulament.

(92) Cadrul de supraveghere nu ar trebui să înlocuiască sau să substituie în niciun fel sau parțial cerința ca entitățile financiare să gestioneze ele însele riscurile generate de utilizarea furnizorilor terți de servicii TIC, inclusiv obligația acestora de a menține o monitorizare continuă a acordurilor contractuale încheiate cu furnizorii terți esențiali de servicii TIC. În mod similar, cadrul de supraveghere nu ar trebui să afecteze responsabilitatea deplină a entităților financiare de respectare și îndeplinire a tuturor obligațiilor legale prevăzute în prezentul regulament și în dreptul relevant privind serviciile financiare.

(93) Pentru a evita duplicările și suprapunerile, autoritățile competente ar trebui să se abțină de la a lua în mod individual orice măsuri destinate monitorizării riscurilor implicate de furnizorul terț esențial de servicii TIC și ar trebui, în acest sens, să se bazeze pe evaluarea relevantă a supraveghetorului principal. Orice măsuri ar trebui, în orice caz, să fie coordonate și convenite în prealabil cu supraveghetorul principal în contextul exercitării sarcinilor din cadrul de supraveghere.

(94) Pentru a promova convergența la nivel internațional în ceea ce privește utilizarea celor mai bune practici în revizuirea și monitorizarea gestionării riscurilor digitale de către furnizorii terți de servicii TIC, AES ar trebui încurajate să încheie acorduri de cooperare cu autoritățile relevante de supraveghere și de reglementare din țări terțe.

(95) Pentru a valorifica competențele, aptitudinile tehnice și expertiza specifice ale personalului specializat în riscurile operaționale și cele legate de TIC din cadrul autorităților competente, din cadrul celor trei AES și, în mod voluntar, din cadrul autorităților competente în temeiul Directivei (UE) 2022/2555, supraveghetorul principal ar trebui să se bazeze pe capacitățile și cunoștințele naționale de supraveghere și să înființeze echipe specializate de examinare pentru fiecare furnizor terț esențial de servicii TIC, reunind echipe multidisciplinare în sprijinul pregătirii și executării activităților de supraveghere, inclusiv al investigațiilor și inspecțiilor generale ale furnizorilor terți esențiali de servicii TIC, precum și pentru orice acțiuni ulterioare necesare în acest sens.

(96) Deși costurile care rezultă din sarcinile de supraveghere ar urma să fie finanțate integral din taxele percepute furnizorilor terți esențiali de servicii TIC, este totuși probabil ca AES să suporte, înainte de începerea cadrului de supraveghere, costuri pentru punerea în aplicare a unor sisteme TIC specifice care să sprijine supravegherea viitoare, deoarece sistemele TIC specifice ar trebui să fie dezvoltate și implementate în prealabil. Prin urmare, prezentul regulament prevede un model de finanțare hibrid, prin care cadrul de supraveghere ar fi, ca atare, finanțat integral din taxe, în timp ce dezvoltarea sistemelor TIC ale AES ar fi finanțată din contribuțiile Uniunii și ale autorităților naționale competente.

(97) Autoritățile competente ar trebui să dispună de toate competențele de supraveghere, de investigare și de sancționare necesare pentru a asigura exercitarea corespunzătoare a atribuțiilor care le revin în temeiul prezentului regulament. Acestea ar trebui, în principiu, să publice anunțuri privind sancțiunile administrative pe care le impun. Întrucât entitățile financiare și furnizorii terți de servicii TIC pot fi stabiliți în state membre diferite și pot fi supravegheați de autorități competente diferite, aplicarea prezentului regulament ar trebui să fie facilitată, pe de o parte, printr-o cooperare strânsă între autoritățile competente relevante, inclusiv BCE în ceea ce privește atribuțiile specifice care îi sunt conferite prin Regulamentul (UE) nr. 1024/2013 al Consiliului și, pe de altă parte, prin consultarea cu AES prin intermediul schimbului reciproc de informații și prin furnizarea de asistență în contextul activităților de supraveghere relevante.

(98) Pentru a cuantifica și a califica suplimentar criteriile pentru desemnarea furnizorilor terți de servicii TIC ca fiind esențiali și pentru a armoniza taxele de supraveghere, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei pentru a completa prezentul regulament, pentru a preciza mai în detaliu impactul sistemic pe care l-ar putea avea o defecțiune sau o întrerupere operațională a unui furnizor terț de servicii TIC asupra entităților financiare cărora le furnizează servicii TIC, numărul de instituții globale de importanță sistemică (G-SII) sau de alte instituții de importanță sistemică (O-SII), care se bazează pe furnizorul terț de servicii TIC în cauză, numărul furnizorilor terți de servicii TIC activi pe o anumită piață, costurile aferente migrării datelor și sarcinilor TIC către alți furnizori terți de servicii TIC, precum și cuantumul taxelor de supraveghere și modul în care acestea trebuie plătite. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([22]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul ar trebui să primească toate documentele în același timp cu experții din statele membre, iar experții acestor instituții ar trebui să aibă acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(99) Standardele tehnice de reglementare ar trebui să asigure armonizarea consecventă a cerințelor prevăzute în prezentul regulament. În rolurile lor de organisme care dispun de o expertiză foarte specializată, AES ar trebui să elaboreze proiecte de standarde tehnice de reglementare care nu implică opțiuni de politică, pe care să le prezinte Comisiei. Ar trebui elaborate standarde tehnice de reglementare în domeniul gestionării riscurilor TIC, al raportării incidentelor majore legate de TIC, al testării, precum și în ceea ce privește cerințele-cheie pentru o monitorizare riguroasă a riscurilor TIC generate de părți terțe. Comisia și AES ar trebui să se asigure că standardele și cerințele respective pot fi aplicate de toate entitățile financiare într-un mod proporțional cu dimensiunea și profilul lor general de risc, precum și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor. Comisia ar trebui să fie împuternicită să adopte aceste standarde tehnice de reglementare prin intermediul unor acte delegate în temeiul articolului 290 din TFUE și al articolelor 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

(100) Pentru a facilita comparabilitatea rapoartelor privind incidentele majore legate de TIC și incidentele operaționale sau de securitate majore legate de plăți, precum și pentru a asigura transparența cu privire la acordurile contractuale pentru utilizarea serviciilor TIC furnizate de furnizorii terți de servicii TIC, AES ar trebui să elaboreze proiecte de standarde tehnice de punere în aplicare care să stabilească modele, formulare și proceduri standardizate prin care entitățile financiare să raporteze un incident major legat de TIC și un incident operațional sau de securitate major legat de plăți, precum și modele standardizate pentru înregistrarea informațiilor. Atunci când elaborează standardele respective, AES ar trebui să ia în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale. Comisia ar trebui să fie împuternicită să adopte standardele tehnice de punere în aplicare respective prin intermediul unor acte de punere în aplicare, în temeiul articolului 291 din TFUE și în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

([22]) JO L 123, 12.5.2016, p. 1.

(101) Întrucât au fost deja specificate cerințe suplimentare prin intermediul actelor delegate și al actelor de punere în aplicare, pe baza standardelor tehnice de reglementare și de punere în aplicare din Regulamentele (CE) nr. 1060/2009 ([23]), (UE) nr. 648/2012 ([24]), (UE) nr. 600/2014 ([25]) și (UE) nr. 909/2014 ([26]) ale Parlamentului European și ale Consiliului, este adecvat ca AES să fie mandatate, fie individual, fie în comun, prin intermediul Comitetului comun, să prezinte Comisiei standarde tehnice de reglementare și de punere în aplicare pentru adoptarea actelor delegate și de punere în aplicare care preiau și actualizează normele existente privind gestionarea riscurilor TIC.

(102) Întrucât prezentul regulament, împreună cu Directiva (UE) 2022/2556 a Parlamentului European și a Consiliului ([27]), implică o consolidare a dispozițiilor privind gestionarea riscurilor TIC din mai multe regulamente și directive din acquis-ul Uniunii privind serviciile financiare, inclusiv Regulamentele (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014 și Regulamentul (UE) 2016/1011 al Parlamentului European și al Consiliului ([28]), pentru a se asigura coerența deplină, regulamentele respective ar trebui să fie modificate pentru a clarifica faptul că dispozițiile aplicabile legate de riscurile TIC sunt prevăzute în prezentul regulament.

(103) În consecință, domeniul de aplicare al articolelor relevante referitoare la riscul operațional, pe baza cărora delegările de competențe prevăzute în Regulamentele (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 au prevăzut adoptarea de acte delegate și de punere în aplicare, ar trebui să fie restrâns în vederea transferării în prezentul regulament a tuturor dispozițiilor care acoperă aspectele legate de reziliența operațională digitală care fac parte în prezent din regulamentele respective.

(104) Riscul cibernetic sistemic potențial asociat cu utilizarea infrastructurilor TIC care permit operarea sistemelor de plată și furnizarea de activități de prelucrare a plăților ar trebui să fie abordat în mod corespunzător la nivelul Uniunii prin norme armonizate în materie de reziliență digitală. În acest scop, Comisia ar trebui să evalueze rapid necesitatea revizuirii domeniului de aplicare al prezentului regulament, aliniind în același timp această revizuire la rezultatul revizuirii cuprinzătoare prevăzute în Directiva (UE) 2015/2366. Numeroasele atacuri la scară largă din ultimul deceniu demonstrează măsura în care sistemele de plată au ajuns să fie expuse în fața amenințările cibernetice. Plasate în centrul lanțului de servicii de plată și prezentând interconexiuni puternice cu sistemul financiar general, sistemele de plată și activitățile de procesare a plăților au dobândit o importanță critică pentru funcționarea piețelor financiare ale Uniunii. Atacurile cibernetice asupra unor astfel de sisteme pot provoca perturbări operaționale grave ale activității, cu repercusiuni directe asupra funcțiilor economice esențiale, cum ar fi facilitarea plăților, și efecte indirecte asupra proceselor economice conexe. Până la instituirea la nivelul Uniunii a unui regim armonizat și a supravegherii operatorilor de sisteme de plată și a entităților de prelucrare, statele membre pot, în vederea aplicării unor practici de piață similare, să se inspire din cerințele privind reziliența operațională digitală prevăzute în prezentul regulament, atunci când aplică norme operatorilor de sisteme de plată și entităților de prelucrare supravegheate în jurisdicțiile lor.

([23]) Regulamentul (CE) nr. 1060/2009 al Parlamentului European și al Consiliului din 16 septembrie 2009 privind agențiile de rating de credit (JO L 302, 17.11.2009, p. 1).

([24]) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1).

([25]) Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 173, 12.6.2014, p. 84).

([26]) Regulamentul (UE) nr. 909/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind îmbunătățirea decontării titlurilor de valoare în Uniunea Europeană și privind depozitarii centrali de titluri de valoare și de modificare a Directivelor 98/26/CE și 2014/65/UE și a Regulamentului (UE) nr. 236/2012 (JO L 257, 28.8.2014, p. 1).

([27]) Directiva (UE) 2022/2556 a Parlamentului European și a Consiliului din 14 decembrie 2022 de modificare a Directivelor 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341 în ceea ce privește reziliența operațională digitală pentru sectorul financiar (a se vedea pagina 153 din prezentul Jurnal Oficial).

([28]) Regulamentul (UE) 2016/1011 al Parlamentului European și al Consiliului din 8 iunie 2016 privind indicii utilizați ca indici de referință în cadrul instrumentelor financiare și al contractelor financiare sau pentru a măsura performanțele fondurilor de investiții și de modificare a Directivelor 2008/48/CE și 2014/17/UE și a Regulamentului (UE) nr. 596/2014 (JO L 171, 29.6.2016, p. 1).

(105) Întrucât obiectivul prezentului regulament, și anume atingerea unui nivel ridicat de reziliență operațională digitală pentru entitățile financiare reglementate, nu poate fi realizat în mod satisfăcător de către statele membre deoarece necesită armonizarea diferitelor norme din dreptul Uniunii și din dreptul intern, dar, având în vedere amploarea și efectele sale, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv.

(106) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([29]) și a emis un aviz la 10 mai 2021 ([30]),

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

Dispoziții generale

Articolul 1

Obiectul

(1) Pentru a atinge un nivel comun ridicat de reziliență operațională digitală, prezentul regulament stabilește cerințe uniforme privind securitatea rețelelor și a sistemelor informatice care sprijină procesele operaționale ale entităților financiare, după cum urmează:

(a) cerințe aplicabile entităților financiare în legătură cu:

(i) gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC);

(ii) raportarea incidentelor majore legate de TIC și notificarea, în mod voluntar, a amenințărilor cibernetice semnificative către autoritățile competente;

(iii) raportarea de către entitățile financiare menționate la articolul 2 alineatul (1) literele (a)-(d) către autoritățile competente a incidentelor operaționale sau de securitate majore legate de plăți;

(iv) testarea rezilienței operaționale digitale;

(v) schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități;

(vi) măsuri pentru buna gestionare a riscurilor TIC generate de părți terțe;

(b) cerințe în legătură cu acordurile contractuale încheiate între furnizorii terți de servicii TIC și entitățile financiare;

(c) reguli privind instituirea și desfășurarea cadrului de supraveghere pentru furnizorii terți esențiali de servicii TIC, atunci când furnizează servicii entităților financiare;

(d) reguli privind cooperarea între autoritățile competente și norme privind supravegherea și asigurarea conformității de către autoritățile competente în legătură cu toate aspectele vizate de prezentul regulament.

(2) În ceea ce privește entitățile financiare identificate drept entități esențiale sau importante în temeiul normelor naționale care transpun articolul 3 din Directiva (UE) 2022/2555, prezentul regulament este considerat un act juridic sectorial al Uniunii în sensul articolului 4 din directiva respectivă.

(3) Prezentul regulament nu aduce atingere responsabilității statelor membre în ceea ce privește funcțiile esențiale ale statului cu privire la siguranța publică, apărarea și securitatea națională, în conformitate cu dreptul Uniunii.

([29]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

([30]) JO C 229, 15.6.2021, p. 16.

Articolul 2

Domeniul de aplicare

(1) Fără a aduce atingere alineatelor (3) și (4), prezentul regulament se aplică următoarelor entități:

(a) instituțiile de credit;

(b) instituțiile de plată, inclusiv instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366;

(c) prestatorii de servicii de informare cu privire la conturi;

(d) instituțiile emitente de monedă electronică, inclusiv instituțiile emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE;

(e) firmele de investiții;

(f) prestatorii de servicii de criptoactive autorizați în temeiul unui regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937 (denumit în continuare „Regulamentul privind piețele criptoactivelor") și emitenții de tokenuri raportate la active;

(g) depozitarii centrali de titluri de valoare;

(h) contrapărțile centrale;

(i) locurile de tranzacționare;

(j) registrele centrale de tranzacții;

(k) administratorii de fonduri de investiții alternative;

(l) societățile de administrare;

(m) furnizorii de servicii de raportare a datelor;

(n) întreprinderile de asigurare și de reasigurare;

(o) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare;

(p) instituțiile pentru furnizarea de pensii ocupaționale;

(q) agențiile de rating de credit;

(r) administratorii de indici de referință critici;

(s) furnizorii de servicii de finanțare participativă;

(t) registrele centrale de securitizări;

(u) furnizorii terți de servicii TIC.

(2) În sensul prezentului regulament, entitățile menționate la alineatul (1) literele (a)-(t) sunt denumite colectiv „entități financiare".

(3) Prezentul regulament nu se aplică următoarelor entități:

(a) administratorii de fonduri de investiții alternative, astfel cum sunt menționați la articolul 3 alineatul (2) din Directiva 2011/61/UE;

(b) întreprinderile de asigurare și de reasigurare, astfel cum sunt menționate la articolul 4 din Directiva 2009/138/CE;

(c) instituțiile pentru furnizarea de pensii ocupaționale care gestionează sisteme de pensii care împreună nu au mai mult de 15 membri în total;

(d) persoanele fizice sau juridice exceptate în temeiul articolelor 2 și 3 din Directiva 2014/65/UE;

(e) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare care sunt microîntreprinderi sau întreprinderi mici sau mijlocii;

(f) oficiile poștale care efectuează operațiuni de virament, astfel cum sunt menționate la articolul 2 alineatul (5) punctul 3 din Directiva 2013/36/UE.

(4) Statele membre pot exclude din domeniul de aplicare al prezentului regulament entitățile menționate la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE care sunt situate pe teritoriile lor. În cazul în care un stat membru face uz de această opțiune, acesta informează Comisia cu privire la aceasta, precum și cu privire la orice modificare ulterioară. Comisia pune aceste informații la dispoziția publicului pe site-ul său sau prin alte mijloace ușor accesibile.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „reziliență operațională digitală” înseamnă capacitatea unei entități financiare de a construi, a asigura și a reevalua integritatea și fiabilitatea sa operațională, prin asigurarea, în mod direct sau indirect, utilizând servicii oferite de furnizori terți de servicii TIC, a întregii game de capacități legate de TIC care sunt necesare pentru a aborda securitatea rețelelor și a sistemelor informatice utilizate de o entitate financiară și care sprijină furnizarea continuă de servicii financiare și calitatea acestora, inclusiv pe întreaga durată a perturbărilor;

2. „rețea și sistem informatic” înseamnă rețea și sistem informatic astfel cum sunt definite la articolul 6 punctul 1 din Directiva (UE) 2022/2555;

3. „sistem TIC moștenit” înseamnă un sistem TIC ajuns la sfârșitul ciclului său de viață care nu este adecvat pentru a fi modernizat sau reparat, din motive tehnologice sau comerciale, sau pentru care furnizorul său ori un furnizor terț de servicii TIC nu mai oferă asistență, dar care încă este în uz și sprijină funcțiile entității financiare;

4. „securitatea rețelelor și a sistemelor informatice” înseamnă securitatea rețelelor și a sistemelor informatice astfel cum sunt definite la articolul 6 punctul 2 din Directiva (UE) 2022/2555;

5. „risc TIC” înseamnă orice circumstanță care poate fi identificată în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice care, dacă se materializează, poate compromite securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operațiilor și a proceselor sau a furnizării serviciilor prin crearea de efecte negative în mediul digital sau fizic;

6. „activ informațional” înseamnă o colecție de informații, materială sau imaterială, care merită protejată;

7. „activ TIC” înseamnă un activ software sau hardware din rețelele și sistemele informatice utilizate de entitatea financiară;

8. „incident legat de TIC” înseamnă un eveniment unic sau o serie de evenimente conexe neplanificate de entitatea financiară care compromit securitatea rețelelor și a sistemelor informatice și care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor sau asupra serviciilor furnizate de entitatea financiară;

9. „incident operațional sau de securitate legat de plăți” înseamnă un eveniment unic sau o serie de evenimente conexe neplanificate de entitățile financiare menționate la articolul 2 alineatul (1) literele (a)-(d), legate sau nu de TIC, care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor legate de plăți sau asupra serviciilor legate de plăți furnizate de entitatea financiară;

10. „incident major legat de TIC” înseamnă un incident legat de TIC care are un impact negativ puternic asupra rețelelor și sistemelor informatice care sprijină funcțiile critice sau importante ale entității financiare;

11. „incident major operațional sau de securitate legat de plăți” înseamnă un incident operațional sau de securitate legat de plăți care are un efect negativ puternic asupra serviciilor legate de plăți furnizate;

12. „amenințare cibernetică” înseamnă amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

13. „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică ale cărei caracteristici tehnice indică faptul că ar putea avea ca rezultat un incident major legat de TIC sau un incident major operațional sau de securitate legat de plăți;

14. „atac cibernetic” înseamnă un incident rău-intenționat legat de TIC, cauzat prin intermediul unei tentative comise de un factor perturbator care generează amenințări de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține acces neautorizat la un activ ori a utiliza în mod neautorizat un activ;

15. „date operative privind amenințările” înseamnă informații care au fost agregate, transformate, analizate, interpretate sau îmbogățite pentru a oferi contextul necesar procesului decizional și pentru a face posibilă o înțelegere adecvată și suficientă cu scopul de a atenua impactul unui incident legat de TIC sau al unei amenințări cibernetice, inclusiv detaliile tehnice ale unui atac cibernetic, persoanele responsabile de atac, modul de operare și motivațiile acestora;

16. „vulnerabilitate” înseamnă un punct slab, o sensibilitate sau un defect al unui activ, sistem, proces sau control care poate fi exploatat;

17. „teste de penetrare bazate pe amenințări (TLPT)” înseamnă un cadru care imită tacticile, tehnicile și procedurile utilizate de actorii din viața reală care generează amenințări, percepute ca reprezentând o amenințare cibernetică autentică, și care asigură o testare controlată, personalizată, bazată pe date operative (de tipul „echipa roșie”) a sistemelor critice de producție în timp real ale entității financiare;

18. „risc TIC generat de părți terțe” înseamnă un risc TIC care poate apărea pentru o entitate financiară în legătură cu utilizarea, de către aceasta, a serviciilor TIC oferite de furnizori terți de servicii TIC sau de subcontractanți ai acestora din urmă, inclusiv prin acorduri de externalizare;

19. „furnizor terț de servicii TIC” înseamnă o întreprindere care furnizează servicii TIC;

20. „furnizor de servicii TIC intragrup” înseamnă o întreprindere care face parte dintr-un grup financiar și care oferă servicii predominant TIC exclusiv entităților financiare din același grup ori entităților financiare care țin de același sistem instituțional de protecție, inclusiv societăților-mamă ale acestora, filialelor și sucursalelor sau altor entități care sunt în proprietate comună ori sub control comun;

21. „servicii TIC” înseamnă servicii digitale și de date furnizate prin intermediul sistemelor TIC către unul sau mai mulți utilizatori interni sau externi în mod continuu, inclusiv hardware ca serviciu și servicii hardware, care includ furnizarea de asistență tehnică prin actualizări de software sau firmware din partea furnizorului de hardware, cu excepția serviciilor de telefonie analogică tradiționale;

22. „funcție critică sau importantă” înseamnă o funcție a cărei întrerupere ar afecta în mod semnificativ performanța financiară a unei entități financiare sau soliditatea ori continuitatea serviciilor și activităților sale sau a cărei întrerupere, deficiență sau eșuare în executare ar afecta în mod semnificativ respectarea în continuare, de către o entitate financiară, a condițiilor și obligațiilor aferente autorizației sale sau a altor obligații care îi revin în temeiul dreptului aplicabil în domeniul serviciilor financiare;

23. „furnizor terț esențial de servicii TIC” înseamnă un furnizor terț de servicii TIC desemnat drept esențial în conformitate cu articolul 31;

24. „furnizor terț de servicii TIC stabilit într-o țară terță” înseamnă un furnizor terț de servicii TIC care este o persoană juridică stabilită într-o țară terță și care a încheiat un acord contractual cu o entitate financiară pentru furnizarea de servicii TIC;

25. „filială” înseamnă o filială în sensul articolului 2 punctul 10 și al articolului 22 din Directiva 2013/34/UE;

26. „grup” înseamnă un grup în sensul articolului 2 punctul 11 din Directiva 2013/34/UE;

27. „societate-mamă” înseamnă o societate-mamă în sensul articolului 2 punctul 9 și al articolului 22 din Directiva 2013/34/UE;

28. „subcontractant TIC stabilit într-o țară terță” înseamnă un subcontractant TIC care este o persoană juridică stabilită într-o țară terță și care a încheiat un acord contractual fie cu un furnizor terț de servicii TIC, fie cu un furnizor terț de servicii TIC stabilit într-o țară terță;

29. „risc de concentrare a serviciilor TIC” înseamnă o expunere la furnizori terți esențiali de servicii TIC individuali sau multipli relaționați, care creează un grad de dependență față de astfel de furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficiență a acestor furnizori poate pune în pericol capacitatea unei entități financiare de a oferi funcții critice sau importante ori ar putea genera alte tipuri de efecte negative pentru aceasta, inclusiv pierderi mari sau poate pune în pericol stabilitatea financiară a Uniunii în ansamblu;

30. „organ de conducere” înseamnă un organ de conducere astfel cum este definit la articolul 4 alineatul (1) punctul 36 din Directiva 2014/65/UE, la articolul 3 alineatul (1) punctul 7 din Directiva 2013/36/UE, la articolul 2 alineatul (1) litera (s) din Directiva 2009/65/CE a Parlamentului European și al Consiliului ([31]), la articolul 2 alineatul (1) punctul 45 din Regulamentul (UE) nr. 909/2014, la articolul 3 alineatul (1) punctul 20 din Regulamentul (UE) 2016/1011 și în dispozițiile relevante din Regulamentul privind piețele criptoactivelor, sau persoanele echivalente care conduc efectiv entitatea sau dețin funcții-cheie în conformitate cu dreptul Uniunii sau cu dreptul intern relevant;

31. „instituție de credit” înseamnă o instituție de credit astfel cum este definită la articolul 4 alineatul (1) punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului ([32]);

32. „instituție de credit exceptată în temeiul Directivei 2013/36/UE” înseamnă o entitate astfel cum este menționată la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE;

33. „firmă de investiții” înseamnă o firmă de investiții astfel cum este definită la articolul 4 alineatul (1) punctul 1 din Directiva 2014/65/UE;

34. „firmă de investiții mică și neinterconectată” înseamnă o firmă de investiții care îndeplinește condițiile prevăzute la articolul 12 alineatul (1) din Regulamentul (UE) 2019/2033 al Parlamentului European și al Consiliului ([33]);

35. „instituție de plată” înseamnă o instituție de plată astfel cum este definită la articolul 4 punctul 4 din Directiva (UE) 2015/2366;

36. „instituție de plată exceptată în temeiul Directivei (UE) 2015/2366” înseamnă o instituție de plată exceptată în temeiul articolului 32 alineatul (1) din Directiva (UE) 2015/2366;

37. „prestator de servicii de informare cu privire la conturi” înseamnă un prestator de servicii de informare cu privire la conturi astfel cum este menționat la articolul 33 alineatul (1) din Directiva (UE) 2015/2366;

38. „instituție emitentă de monedă electronică” înseamnă o instituție emitentă de monedă electronică astfel cum este definită la articolul 2 punctul 1 din Directiva 2009/110/CE;

39. „instituție emitentă de monedă electronică exceptată în temeiul Directivei 2009/110/CE” înseamnă o instituție emitentă de monedă electronică care beneficiază de o exceptare astfel cum se menționează la articolul 9 alineatul (1) din Directiva 2009/110/CE;

40. „contraparte centrală” înseamnă o contraparte centrală astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012;

41. „registru central de tranzacții” înseamnă un registru central de tranzacții astfel cum este definit la articolul 2 punctul 2 din Regulamentul (UE) nr. 648/2012;

42. „depozitar central de titluri de valoare” înseamnă un depozitar central de titluri de valoare astfel cum este definit la articolul 2 alineatul (1) punctul 1 din Regulamentul (UE) nr. 909/2014;

43. „loc de tranzacționare” înseamnă un loc de tranzacționare astfel cum este definit la articolul 4 alineatul (1) punctul 24 din Directiva 2014/65/UE;

44. „administrator de fonduri de investiții alternative” înseamnă un administrator de fonduri de investiții alternative astfel cum este definit la articolul 4 alineatul (1) litera (b) din Directiva 2011/61/UE;

45. „societate de administrare” înseamnă o societate de administrare astfel cum este definită la articolul 2 alineatul (1) litera (b) din Directiva 2009/65/CE;

46. „furnizor de servicii de raportare a datelor” înseamnă un furnizor de servicii de raportare a datelor în sensul Regulamentului (UE) nr. 600/2014, astfel cum se menționează la articolul 2 alineatul (1) punctele 34-36;

47. „întreprindere de asigurare” înseamnă o întreprindere de asigurare astfel cum este definită la articolul 13 punctul 1 din Directiva 2009/138/CE;

48. „întreprindere de reasigurare” înseamnă o întreprindere de reasigurare astfel cum este definită la articolul 13 punctul 4 din Directiva 2009/138/CE;

([31]) Directiva 2009/65/CE a Parlamentului European și a Consiliului din 13 iulie 2009 de coordonare a actelor cu putere de lege și a actelor administrative privind organismele de plasament colectiv în valori mobiliare (OPCVM) (JO L 302, 17.11.2009, p. 32).

([32]) Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

([33]) Regulamentul (UE) 2019/2033 al Parlamentului European și al Consiliului din 27 noiembrie 2019 privind cerințele prudențiale ale firmelor de investiții și de modificare a Regulamentelor (UE) nr. 1093/2010, (UE) nr. 575/2013, (UE) nr. 600/2014 și (UE) nr. 806/2014 (JO L 314, 5.12.2019, p. 1).

49. „intermediar de asigurări” înseamnă un intermediar de asigurări astfel cum este definit la articolul 2 alineatul (1) punctul 3 din Directiva (UE) 2016/97 a Parlamentului European și a Consiliului ([34]);

50. „intermediar de asigurări auxiliare” înseamnă un intermediar de asigurări auxiliare astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva (UE) 2016/97;

51. „intermediar de reasigurări” înseamnă un intermediar de reasigurări astfel cum este definit la articolul 2 alineatul (1) punctul 5 din Directiva (UE) 2016/97;

52. „instituție pentru furnizarea de pensii ocupaționale” înseamnă o instituție pentru furnizarea de pensii ocupaționale astfel cum este definită la articolul 6 punctul 1 din Directiva (UE) 2016/2341;

53. „instituție mică pentru furnizarea de pensii ocupaționale” înseamnă o instituție pentru furnizarea de pensii ocupaționale care gestionează scheme de pensii care împreună au mai puțin de 100 de membri în total;

54. „agenție de rating de credit” înseamnă o agenție de rating de credit astfel cum este definită la articolul 3 alineatul (1) litera (b) din Regulamentul (CE) nr. 1060/2009;

55. „furnizor de servicii de criptoactive” înseamnă un furnizor de servicii de criptoactive astfel cum este definit în dispozițiile relevante din Regulamentul privind piețele criptoactivelor;

56. „emitent de tokenuri raportate la active” înseamnă un emitent de tokenuri raportate la active astfel cum sunt definite în dispozițiile relevante din Regulamentul privind piețele criptoactivelor;

57. „administrator de indici de referință critici” înseamnă un administrator de indici de referință critici astfel cum sunt definiți la articolul 3 alineatul (1) punctul 25 din Regulamentul (UE) 2016/1011;

58. „furnizor de servicii de finanțare participativă” înseamnă un furnizor de servicii de finanțare participativă astfel cum este definit la articolul 2 alineatul (1) litera (e) din Regulamentul (UE) 2020/1503 al Parlamentului European și al Consiliului ([35]);

59. „registru central de securitizări” înseamnă un registru central de securitizări astfel cum este definit la articolul 2 punctul 23 din Regulamentul (UE) 2017/2402 al Parlamentului European și al Consiliului ([36]);

60. „microîntreprindere” înseamnă o entitate financiară, alta decât un loc de tranzacționare, o contraparte centrală, un registru central de tranzacții sau un depozitar central de titluri de valoare, care are mai puțin de 10 angajați și o cifră de afaceri anuală și/sau un bilanț anual total care nu depășește 2 milioane EUR;

61. „supraveghetor principal” înseamnă autoritatea europeană de supraveghere desemnată în conformitate cu articolul 31 alineatul (1) litera (b) din prezentul regulament;

62. „Comitetul comun” înseamnă comitetul menționat la articolul 54 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010;

63. „întreprindere mică” înseamnă o entitate financiară care are cel puțin 10 angajați, dar mai puțin de 50 de angajați, și o cifră de afaceri anuală și/sau un bilanț anual total care depășește 2 milioane EUR, dar nu depășește 10 milioane EUR;

64. „întreprindere mijlocie” înseamnă o entitate financiară care nu este o întreprindere mică și care are mai puțin de 250 de angajați și o cifră de afaceri anuală care nu depășește 50 de milioane EUR și/sau un bilanț anual care nu depășește 43 de milioane EUR;

65. „autoritate publică” înseamnă orice entitate guvernamentală sau altă entitate a administrației publice, inclusiv băncile centrale naționale.

([34]) Directiva (UE) 2016/97 a Parlamentului European și a Consiliului din 20 ianuarie 2016 privind distribuția de asigurări (JO L 26, 2.2.2016, p. 19).

([35]) Regulamentul (UE) 2020/1503 al Parlamentului European și al Consiliului din 7 octombrie 2020 privind furnizorii europeni de servicii de finanțare participativă pentru afaceri și de modificare a Regulamentului (UE) 2017/1129 și a Directivei (UE) 2019/1937 (JO L 347, 20.10.2020, p. 1).

([36]) Regulamentul (UE) 2017/2402 al Parlamentului European și al Consiliului din 12 decembrie 2017 de stabilire a unui cadru general privind securitizarea și de creare a unui cadru specific pentru o securitizare simplă, transparentă și standardizată, și de modificare a Directivelor 2009/65/CE, 2009/138/CE și 2011/61/UE, precum și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 648/2012 (JO L 347, 28.12.2017, p. 35).

Articolul 4

Principiul proporționalității

(1) Entitățile financiare pun în aplicare normele prevăzute la capitolul II în conformitate cu principiul proporționalității, luând în considerare dimensiunea și profilul lor general de risc și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor.

(2) În plus, entitățile financiare aplică capitolele III și IV și capitolul V secțiunea I proporțional cu dimensiunea și profilul lor general de risc și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, astfel cum se prevede în mod specific în normele relevante din capitolele respective.

(3) Autoritățile competente iau în considerare aplicarea principiului proporționalității de către entitățile financiare atunci când revizuiesc coerența cadrului de gestionare a riscurilor TIC pe baza rapoartelor prezentate la cererea autorităților competente în temeiul articolului 6 alineatul (5) și al articolului 16 alineatul (2).

CAPITOLUL II

Gestionarea riscurilor TIC

Secțiunea I

Articolul 5

Guvernanță și organizare

(1) Entitățile financiare dispun de un cadru intern de guvernanță și control care asigură o gestionare eficace și prudentă a riscurilor TIC, în conformitate cu articolul 6 alineatul (4), cu scopul de a obține un nivel ridicat de reziliență operațională digitală.

(2) Organul de conducere al entității financiare definește, aprobă, supraveghează și este responsabil de punerea în aplicare a tuturor dispozițiilor legate de cadrul de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1).

În scopul aplicării primului paragraf, organul de conducere:

(a) poartă responsabilitatea finală pentru gestionarea riscurilor TIC ale entității financiare;

(b) stabilește politici menite să asigure menținerea unor standarde ridicate de disponibilitate, autenticitate, integritate și confidențialitate a datelor;

(c) stabilește roluri și responsabilități clare pentru toate funcțiile legate de TIC și instituie mecanisme de guvernanță adecvate pentru a asigura comunicarea, cooperarea și coordonarea eficace și în timp util între aceste funcții;

(d) poartă responsabilitatea generală pentru stabilirea și aprobarea strategiei privind reziliența operațională digitală, astfel cum este menționată la articolul 6 alineatul (8), inclusiv pentru determinarea nivelul adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare, astfel cum este menționată la articolul 6 alineatul (8) litera (b);

(e) aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC ale entității financiare, menționate la articolul 11 alineatul (1) și, respectiv, alineatul (3), care pot fi adoptate sub forma unei politici specifice dedicate care să facă parte integrantă din politica generală de continuitate a activității și planul general de răspuns și de recuperare ale entității financiare;

(f) aprobă și verifică periodic planurile de audit intern TIC și auditurile TIC ale entității financiare, precum și modificările semnificative aduse acestora;

(g) alocă și verifică periodic bugetul adecvat pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare în ceea ce privește toate tipurile de resurse, inclusiv programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante menționate la articolul 13 alineatul (6), precum și competențe TIC pentru toți membrii personalului;

(h) aprobă și verifică periodic politica entității financiare cu privire la acordurile privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC;

(i) instituie, la nivel corporativ, canale de raportare care să îi permită să fie informat în mod corespunzător cu privire la:

(i) acordurile încheiate cu furnizorii terți de servicii TIC privind utilizarea serviciilor TIC;

(ii) orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC;

(iii) impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acordurilor respective, inclusiv un rezumat al analizei de risc pentru a evalua impactul modificărilor respective, și cel puțin incidentele majore legate de TIC și impactul acestora, precum și cu privire la măsurile de răspuns, de recuperare și corective.

(3) Entitățile financiare, altele decât microîntreprinderile, stabilesc un rol pentru a monitoriza acordurile încheiate cu furnizorii terți de servicii TIC cu privire la utilizarea serviciilor TIC sau desemnează un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante.

(4) Membrii organului de conducere al entității financiare își actualizează în mod activ cunoștințele și competențele pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, inclusiv prin frecventarea cu regularitate a unor cursuri de formare specifice, pe măsura riscurilor TIC gestionate.

Secțiunea II

Articolul 6

Cadrul de gestionare a riscurilor TIC

(1) Entitățile financiare dispun de un cadru solid, cuprinzător și bine documentat de gestionare a riscurilor TIC, ca parte a sistemului lor general de gestionare a riscurilor, care le permite să abordeze riscurile TIC în mod rapid, eficient și cuprinzător și să asigure un nivel ridicat de reziliență operațională digitală.

(2) Cadrul de gestionare a riscurilor TIC include cel puțin strategii, politici, proceduri, precum și protocoale și instrumente TIC care sunt necesare pentru a proteja în mod corespunzător și adecvat toate activele informaționale și toate activele TIC, inclusiv software pentru calculatoare, hardware și servere, precum și pentru a proteja toate componentele și infrastructurile fizice relevante, precum sediile, centrele de date și zonele desemnate sensibile, pentru a asigura că toate activele informaționale și toate activele TIC sunt protejate în mod adecvat împotriva riscurilor, inclusiv împotriva pagubelor și a accesului sau utilizării neautorizate.

(3) În conformitate cu cadrul lor de gestionare a riscurilor TIC, entitățile financiare reduc la minimum impactul riscurilor TIC prin utilizarea unor strategii, politici, proceduri, protocoale și instrumente TIC adecvate. Acestea furnizează autorităților competente, la cererea acestora, informații complete și actualizate cu privire la riscurile TIC și la cadrul lor de gestionare a riscurilor TIC.

(4) Entitățile financiare, altele decât microîntreprinderile, atribuie responsabilitatea pentru gestionarea și supravegherea riscurilor TIC unei funcții de control și asigură independența acestei funcții de control la un nivel adecvat, pentru a evita conflictele de interese. Entitățile financiare asigură în mod adecvat separarea și independența a funcțiilor de gestionare a riscurilor TIC, a funcțiilor de control și a funcțiilor de audit intern, în conformitate cu cele trei linii ale modelului de apărare sau cu un model intern de gestionare și control al riscurilor.

(5) Cadrul de gestionare a riscurilor TIC se documentează și se revizuiește cel puțin o dată pe an, sau periodic în cazul microîntreprinderilor, precum și în cazul unor incidente majore legate de TIC și în urma instrucțiunilor sau concluziilor în materie de supraveghere care decurg din testarea relevantă a rezilienței operaționale digitale sau din procesele de audit relevante. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării. Autorității competente i se prezintă, la cererea sa, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.

(6) Cadrul de gestionare a riscurilor TIC al entităților financiare, altele decât microîntreprinderile, este supus auditului intern de către auditori în mod regulat, în conformitate cu planul de audit al entităților financiare. Auditorii respectivi dețin suficiente cunoștințe, competențe și expertiză în ceea ce privește riscurile TIC, precum și o independență adecvată. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entităților financiare.

(7) Pe baza concluziilor evaluării de audit intern, entitățile financiare stabilesc un proces formal de urmărire, care include reguli pentru verificarea și remedierea în timp util a elementelor critice constatate în cadrul auditurilor TIC.

(8) Cadrul de gestionare a riscurilor TIC include o strategie privind reziliența operațională digitală, care stabilește modul de punere în aplicare a cadrului. În acest scop, strategia privind reziliența operațională digitală include metode de abordare a riscurilor TIC și de realizare a obiectivelor TIC specifice, prin:

(a) explicarea modului în care cadrul de gestionare a riscurilor TIC sprijină strategia de afaceri și obiectivele entității financiare;

(b) stabilirea nivelului de toleranță la risc pentru riscurile TIC, în conformitate cu apetitul pentru risc al entității financiare, și analizarea toleranței la impact pentru perturbările TIC;

(c) stabilirea unor obiective clare privind securitatea informațiilor, inclusiv indicatori-cheie de performanță și indicatori-cheie de risc;

(d) explicarea arhitecturii TIC de referință și a oricăror modificări necesare pentru atingerea obiectivelor specifice de activitate;

(e) prezentarea diferitelor mecanisme instituite pentru a detecta incidentele legate de TIC, a preveni impactul acestora și a asigura protecție împotriva acestora;

(f) evidențierea situației actuale a rezilienței operaționale digitale pe baza numărului de incidente majore legate de TIC raportate și a eficacității măsurilor preventive;

(g) implementarea testării rezilienței operaționale digitale, în conformitate cu capitolul IV din prezentul regulament;

(h) conturarea unei strategii de comunicare în cazul producerii unor incidente legate de TIC cu privire la care este necesară informarea în conformitate cu articolul 14.

(9) Entitățile financiare pot defini, în contextul strategiei privind reziliența operațională digitală menționate la alineatul (8), o strategie TIC cuprinzătoare privind existența mai multor furnizori, la nivel de grup sau de entitate, care să prezinte principalele dependențe față de furnizorii terți de servicii TIC și să explice raționamentul care stă la baza mixului de achiziții de la furnizori terți de servicii TIC.

(10) Entitățile financiare pot externaliza, în conformitate cu legislația sectorială a Uniunii și cea națională, sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către entități intragrup sau externe. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de verificarea conformității cu cerințele de gestionare a riscurilor TIC.

Articolul 7

Sisteme, protocoale și instrumente TIC

Pentru a aborda și a gestiona riscurile TIC, entitățile financiare utilizează și mențin sisteme, protocoale și instrumente TIC actualizate care sunt:

(a) adecvate magnitudinii operațiunilor care sprijină desfășurarea activităților lor, în conformitate cu principiul proporționalității astfel cum este menționat la articolul 4;

(b) fiabile;

(c) dotate cu suficientă capacitate de a prelucra cu precizie datele necesare pentru desfășurarea activităților și furnizarea serviciilor în timp util, precum și pentru a face față volumelor ridicate de ordine, mesaje sau tranzacții, după caz, inclusiv în cazul introducerii unor noi tehnologii;

(d) reziliente din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, calitate necesară în condiții de criză a pieței sau în alte situații adverse.

Articolul 8

Identificare

(1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare identifică, clasifică și documentează în mod corespunzător toate funcțiile operaționale și toate rolurile și responsabilitățile sprijinite de TIC, activele informaționale și activele TIC care sprijină funcțiile respective, precum și rolurile și dependențele lor în legătură cu riscurile TIC. Entitățile financiare revizuiesc după caz, dar cel puțin anual, caracterul adecvat al acestei clasificări și al oricărei documentări relevante.

(2) Entitățile financiare identifică în mod constant toate sursele de riscuri TIC, în special expunerea la riscuri față de alte entități financiare și din partea altor entități financiare, și evaluează amenințările cibernetice și vulnerabilitățile TIC relevante pentru funcțiile lor operaționale sprijinite de TIC, activele lor informaționale și activele lor TIC. Entitățile financiare revizuiesc în mod regulat și cel puțin o dată pe an scenariile de risc care au un impact asupra lor.

(3) Entitățile financiare, altele decât microîntreprinderile, efectuează o evaluare a riscurilor cu ocazia fiecărei modificări majore aduse infrastructurii rețelei și a sistemului informatic și proceselor sau procedurilor care le afectează funcțiile operaționale sprijinite de TIC, activele informaționale sau activele TIC.

(4) Entitățile financiare identifică toate activele informaționale și activele TIC, inclusiv cele din locații aflate la distanță, resursele de rețea și echipamentele hardware și le inventariază pe cele considerate esențiale. Acestea cartografiază configurația activelor informaționale și a activelor TIC și legăturile și interdependențele dintre diferitele active informaționale și active TIC.

(5) Entitățile financiare identifică și documentează toate procesele care depind de furnizori terți de servicii TIC și identifică interconexiunile cu furnizori terți de servicii TIC care oferă servicii care sprijină funcții critice sau importante.

(6) În scopul aplicării alineatelor (1), (4) și (5), entitățile financiare mențin inventarele relevante și le actualizează periodic și de fiecare dată când are loc orice modificare majoră, astfel cum este menționată la alineatul (3).

(7) Entitățile financiare, altele decât microîntreprinderile, efectuează periodic și cel puțin o dată pe an o evaluare specifică a riscurilor TIC vizând toate sistemele TIC moștenite și, în orice caz, înainte și după conectarea tehnologiilor, aplicațiilor sau sistemelor.

Articolul 9

Protecție și prevenire

(1) În scopul protejării adecvate a sistemelor TIC și în vederea organizării măsurilor de răspuns, entitățile financiare monitorizează și controlează în mod continuu securitatea și funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul riscurilor TIC asupra sistemelor TIC prin utilizarea unor instrumente, politici și proceduri de securitate TIC adecvate.

(2) Entitățile financiare concep, achiziționează și pun în aplicare politici, proceduri, protocoale și instrumente în domeniul securității TIC care vizează să asigure reziliența, continuitatea și disponibilitatea sistemelor TIC, în special pentru cele care sprijină funcții critice sau importante, precum și să mențină standarde înalte de disponibilitate, autenticitate, integritate și confidențialitate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.

(3) În vederea realizării obiectivelor menționate la alineatul (2), entitățile financiare utilizează soluții și procese TIC care sunt adecvate în conformitate cu articolul 4. Respectivele soluții și procese TIC:

(a) asigură securitatea mijloacelor de transfer al datelor;

(b) reduc la minimum riscul de corupere sau de pierdere a datelor, de acces neautorizat și de defecțiuni tehnice care pot împiedica derularea activităților;

(c) previn lipsa disponibilității, deteriorarea autenticității și a integrității, încălcarea confidențialității și pierderea datelor;

(d) asigură protecția datelor împotriva riscurilor care decurg din gestionarea datelor, inclusiv gestionarea deficitară, precum și împotriva riscurilor legate de prelucrare și a erorii umane.

(4) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare:

(a) elaborează și documentează o politică de securitate a informațiilor care definește norme de protecție a disponibilității, autenticității, integrității și confidențialității datelor, a activelor informaționale și a activelor TIC, inclusiv a celor ale clienților lor, după caz;

(b) stabilesc, urmând o abordare bazată pe riscuri, o structură de gestionare solidă a rețelei și a infrastructurii care utilizează tehnici, metode și protocoale adecvate ce pot include punerea în aplicare a unor mecanisme automatizate pentru a izola activele informaționale afectate în cazul unor atacuri cibernetice;

(c) pun în aplicare politici care limitează accesul fizic sau logic la activele informaționale și activele TIC la ceea ce este necesar exclusiv pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să vizeze drepturile de acces și o bună administrare a acestora;

(d) pun în aplicare politici și protocoale pentru mecanisme solide de autentificare, bazate pe standarde relevante și sisteme de control specifice, precum și măsuri de protecție a cheilor criptografice, prin care datele sunt criptate în funcție de rezultatele proceselor aprobate de clasificare a datelor și de evaluare a riscurilor TIC;

(e) pun în aplicare politici, proceduri și controale documentate pentru gestionarea modificărilor la nivelul TIC, inclusiv modificări la nivelul componentelor software, hardware, firmware, parametrii sistemelor sau de securitate, care sunt fondate pe o abordare bazată pe evaluarea riscurilor și fac parte integrantă din procesul general de gestionare a modificărilor din cadrul entității financiare, pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, puse în aplicare și verificate în mod controlat;

(f) dispun de politici documentate adecvate și cuprinzătoare pentru corecții și actualizări.

În scopul aplicării literei (b) de la primul paragraf, entitățile financiare concep infrastructura de conectare a rețelei într-un mod care permite întreruperea sau segmentarea instantanee a acesteia, pentru a reduce la minimum și a preveni contagiunea, în special în cazul proceselor financiare interconectate.

În scopul aplicării literei (e) de la primul paragraf, procesul de gestionare a modificărilor la nivelul TIC este aprobat de liniile de management corespunzătoare și dispune de protocoale specifice.

Articolul 10

Detectare

(1) Entitățile financiare dispun de mecanisme pentru detectarea rapidă a activităților anormale, în conformitate cu articolul 17, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea posibilelor puncte unice de defecțiune semnificative.

Toate mecanismele de detectare menționate la primul paragraf sunt testate cu regularitate în conformitate cu articolul 25.

(2) Mecanismele de detectare menționate la alineatul (1) permit niveluri multiple de control, definesc praguri de alertă și criterii de declanșare și inițiere a proceselor de răspuns la incidentele legate de TIC, inclusiv mecanisme de alertă automată pentru personalul relevant responsabil de răspunsul la incidentele legate de TIC.

(3) Entitățile financiare alocă suficiente resurse și capacități pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC, în special a atacurilor cibernetice.

(4) Furnizorii de servicii de raportare a datelor dispun, în plus, de sisteme care pot verifica în mod eficace integralitatea rapoartelor de tranzacționare, pot identifica omisiunile și erorile evidente și pot solicita retransmiterea rapoartelor respective.

Articolul 11

Răspuns și recuperare

(1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1) și pe baza cerințelor de identificare prevăzute la articolul 8, entitățile financiare instituie o politică cuprinzătoare de continuitate a activității TIC, care poate fi adoptată sub forma unei politici specifice dedicate, ca parte integrantă a politicii generale de continuitate a activității a entității financiare.

(2) Entitățile financiare pun în aplicare politica de continuitate a activității TIC prin măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate care vizează:

(a) asigurarea continuității funcțiilor critice sau importante ale entității financiare;

(b) un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare;

(c) activarea fără întârziere a unor planuri specifice care permit aplicarea unor măsuri, procese și tehnologii de limitare adecvate pentru fiecare tip de incident legat de TIC și previn producerea unor daune suplimentare, precum și a unor proceduri de răspuns și de recuperare adaptate, stabilite în conformitate cu articolul 12;

(d) estimarea efectelor, a daunelor și a pierderilor preliminare;

(e) stabilirea unor măsuri de comunicare și de gestionare a crizelor care să asigure faptul că informațiile actualizate sunt transmise tuturor membrilor personalului intern relevant și părților interesate externe relevante, în conformitate cu articolul 14, și raportarea către autoritățile competente, în conformitate cu articolul 19.

(3) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare pun în aplicare planuri de răspuns și de recuperare în domeniul TIC asociate care, în cazul altor entități financiare decât microîntreprinderile, sunt supuse unor evaluări de audit intern independente.

(4) Entitățile financiare instituie, mențin și testează periodic planuri de continuitate a activității TIC adecvate, în special în ceea ce privește funcțiile critice sau importante externalizate sau contractate prin acorduri cu furnizori terți de servicii TIC.

(5) Ca parte a politicii generale de continuitate a activității, entitățile financiare efectuează o analiză a impactului asupra activității (AIA) al expunerilor lor la perturbări grave ale activității. În conformitate cu AIA, entitățile financiare evaluează impactul potențial al perturbărilor grave ale activității cu ajutorul unor criterii cantitative și calitative, utilizând date interne și externe și analize de scenarii, după caz. AIA ia în considerare caracterul critic al funcțiilor operaționale identificate și cartografiate, al proceselor de sprijin, al dependențelor față de terți și al activelor informaționale, precum și interdependențele acestora. Entitățile financiare se asigură că activele TIC și serviciile TIC sunt proiectate și utilizate în deplină conformitate cu AIA, în special în ceea ce privește asigurarea în mod adecvat a redundanței tuturor componentelor critice.

(6) Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare:

(a) testează planurile de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC în legătură cu sistemele TIC care sprijină toate funcțiile cel puțin o dată pe an, precum și în caz de eventuale modificări substanțiale ale sistemelor TIC care sprijină funcții critice sau importante;

(b) testează planurile de comunicare în situații de criză instituite în conformitate cu articolul 14.

În scopul aplicării literei (a) de la primul paragraf, entitățile financiare altele decât microîntreprinderile includ în planurile de testare scenarii de atacuri cibernetice și transferuri între infrastructura TIC primară și capacitățile redundante, copiile de rezervă și instalațiile redundante necesare pentru a îndeplini obligațiile prevăzute la articolul 12.

Entitățile financiare își revizuiesc periodic politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC, ținând seama de rezultatele testelor efectuate în conformitate cu primul paragraf, precum și de recomandările care decurg din evaluările de audit sau procesele de supraveghere.

(7) Entitățile financiare altele decât microîntreprinderile au o funcție de gestionare a crizelor, care, în caz de activare a planurilor lor de continuitate a activității TIC sau a planurilor lor de răspuns și de recuperare în domeniul TIC, stabilește, printre altele, proceduri clare de gestionare a comunicărilor interne și externe în situații de criză, în conformitate cu articolul 14.

(8) Entitățile financiare păstrează o evidență ușor accesibilă a activităților înainte și în timpul evenimentelor perturbatoare atunci când sunt activate planurile lor de continuitate a activității TIC și planurile lor de răspuns și de recuperare în domeniul TIC.

(9) Depozitarii centrali de titluri de valoare furnizează autorităților competente copii ale rezultatelor testelor privind continuitatea activității TIC sau ale unor exerciții similare.

(10) Entitățile financiare, altele decât microîntreprinderile, raportează autorităților competente, la cererea acestora, o estimare a costurilor și a pierderilor anuale agregate cauzate de incidente majore legate de TIC.

(11) În conformitate cu articolul 16 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES elaborează, prin intermediul Comitetului comun, până la 17 iulie 2024, orientări comune privind estimarea costurilor și pierderilor anuale agregate menționate la alineatul (10).

Articolul 12

Politici și proceduri privind copiile de rezervă și proceduri și metode de restaurare și recuperare

(1) Pentru a asigura restaurarea sistemelor TIC și a datelor cu o perioadă de indisponibilitate minimă și o perturbare și o pierdere limitate, ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare elaborează și documentează:

(a) politici și proceduri privind copiile de rezervă care precizează sfera de acoperire a datelor care fac obiectul copierii de rezervă, precum și frecvența minimă a copierii de rezervă, pe baza caracterului critic al informațiilor sau al nivelului de confidențialitate al datelor;

(b) proceduri și metode de restaurare și recuperare.

(2) Entitățile financiare instituie sisteme de rezervă care pot fi activate în conformitate cu politicile și procedurile privind copiile de rezervă, precum și cu procedurile și metodele de restaurare și recuperare. Activarea sistemelor de rezervă nu pune în pericol securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea ori confidențialitatea datelor. Periodic se efectuează testarea procedurilor privind copiile de rezervă și a procedurilor și metodelor de restaurare și recuperare.

(3) Atunci când restaurează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care sunt separate fizic și logic de sistemul TIC sursă. Sistemele TIC sunt securizate împotriva oricărui acces neautorizat sau a deteriorării TIC și permit restaurarea în timp util a serviciilor care utilizează copii de rezervă ale datelor și sistemelor, după caz.

În cazul contrapărților centrale, planurile de recuperare permit recuperarea tuturor tranzacțiilor în momentul perturbării, pentru a permite contrapărții centrale să continue să opereze în condiții de siguranță și să finalizeze decontarea la data stabilită.

În plus, furnizorii de servicii de raportare a datelor mențin resurse adecvate și dispun de instalații pentru copii de rezervă și de restaurare, cu scopul de a-și oferi și a-și menține serviciile viabile în orice moment.

(4) Entitățile financiare, altele decât microîntreprinderile, mențin capacități TIC redundante dotate cu resurse, capacități și funcții care sunt adecvate pentru a acoperi nevoile operaționale. Microîntreprinderile evaluează necesitatea menținerii unor astfel de capacități TIC redundante pe baza profilului lor de risc.

(5) Depozitarii centrali de titluri de valoare mențin cel puțin o unitate de prelucrare secundară, dotată cu resurse adecvate, capacități, funcții și resurse umane pentru a acoperi nevoile operaționale.

Unitatea de prelucrare secundară:

(a) este situată la o distanță geografică față de unitatea de prelucrare principală pentru a se asigura că are un profil de risc distinct și pentru a preveni afectarea acesteia de către evenimentul care a afectat unitatea de prelucrare principală;

(b) este capabilă să asigure continuitatea funcțiilor critice sau importante în mod identic cu unitatea de prelucrare principală sau să furnizeze serviciile la nivelul necesar pentru a se asigura că entitatea financiară își desfășoară operațiunile critice în conformitate cu obiectivele de recuperare;

(c) este imediat accesibilă personalului entității financiare pentru a asigura continuitatea funcțiilor critice sau importante în cazul în care unitatea de prelucrare principală a devenit indisponibilă.

(6) Pentru a stabili obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, pentru fiecare funcție, entitățile financiare iau în considerare dacă este vorba de o funcție critică sau importantă și impactul potențial global asupra eficienței pieței. Aceste obiective temporale asigură că, în scenarii extreme, nivelurile convenite ale serviciilor sunt respectate.

(7) În cazul recuperării în urma unui incident legat de TIC, entitățile financiare efectuează verificări necesare, inclusiv verificări și reconcilieri multiple, pentru a se asigura că nivelul de integritate a datelor este cel mai ridicat. Aceste verificări se efectuează, de asemenea, atunci când sunt reconstituite date de la părțile interesate externe, pentru a se asigura că toate datele sunt coerente între sisteme.

Articolul 13

Învățăminte și perspective de dezvoltare

(1) Entitățile financiare dispun de capacități și de personal pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, și pentru a analiza impactul pe care acestea l-ar putea avea asupra rezilienței lor operaționale digitale.

(2) Entitățile financiare instituie verificări ulterioare incidentelor legate de TIC după ce un incident major legat de TIC le perturbă activitățile de bază, analizând cauzele perturbării și identificând îmbunătățirile necesare pentru operațiunile TIC sau în cadrul politicii de continuitate a activității TIC menționate la articolul 11.

Entitățile financiare, altele decât microîntreprinderile, comunică autorităților competente, la cerere, modificările care au fost operate în urma verificărilor ulterioare incidentelor legate de TIC, astfel cum sunt menționate la primul paragraf.

Verificările ulterioare incidentelor legate de TIC menționate la primul paragraf stabilesc dacă procedurile instituite au fost urmate și dacă măsurile luate au fost eficace, inclusiv în ceea ce privește următoarele:

(a) promptitudinea reacției la alertele de securitate și determinarea impactului și a gravității incidentelor legate de TIC;

(b) calitatea și rapiditatea efectuării unei analize judiciare, acolo unde se consideră necesar;

(c) eficacitatea activării nivelurilor succesive de intervenție (incident escalation) în caz de incidente în cadrul entității financiare;

(d) eficacitatea comunicării interne și externe.

(3) Învățămintele desprinse în urma testării rezilienței operaționale digitale, efectuată în conformitate cu articolele 26 și 27, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC, împreună cu informațiile relevante schimbate cu contrapărțile și evaluate în timpul proceselor de supraveghere, sunt încorporate în mod corespunzător și continuu în procesul de evaluare a riscurilor TIC. Constatările respective stau la baza unor revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1).

(4) Entitățile financiare monitorizează eficacitatea punerii în aplicare a strategiei lor privind reziliența operațională digitală menționate la articolul 6 alineatul (8). Acestea cartografiază evoluția riscurilor TIC de-a lungul timpului, analizează frecvența, tipurile, magnitudinea și evoluția incidentelor legate de TIC, în special a atacurilor cibernetice și a modelelor lor, în vederea înțelegerii nivelului expunerii la riscurile TIC, în special în legătură cu funcțiile critice sau importante, și a consolidării gradului de maturitate și de pregătire cibernetică a entității financiare.

(5) Personalul de nivel superior din domeniul TIC raportează cel puțin o dată pe an către organul de conducere cu privire la rezultatele menționate la alineatul (3) și propune recomandări.

(6) Entitățile financiare elaborează programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale ca module obligatorii în cadrul programelor lor de formare a personalului. Respectivele programe și cursuri de formare se aplică tuturor angajaților și personalului de conducere de nivel superior și au un nivel de complexitate proporțional cu sfera de competență a funcțiilor lor. După caz, entitățile financiare includ, de asemenea, furnizorii terți de servicii TIC în programele lor de formare relevante, în conformitate cu articolul 30 alineatul (2) litera (i).

(7) Entitățile financiare altele decât microîntreprinderile monitorizează evoluțiile tehnologice relevante în mod continuu, inclusiv pentru a înțelege posibilul impact al implementării unor astfel de noi tehnologii asupra cerințelor în materie de securitate TIC și a rezilienței operaționale digitale. Acestea trebuie să aibă informații actualizate cu privire la cele mai recente procese de gestionare a riscurilor TIC, cu scopul de a contracara cu eficacitate formele existente sau noi de atacuri cibernetice.

Articolul 14

Comunicare

(1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare instituie planuri de comunicare în situații de criză care permit o informare responsabilă a clienților și a contrapărților, precum și a publicului, după caz, cu privire la, cel puțin, incidentele majore sau vulnerabilitățile legate de TIC.

(2) Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare politici de comunicare pentru personalul intern și pentru părțile interesate externe. Politicile de comunicare pentru personal țin seama de necesitatea de a face distincția între personalul implicat în gestionarea riscurilor TIC, în special personalul responsabil pentru răspuns și recuperare, și personalul care trebuie să fie informat.

(3) Cel puțin o persoană din entitatea financiară este însărcinată cu punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și îndeplinește în acest scop funcția de legătură cu publicul și mass-media.

Articolul 15

Armonizarea suplimentară a instrumentelor, metodelor, proceselor și politicilor de gestionare a riscurilor TIC

AES elaborează, prin intermediul Comitetului comun, în consultare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), proiecte comune de standarde tehnice de reglementare în următoarele scopuri:

(a) pentru a aduce precizări suplimentare privind elementele necesare a fi incluse în politicile, procedurile, protocoalele și instrumentele de securitate TIC menționate la articolul 9 alineatul (2), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor, al menținerii disponibilității, autenticității, integrității și confidențialității datelor, inclusiv tehnici criptografice, și al garantării unei transmiteri exacte și rapide a datelor fără perturbări majore și fără întârzieri nejustificate;

(b) pentru a aduce precizări suplimentare privind componentele controalelor drepturilor de gestionare a accesului menționate la articolul 9 alineatul (4) litera (c) și politica privind resursele umane aferentă, precizând drepturile de acces, procedurile de acordare și de revocare a drepturilor, monitorizarea comportamentului anormal în ceea ce privește riscurile TIC prin intermediul unor indicatori adecvați, inclusiv pentru modelele de utilizare a rețelei, orele, activitatea IT și dispozitivele necunoscute;

(c) pentru a aduce precizări suplimentare privind mecanismele menționate la articolul 10 alineatul (1) care permit detectarea rapidă a activităților anormale și criteriile menționate la articolul 10 alineatul (2) care declanșează procesele de detectare și de răspuns la incidentele legate de TIC;

(d) pentru a aduce precizări suplimentare privind componentele politicii de continuitate a activității TIC, menționată la articolul 11 alineatul (1);

(e) pentru a aduce precizări suplimentare privind testarea planurilor de continuitate a activității TIC menționate la articolul 11 alineatul (6), pentru a asigura faptul că o astfel de testare ține seama în mod corespunzător de scenariile în care calitatea furnizării unei funcții critice sau importante se deteriorează până la un nivel inacceptabil sau eșuează, precum și că ia în considerare în mod corespunzător impactul potențial al insolvenței sau al altor disfuncționalități ale oricărui furnizor terț de servicii TIC relevant și, dacă este cazul, riscurile politice din jurisdicțiile furnizorilor respectivi;

(f) pentru a aduce precizări suplimentare privind componentele planurilor de răspuns și de recuperare în domeniul TIC menționate la articolul 11 alineatul (3);

(g) pentru a aduce precizări suplimentare privind conținutul și formatul raportului referitor la revizuirea cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (5).

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale, ținând seama în mod corespunzător de orice caracteristică specifică care decurge din natura distinctă a activităților din diferite sectoare de servicii financiare.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Articolul 16

Cadrul simplificat de gestionare a riscurilor TIC

(1) Articolele 5-15 din prezentul regulament nu se aplică firmelor de investiții mici și neinterconectate, instituțiilor de plată exceptate în temeiul Directivei (UE) 2015/2366; instituțiilor exceptate în temeiul Directivei 2013/36/UE în cazul cărora statele membre au decis să nu aplice opțiunea menționată la articolul 2 alineatul (4) din prezentul regulament; instituțiilor emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE; și nici instituțiilor mici pentru furnizarea de pensii ocupaționale.

Fără a aduce atingere primului paragraf, entitățile menționate la primul paragraf:

(a) instituie și mențin un cadru solid și documentat de gestionare a riscurilor TIC care detaliază mecanismele și măsurile care vizează o gestionare rapidă, eficientă și cuprinzătoare a riscurilor TIC, inclusiv pentru protecția componentelor și infrastructurilor fizice relevante;

(b) monitorizează în permanență securitatea și funcționarea tuturor sistemelor TIC;

(c) reduc la minimum impactul riscurilor TIC prin utilizarea unor sisteme, protocoale și instrumente TIC solide, reziliente și actualizate care sunt adecvate pentru a sprijini desfășurarea activităților lor și furnizarea serviciilor și protejează în mod adecvat disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor din rețele și sistemele informatice;

(d) permit identificarea și detectarea rapidă a surselor de riscuri TIC și a anomaliilor din rețele și sistemele informatice, precum și gestionarea rapidă a incidentelor legate de TIC;

(e) identifică principalele dependențe față de furnizorii terți de servicii TIC;

(f) asigură continuitatea funcțiilor critice sau importante, prin planuri de continuitate a activității și măsuri de răspuns și de recuperare, care includ, cel puțin, măsuri privind copii de rezervă și restaurarea;

(g) testează cu regularitate planurile și măsurile menționate la litera (f), precum și eficacitatea controalelor puse în aplicare în conformitate cu literele (a) și (c);

(h) implementează, după caz, concluziile operaționale relevante rezultate din testele menționate la litera (g) și din analiza ulterioară incidentului în procesul de evaluare a riscurilor TIC și elaborează, în funcție de nevoi și de profilul de risc TIC, programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale destinate personalului și conducerii.

(2) Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) al doilea paragraf litera (a) se documentează și se revizuiește periodic, precum și în momentul producerii unor incidente majore legate de TIC, în conformitate cu instrucțiunile de supraveghere. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării. Autorității competente i se prezintă, la cererea sa, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.

(3) AES elaborează, prin intermediul Comitetului comun, în consultare cu ENISA, proiecte comune de standarde tehnice de reglementare în următoarele scopuri:

(a) pentru a aduce precizări suplimentare privind elementele care trebuie incluse în cadrul de gestionare a riscurilor TIC menționat la alineatul (1) al doilea paragraf litera (a);

(b) pentru a aduce precizări suplimentare privind elementele legate de sistemele, protocoalele și instrumentele destinate reducerii la minimum a impactului riscurilor TIC menționate la alineatul (1) al doilea paragraf litera (c), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor și al menținerii disponibilității, autenticității, integrității și confidențialității datelor;

(c) pentru a aduce precizări suplimentare privind componentele planurilor de continuitate a activității TIC menționate la alineatul (1) al doilea paragraf litera (f);

(d) pentru a aduce precizări suplimentare privind normele referitoare la testarea planurilor de continuitate a activității și pentru a asigura eficacitatea controalelor menționate la alineatul (1) al doilea paragraf litera (g), precum și pentru a garanta faptul că o astfel de testare ține seama în mod corespunzător de scenariile în care calitatea furnizării unei funcții critice sau importante se deteriorează până la un nivel inacceptabil sau eșuează;

(e) pentru a aduce precizări suplimentare privind conținutul și formatul raportului referitor la revizuirea cadrului de gestionare a riscurilor TIC menționat la alineatul (2).

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

CAPITOLUL III

Gestionarea, clasificarea și raportarea incidentelor legate de TIC

Articolul 17

Procesul de gestionare a incidentelor legate de TIC

(1) Entitățile financiare definesc, instituie și pun în aplicare un proces de gestionare a incidentelor legate de TIC pentru a detecta, a gestiona și a notifica incidentele legate de TIC.

(2) Entitățile financiare înregistrează toate incidentele legate de TIC și amenințările cibernetice semnificative. Entitățile financiare instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor legate de TIC, pentru a asigura identificarea, documentarea și abordarea cauzelor lor principale, astfel încât să se prevină apariția unor astfel de incidente.

(3) Procesul de gestionare a incidentelor legate de TIC menționat la alineatul (1):

(a) instituie indicatori de avertizare timpurie;

(b) stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC în funcție de prioritatea și de gravitatea lor și în funcție de caracterul critic al serviciilor afectate, în conformitate cu criteriile stabilite la articolul 18 alineatul (1);

(c) alocă roluri și responsabilități care trebuie activate pentru diferite tipuri și scenarii de incidente legate de TIC;

(d) stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media, în conformitate cu articolul 14, și pentru notificarea clienților, proceduri interne de activare a nivelurilor succesive de intervenție (escalation), inclusiv în cazul unor plângeri din partea clienților legate de TIC, precum și pentru furnizarea de informații entităților financiare care acționează în calitate de contrapărți, după caz;

(e) asigură că cel puțin incidentele majore legate de TIC sunt raportate conducerii superioare relevante și informează organul de conducere cu privire la cel puțin incidentele majore legate de TIC, explicând impactul, răspunsul și controalele suplimentare care urmează să fie instituite ca urmare a unor astfel de incidente legate de TIC;

(f) stabilește proceduri de răspuns la incidentele legate de TIC în vederea atenuării efectelor și a asigurării faptului că serviciile devin operaționale și sigure în timp util.

Articolul 18

Clasificarea incidentelor legate de TIC și a amenințărilor cibernetice

(1) Entitățile financiare clasifică incidentele legate de TIC și determină impactul acestora pe baza următoarelor criterii:

(a) numărul și/sau relevanța clienților sau a contrapărților financiare afectate și, după caz, cuantumul și numărul tranzacțiilor afectate de incidentul legat de TIC, precum și eventualul impact al incidentului legat de TIC asupra reputației;

(b) durata incidentului legat de TIC, inclusiv perioada de indisponibilitate a serviciului;

(c) întinderea geografică în ceea ce privește zonele afectate de incidentul legat de TIC, în special în cazul în care acesta afectează mai mult de două state membre;

(d) pierderile de date pe care le implică incidentul legat de TIC, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor;

(e) caracterul critic al serviciilor afectate, inclusiv al tranzacțiilor și operațiunilor entității financiare;

(f) impactul economic, în special costurile și pierderile directe și indirecte, ale incidentului legat de TIC, în termeni atât absoluți, cât și relativi.

(2) Entitățile financiare clasifică amenințările cibernetice ca fiind semnificative pe baza caracterului critic al serviciilor expuse riscului, inclusiv al tranzacțiilor și operațiunilor entității financiare, precum și pe baza numărului și/sau relevanței clienților sau a contrapărților financiare vizate și a întinderii geografice a zonelor expuse riscului.

(3) AES elaborează, prin intermediul Comitetului comun și în consultare cu BCE și ENISA, proiecte comune de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind următoarele:

(a) criteriile menționate la alineatul (1), inclusiv pragurile de semnificație pentru determinarea incidentelor majore legate de TIC sau, după caz, a incidentelor majore operaționale sau de securitate legate de plăți care fac obiectul obligației de raportare prevăzute la articolul 19 alineatul (1);

(b) criteriile care trebuie aplicate de autoritățile competente în scopul evaluării relevanței incidentelor majore legate de TIC sau, după caz, a incidentelor majore operaționale sau de securitate legate de plăți, pentru autoritățile competente relevante ale altor state membre, precum și detaliile rapoartelor referitoare la incidentele majore legate de TIC sau, după caz, incidentele majore operaționale sau de securitate legate de plăți care trebuie să fie comunicate altor autorități competente în temeiul articolului 19 alineatele (6) și (7);

(c) criteriile prevăzute la alineatul (2) de la prezentul articol, inclusiv pragurile înalte de semnificație pentru determinarea amenințărilor cibernetice semnificative.

(4) Atunci când elaborează proiectele comune de standarde tehnice de reglementare menționate la alineatul (3) de la prezentul articol, AES țin seama de criteriile stabilite la articolul 4 alineatul (2), precum și de standardele internaționale și de orientările și specificațiile elaborate și publicate de ENISA, inclusiv, după caz, de specificațiile pentru alte sectoare economice. În scopul aplicării criteriilor prevăzute la articolul 4 alineatul (2), AES iau în considerare în mod corespunzător necesitatea ca microîntreprinderile și întreprinderile mici și mijlocii să mobilizeze resurse și capacități suficiente pentru a se asigura că incidentele legate de TIC sunt gestionate rapid.

AES transmit Comisiei aceste proiecte comune de standarde tehnice de reglementare până la 17 ianuarie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la alineatul (3), în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Articolul 19

Raportarea incidentelor majore legate de TIC și notificarea voluntară a amenințărilor cibernetice semnificative

(1) Entitățile financiare raportează incidentele majore legate de TIC autorității competente relevante menționate la articolul 46 în conformitate cu alineatul (4) de la prezentul articol.

În cazul în care o entitate financiară face obiectul supravegherii de către mai mult de o autoritate națională competentă astfel cum este menționată la articolul 46, statele membre desemnează o autoritate competentă unică drept autoritate competentă relevantă responsabilă cu îndeplinirea funcțiilor și a sarcinilor prevăzute la prezentul articol.

Instituțiile de credit clasificate drept semnificative, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, prezintă un raport referitor la incidentele majore legate de TIC autorității naționale competente relevante desemnate în conformitate cu articolul 4 din Directiva 2013/36/UE, care transmite imediat raportul respectiv către BCE.

În sensul primului paragraf, după colectarea și analizarea tuturor informațiilor relevante, entitățile financiare efectuează notificarea inițială și elaborează rapoartele menționate la alineatul (4) de la prezentul articol, utilizând modelele menționate la articolul 20, și le transmit autorității competente. În cazul în care o imposibilitate tehnică împiedică transmiterea notificării inițiale utilizând modelul, entitățile financiare informează autoritatea competentă cu privire la aceasta prin mijloace alternative.

Notificarea inițială și rapoartele menționate la alineatul (4) includ toate informațiile necesare autorității competente pentru a determina semnificația incidentului major legat de TIC și a evalua posibilele efecte transfrontaliere.

Fără a aduce atingere raportării prevăzute la primul paragraf de către entitățile financiare către autoritatea competentă relevantă, statele membre pot stabili în plus ca unele entități financiare sau toate aceste entități să transmită, de asemenea, notificarea inițială și fiecare raport menționat la alineatul (4) de la prezentul articol, folosind modelele menționate la articolul 20, autorităților competente sau echipelor de intervenție în caz de incidente de securitate informatică (echipe CSIRT) desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.

(2) Entitățile financiare pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea competentă relevantă atunci când consideră că amenințarea este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți. Autoritatea competentă relevantă poate furniza astfel de informații și altor autorități relevante, menționate la alineatul (6).

Instituțiile de credit clasificate drept semnificative, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea națională competentă relevantă, desemnată în conformitate cu articolul 4 din Directiva 2013/36/UE, care transmite imediat notificarea către BCE.

Statele membre pot stabili că entitățile financiare care fac în mod voluntar o notificare în conformitate cu primul paragraf pot transmite, de asemenea, notificarea respectivă către echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.

(3) În cazul în care are loc un incident major legat de TIC care are un impact asupra intereselor financiare ale clienților lor, entitățile financiare îi informează pe aceștia, fără întârzieri nejustificate, de îndată ce află despre incidentul major legat de TIC, cu privire la incidentul respectiv și la măsurile care au fost luate pentru a atenua efectele negative ale unui astfel de incident.

În cazul unei amenințări cibernetice semnificative, entitățile financiare își informează, după caz, clienții care ar putea fi afectați cu privire la eventualele măsuri de protecție adecvate pe care aceștia din urmă ar putea dori să le ia.

(4) Până la termenele care urmează să fie stabilite în conformitate cu articolul 20 primul paragraf litera (a) punctul (ii), entitățile financiare transmit autorității competente relevante următoarele:

(a) o notificare inițială;

(b) un raport intermediar după notificarea inițială menționată la litera (a) de îndată ce starea incidentului inițial s-a schimbat în mod semnificativ sau gestionarea incidentului major legat de TIC s-a schimbat pe baza noilor informații disponibile, urmat, după caz, de notificări actualizate de fiecare dată când este disponibilă o actualizare relevantă a stării, precum și la cererea specifică a autorității competente;

(c) un raport final, atunci când analiza cauzelor principale a fost finalizată, indiferent dacă măsurile de atenuare au fost sau nu deja puse în aplicare, precum și atunci când cifrele efective ale impactului sunt disponibile pentru a înlocui estimările.

(5) Entitățile financiare pot externaliza, în conformitate cu legislația sectorială a Uniunii și cu cea națională, obligațiile de raportare prevăzute la prezentul articol către un furnizor terț de servicii. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de îndeplinirea cerințelor legate de raportarea incidentului.

(6) La primirea notificării inițiale și a fiecărui raport menționat la alineatul (4), autoritatea competentă furnizează, în timp util, detalii privind incidentul major legat de TIC următorilor destinatari, pe baza, după caz, a competențelor lor respective:

(a) ABE, ESMA sau EIOPA;

(b) BCE, în cazul entităților financiare menționate la articolul 2 alineatul (1) literele (a), (b) și (d);

(c) autoritățile competente, punctele unice de contact sau echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555;

(d) autoritățile de rezoluție, astfel cum sunt menționate la articolul 3 din Directiva 2014/59/UE, și Comitetul unic de rezoluție (SRB) în ceea ce privește entitățile menționate la articolul 7 alineatul (2) din Regulamentul (UE) nr. 806/2014 al Parlamentului European și al Consiliului ([37]), precum și în ceea ce privește entitățile și grupurile menționate la articolul 7 alineatul (4) litera (b) și alineatul (5) din Regulamentul (UE) nr. 806/2014 dacă aceste detalii se referă la incidente care prezintă un risc pentru asigurarea funcțiilor critice în sensul articolului 2 alineatul (1) punctul 35 din Directiva 2014/59/UE; și

(e) alte autorități publice relevante în temeiul dreptului intern.

(7) După primirea informațiilor în conformitate cu alineatul (6), ABE, ESMA sau EIOPA și BCE, în consultare cu ENISA și în cooperare cu autoritatea competentă relevantă, evaluează dacă incidentul major legat de TIC este relevant pentru autoritățile competente din alte state membre. În urma acestei evaluări, ABE, ESMA sau EIOPA notifică în consecință, cât mai curând posibil, autoritățile competente relevante din alte state membre. BCE notifică membrilor Sistemului European al Băncilor Centrale aspectele relevante pentru sistemul de plată. Pe baza notificării respective, autoritățile competente iau, după caz, toate măsurile necesare pentru protejarea stabilității imediate a sistemului financiar.

([37]) Regulamentul (UE) nr. 806/2014 al Parlamentului European și al Consiliului din 15 iulie 2014 de stabilire a unor norme uniforme și a unei proceduri uniforme de rezoluție a instituțiilor de credit și a anumitor firme de investiții în cadrul unui mecanism unic de rezoluție și al unui fond unic de rezoluție și de modificare a Regulamentului (UE) nr. 1093/2010 (JO L 225, 30.7.2014, p. 1).

(8) Notificarea care trebuie efectuată de ESMA în temeiul alineatului (7) de la prezentul articol nu aduce atingere responsabilității autorității competente de a transmite de urgență detaliile incidentului major legat de TIC autorității relevante din statul membru gazdă, în cazul în care un depozitar central de titluri de valoare desfășoară o activitate transfrontalieră semnificativă în statul membru gazdă, în cazul în care incidentul major legat de TIC este susceptibil să genereze consecințe grave pentru piețele financiare din statul membru gazdă și în cazul în care există acorduri de cooperare între autoritățile competente în ceea ce privește supravegherea entităților financiare.

Articolul 20

Armonizarea conținutului rapoartelor și a modelelor de rapoarte

AES, prin intermediul Comitetului comun și în consultare cu ENISA și BCE, elaborează:

(a) proiecte comune de standarde tehnice de reglementare având ca scop următoarele:

(i) stabilirea conținutului rapoartelor în cazul incidentelor majore legate de TIC, cu scopul de a reflecta criteriile prevăzute la articolul 18 alineatul (1) și de a include elemente suplimentare, precum detalii pentru a stabili dacă rapoartele sunt relevante pentru alte state membre și dacă incidentele constituie incidente majore operaționale sau de securitate legate de plăți;

(ii) stabilirea termenelor pentru notificarea inițială și pentru fiecare raport menționat la articolul 19 alineatul (4);

(iii) stabilirea conținutului notificării privind amenințările cibernetice semnificative.

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale, în special pentru a se asigura că, în sensul literei (a) punctul (ii) de la prezentul paragraf, existența unor termene diferite poate reflecta, după caz, particularitățile sectoarelor financiare, fără a aduce atingere menținerii unei abordări coerente a raportării incidentelor legate de TIC în temeiul prezentului regulament și al Directivei (UE) 2022/2555. AES furnizează, după caz, justificări atunci când se abat de la abordările adoptate în contextul directivei respective;

(b) proiecte comune de standarde tehnice de punere în aplicare având ca scop stabilirea formularelor, modelelor și procedurilor standard pentru raportarea de către entitățile financiare a unui incident major legat de TIC și notificarea de către acestea a unei amenințări cibernetice semnificative.

AES transmit Comisiei proiectele comune de standarde tehnice de reglementare menționate la primul paragraf litera (a) și proiectele comune de standarde tehnice de punere în aplicare menționate la primul paragraf litera (b), până la 17 iulie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare comune menționate la primul paragraf litera (a), în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Se conferă Comisiei competența de a adopta standardele tehnice de punere în aplicare comune menționate la primul paragraf litera (b), în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Articolul 21

Centralizarea raportării incidentelor majore legate de TIC

(1) AES elaborează, prin intermediul Comitetului comun și în consultare cu BCE și ENISA, un raport comun de evaluare a fezabilității centralizării suplimentare a raportării incidentelor prin crearea unei platforme unice la nivelul UE pentru raportarea incidentelor majore legate de TIC de către entitățile financiare. Raportul comun analizează modalitățile de facilitare a fluxului raportării incidentelor legate de TIC, de reducere a costurilor asociate și de susținere a analizelor tematice în vederea consolidării convergenței în materie de supraveghere.

(2) Raportul comun menționat la alineatul (1) cuprinde cel puțin următoarele elemente:

(a) condițiile prealabile pentru instituirea unei platforme unice la nivelul UE;

(b) beneficiile, limitările și riscurile, inclusiv riscurile asociate concentrării ridicate a informațiilor sensibile;

(c) capacitatea necesară pentru a asigura interoperabilitatea cu alte sisteme de raportare relevante;

(d) elemente ale gestionării operaționale;

(e) condițiile de participare;

(f) modalitățile tehnice de accesare a platformei unice la nivelul UE de către entitățile financiare și autoritățile naționale competente;

(g) o evaluare preliminară a costurilor suportate cu instituirea platformei operaționale care sprijină platforma unică la nivelul UE, inclusiv expertiza necesară.

(3) AES transmit raportul menționat la alineatul (1) Parlamentului European, Consiliului și Comisiei până la 17 ianuarie 2025.

Articolul 22

Feedback privind supravegherea

(1) Fără a aduce atingere contribuției, consultanței sau soluțiilor tehnice și urmăririi ulterioare care pot fi oferite, după caz, în conformitate cu dreptul intern, de către echipele CSIRT în temeiul Directivei (UE) 2022/2555, autoritatea competentă, la primirea notificării inițiale și a fiecărui raport menționate la articolul 19 alineatul (4), confirmă primirea și poate furniza autorității financiare, acolo unde este posibil, în timp util, feedback relevant și proporțional sau îndrumări la nivel înalt, în special prin punerea la dispoziție a oricăror informații și date operative relevante anonimizate cu privire la amenințări similare și poate discuta măsurile de remediere aplicate la nivelul entității financiare și modalități de reducere la minimum și de atenuare a impactului negativ la nivelul sectorului financiar. Fără a aduce atingere feedbackului privind supravegherea primit, entitățile financiare rămân pe deplin responsabile de gestionarea incidentelor legate de TIC raportate în temeiul articolului 19 alineatul (1) și de consecințele acestora.

(2) Prin intermediul Comitetului comun, AES raportează anual, în mod anonim și agregat, cu privire la incidentele majore legate de TIC, ale căror detalii sunt furnizate de autoritățile competente în conformitate cu articolul 19 alineatul (6), menționând cel puțin numărul incidentelor majore legate de TIC, natura acestora și impactul lor asupra operațiunilor entităților financiare sau ale clienților, măsurile de remediere luate și costurile suportate.

AES emit avertismente și elaborează statistici la nivel înalt pentru a sprijini evaluările privind amenințările și vulnerabilitățile din perspectiva TIC.

Articolul 23

Incidente operaționale sau de securitate legate de plăți care vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică

Cerințele prevăzute în prezentul capitol se aplică, de asemenea, incidentelor operaționale sau de securitate legate de plăți și incidentelor operaționale sau de securitate majore legate de plăți, atunci când acestea vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică.

CAPITOLUL IV

Testarea rezilienței operaționale digitale

Articolul 24

Cerințe generale pentru efectuarea testării rezilienței operaționale digitale

(1) În scopul evaluării nivelului de pregătire pentru gestionarea incidentelor legate de TIC, al identificării punctelor slabe, a deficiențelor și a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, entitățile financiare, altele decât microîntreprinderile, stabilesc, mențin și revizuiesc, ținând seama de criteriile prevăzute la articolul 4 alineatul (2), un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC menționat la articolul 6.

(2) Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente care trebuie aplicate în conformitate cu articolele 25 și 26.

(3) Atunci când desfășoară programul de testare a rezilienței operaționale digitale menționat la alineatul (1) de la prezentul articol, entitățile financiare, altele decât microîntreprinderile, urmează o abordare bazată pe riscuri, ținând seama de criteriile prevăzute la articolul 4 alineatul (2) și luând în considerare în mod corespunzător evoluția peisajului riscurilor TIC, orice riscuri specifice la care entitatea financiară în cauză este sau ar putea fi expusă, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor pe care entitatea financiară îl consideră adecvat.

(4) Entitățile financiare, altele decât microîntreprinderile, se asigură că testele sunt efectuate de părți independente, indiferent dacă sunt interne sau externe. Atunci când testele sunt efectuate de o entitate internă, entitățile financiare alocă resurse suficiente și se asigură că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului.

(5) Entitățile financiare, altele decât întreprinderile, stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate chestiunile identificate pe parcursul desfășurării testelor și stabilesc metodologii de validare internă pentru a se asigura că toate punctele slabe, deficiențele sau lacunele identificate sunt abordate integral.

(6) Entitățile financiare, altele decât microîntreprinderile, se asigură că se efectuează teste adecvate cel puțin o dată pe an asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante.

Articolul 25

Testarea instrumentelor și sistemelor TIC

(1) Programul de testare a rezilienței operaționale digitale menționat la articolul 24 asigură, în conformitate cu criteriile prevăzute la articolul 4 alineatul (2), efectuarea de teste adecvate, precum evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă acolo unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste de la un capăt la altul (end-to-end) sau teste de penetrare.

(2) Depozitarii centrali de titluri de valoare și contrapărțile centrale efectuează evaluări ale vulnerabilității înainte de utilizarea sau reutilizarea unor aplicații și componente de infrastructură noi sau existente și servicii TIC care sprijină funcții critice sau importante ale entității financiare.

(3) Microîntreprinderile efectuează testele menționate la alineatul (1) combinând o abordare bazată pe riscuri cu o planificare strategică a testării TIC și luând în considerare în mod corespunzător necesitatea de a menține o abordare echilibrată între amploarea resurselor și timpul care urmează să fie alocat testării TIC prevăzute la prezentul articol, pe de o parte, și urgența, tipul de risc, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor relevant, inclusiv capacitatea entității financiare de a-și asuma riscuri calculate, pe de altă parte.

Articolul 26

Testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul TLPT

(1) Entitățile financiare, altele decât entitățile menționate la articolul 16 alineatul (1) primul paragraf și altele decât microîntreprinderile, care sunt identificate în conformitate cu alineatul (8) al treilea paragraf de la prezentul articol, efectuează, cel puțin o dată la trei ani, testări avansate prin intermediul TLPT. Pe baza profilului de risc al entității financiare și ținând seama de circumstanțele operaționale, autoritatea competentă poate să solicite entității financiare, dacă este necesar, să reducă sau să mărească această frecvență.

(2) Fiecare test de penetrare bazat pe amenințări acoperă unele sau toate funcțiile critice sau importante ale unei entități financiare și este realizat pe sistemele de producție în timp real care sprijină astfel de funcții.

Entitățile financiare identifică toate sistemele, procesele și tehnologiile TIC subiacente relevante care sprijină funcțiile critice sau importante și serviciile TIC, inclusiv pe cele care sprijină funcțiile critice sau importante care au fost externalizate sau contractate unor furnizori terți de servicii TIC.

Entitățile financiare evaluează ce funcții critice sau importante trebuie să fie acoperite de TLPT. Rezultatul acestei evaluări determină sfera de aplicare exactă a TLPT și este validat de autoritățile competente.

(3) În cazul în care furnizorii terți de servicii TIC sunt incluși în sfera de aplicare a TLPT, entitatea financiară ia măsurile și garanțiile necesare pentru a asigura participarea acestor furnizori terți de servicii TIC la TLPT și rămân în orice moment pe deplin responsabile de asigurarea respectării prezentului regulament.

(4) Fără a aduce atingere primului și celui de al doilea paragraf de la alineatul (2), în cazul în care se preconizează în mod rezonabil că participarea unui furnizor terț de servicii TIC la TLPT, astfel cum se menționează la alineatul (3), va avea un impact negativ asupra calității sau securității serviciilor oferite de către furnizorul terț de servicii TIC către clienți care sunt entități ce nu intră în domeniul de aplicare al prezentului regulament, sau asupra confidențialității datelor legate de astfel de servicii, entitatea financiară și furnizorul terț de servicii TIC pot conveni în scris ca furnizorul terț de servicii TIC să încheie în mod direct acorduri contractuale cu o entitate externă de testare în scopul desfășurării, sub conducerea unei entități financiare desemnate unice, a unei TLPT grupate, în care să fie implicate mai multe entități financiare (testare grupată) pentru care furnizorul terț de servicii TIC oferă servicii TIC.

Testarea grupată respectivă acoperă gama relevantă de servicii TIC care sprijină funcțiile critice sau importante contractate de către entitățile financiare respectivului furnizor terț de servicii TIC. Testarea grupată este considerată TLPT efectuată de entitățile financiare care participă la testarea grupată.

Numărul entităților financiare care participă la testarea grupată este calibrat în mod corespunzător, ținând seama de complexitatea și de tipurile serviciilor implicate.

(5) Entitățile financiare efectuează, cu cooperarea furnizorilor terți de servicii TIC și a altor părți implicate, inclusiv a entităților de testare, dar excluzând autoritățile competente, controale eficace ale gestionării riscurilor pentru a atenua riscurile unui potențial impact asupra datelor și riscurile de deteriorare a activelor și de perturbare a funcțiilor, a serviciilor sau a operațiunilor critice sau importante la nivelul entității financiare înseși, al contrapărților acesteia sau al sectorului financiar.

(6) La sfârșitul testării, după ce s-a convenit cu privire la rapoarte și la planurile de remediere, entitatea financiară și, după caz, entitățile externe de testare furnizează autorității desemnate în conformitate cu alineatul (9) sau (10) un rezumat al constatărilor relevante, planurile de remediere și documentația care demonstrează că TLPT a fost efectuată în conformitate cu cerințele.

(7) Autoritățile furnizează entităților financiare o adeverință prin care se confirmă faptul că testul a fost efectuat în conformitate cu cerințele evidențiate în documentație, pentru a permite recunoașterea reciprocă între autoritățile competente a testelor de penetrare bazate pe amenințări. Entitatea financiară notifică autorității competente relevante adeverința, rezumatul constatărilor relevante și planurile de remediere.

Fără a aduce atingere unei astfel de adeverințe, entitățile financiare rămân în orice moment pe deplin responsabile pentru impactul testelor menționate la alineatul (4).

(8) Entitățile financiare contractează entități de testare în scopul efectuării TLPT în conformitate cu articolul 27. Atunci când entitățile financiare utilizează entități interne de testare în scopul efectuării TLPT, acestea contractează entități externe de testare la fiecare trei teste.

Instituțiile de credit care sunt clasificate drept semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, utilizează numai entități externe de testare în conformitate cu articolul 27 alineatul (1) literele (a)-(e).

Autoritățile competente identifică entitățile financiare care sunt obligate să efectueze TLPT ținând seama de criteriile prevăzute la articolul 4 alineatul (2), pe baza unei evaluări a următoarelor elemente:

(a) factorii legați de impact, în special măsura în care serviciile furnizate și activitățile întreprinse de entitatea financiară au impact asupra sectorului financiar;

(b) posibile preocupări legate de stabilitatea financiară, inclusiv caracterul sistemic al entității financiare la nivelul Uniunii sau la nivel național, după caz;

(c) profilul de risc TIC specific, nivelul de maturitate a entității financiare din perspectiva TIC sau caracteristicile tehnologice implicate.

(9) Statele membre pot desemna o autoritate publică unică în sectorul financiar care să fie responsabilă de aspectele legate de TLPT în sectorul financiar la nivel național și îi încredințează acesteia toate competențele și sarcinile în acest sens.

(10) În absența unei desemnări în conformitate cu alineatul (9) de la prezentul articol și fără a aduce atingere competenței de a identifica entitățile financiare care trebuie să efectueze TLPT, o autoritate competentă poate delega exercitarea unora sau a tuturor sarcinilor menționate la prezentul articol și la articolul 27 unei alte autorități naționale din sectorul financiar.

(11) AES elaborează, în acord cu BCE, proiecte comune de standarde tehnice de reglementare în conformitate cu cadrul TIBER–EU pentru a aduce precizări suplimentare privind:

(a) criteriile utilizate în scopul aplicării alineatului (8) al doilea paragraf;

(b) cerințele și standardele care reglementează utilizarea entităților interne de testare;

(c) cerințele privind:

  (i) sfera de aplicare a TLPT menționată la alineatul (2);

  (ii) metodologia de testare și abordarea de urmat pentru fiecare fază specifică a procesului de testare;

  (iii) rezultatele, încheierea și etapele procesului de remediere aferente testării;

(d) tipul de cooperare în materie de supraveghere și alt tip de cooperare relevant care sunt necesare pentru punerea în aplicare a TLPT și pentru facilitarea recunoașterii reciproce a testării respective, în contextul entităților financiare care operează în mai multe state membre, pentru a permite un nivel adecvat de implicare din perspectiva supravegherii și o aplicare flexibilă, astfel încât să se țină seama de specificitățile subsectoarelor financiare sau ale piețelor financiare locale.

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES țin seama în mod corespunzător de orice caracteristică specifică care decurge din natura distinctă a activităților din diferite sectoare de servicii financiare.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Articolul 27

Cerințe pentru entitățile de testare în ceea ce privește efectuarea TLPT

(1) Entitățile financiare utilizează, în scopul efectuării TLPT, numai entități de testare care:

(a) sunt cele mai adecvate și de cea mai înaltă reputație;

(b) dețin capacități tehnice și organizatorice și demonstrează expertiză specifică în ceea ce privește datele operative privind amenințările, testele de penetrare și testarea de tipul „echipa roșie";

(c) sunt certificate de un organism de acreditare dintr-un stat membru sau aderă la coduri de conduită sau cadre etice formale;

(d) oferă o asigurare independentă sau un raport de audit în ceea ce privește gestionarea solidă a riscurilor asociate cu efectuarea TLPT, inclusiv protecția corespunzătoare a informațiilor confidențiale ale entității financiare și măsurile reparatorii pentru riscurile legate de activitățile entității financiare;

(e) sunt acoperite în mod corespunzător și în totalitate de asigurările de răspundere civilă profesională relevante, inclusiv împotriva riscurilor de abatere și neglijență.

(2) În cazul utilizării entităților interne de testare, entitățile financiare se asigură că, în plus față de cerințele de la alineatul (1), se respectă toate condițiile următoare:

(a) utilizarea a fost aprobată de autoritatea competentă relevantă sau de autoritatea publică unică desemnată în conformitate cu articolul 26 alineatele (9) și (10);

(b) autoritatea competentă relevantă a verificat că entitatea financiară are suficiente resurse alocate și s-a asigurat că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului; și

(c) furnizorul de date operative privind amenințările este extern entității financiare.

(3) Entitățile financiare se asigură că contractele încheiate cu entități externe de testare impun o gestionare solidă a rezultatelor TLPT și că orice prelucrare de date de către acestea, inclusiv orice generare, stocare, agregare, elaborare, raportare, comunicare sau distrugere, nu creează riscuri pentru entitatea financiară.

CAPITOLUL V

Gestionarea riscurilor TIC generate de părți terțe

Secțiunea I

Principii-cheie pentru o gestionare solidă a riscurilor TIC generate de părți terțe

Articolul 28

Principii generale

(1) Entitățile financiare gestionează riscurile TIC generate de părți terțe ca parte integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC astfel cum este menționat la articolul 6 alineatul (1) și în conformitate cu următoarele principii:

(a) entitățile financiare care au instituit acorduri contractuale pentru utilizarea serviciilor TIC în scopul desfășurării operațiunilor lor rămân în orice moment pe deplin responsabile de respectarea și de îndeplinirea tuturor obligațiilor care decurg din prezentul regulament și din dreptul aplicabil în domeniul serviciilor financiare;

(b) gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în aplicare din perspectiva principiului proporționalității, luând în considerare:

(i) natura, amploarea, complexitatea și importanța dependențelor legate de TIC;

(ii) riscurile care decurg din acordurile contractuale privind utilizarea serviciilor TIC încheiate cu furnizori terți de servicii TIC, ținând seama de caracterul critic sau importanța serviciului, procesului sau funcției respective, precum și de impactul potențial asupra continuității și disponibilității serviciilor și activităților financiare, la nivel individual și la nivel de grup.

(2) Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare, altele decât entitățile menționate la articolul 16 alineatul (1) primul paragraf și altele decât microîntreprinderile, adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia privind existența mai multor furnizori menționată la articolul 6 alineatul (9), după caz. Această strategie privind riscurile TIC generate de părți terțe include o politică privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC și se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată. Pe baza unei evaluări a profilului general de risc al entității financiare și a amplorii și complexității serviciilor comerciale, organul de conducere examinează periodic riscurile identificate în ceea ce privește acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante.

(3) Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare mențin și actualizează la nivel de entitate și la nivel subconsolidat și consolidat un registru de informații în legătură cu toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC.

Acordurile contractuale menționate la primul paragraf sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă servicii TIC de sprijinire a funcțiilor critice sau importante și cele care nu le acoperă.

Entitățile financiare raportează cel puțin o dată pe an autorităților competente cu privire la numărul de noi acorduri privind utilizarea serviciilor TIC, categoriile de furnizori terți de servicii TIC, tipurile de acorduri contractuale și serviciile și funcțiile TIC care sunt oferite.

Entitățile financiare pun la dispoziția autorității competente, la cererea acesteia, registrul complet de informații sau, după caz, secțiuni specifice din acesta, împreună cu orice informații considerate necesare pentru a permite supravegherea eficace a entității financiare.

Entitățile financiare informează autoritatea competentă în timp util cu privire la orice acord contractual planificat privind utilizarea unor servicii TIC care sprijină funcții critice sau importante, precum și atunci când o funcție a devenit critică sau importantă.

(4) Înainte de a încheia un acord contractual privind utilizarea serviciilor TIC, entitățile financiare:

(a) evaluează dacă acordul contractual vizează utilizarea unor servicii TIC care sprijină o funcție critică sau importantă;

(b) evaluează dacă sunt îndeplinite condițiile pentru contractare din perspectiva supravegherii;

(c) identifică și evaluează toate riscurile relevante legate de acordul contractual, inclusiv posibilitatea ca un astfel de acord contractual să contribuie la consolidarea riscului de concentrare a serviciilor TIC, astfel cum este menționat la articolul 29;

(d) efectuează toate diligențele necesare cu privire la potențialii furnizori terți de servicii TIC și se asigură, pe parcursul proceselor de selecție și evaluare, că furnizorul terț de servicii TIC este adecvat;

(e) identifică și evaluează conflictele de interese pe care acordul contractual le poate cauza.

(5) Entitățile financiare pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standarde adecvate de securitate a informațiilor. În cazul în care acordurile contractuale respective se referă la funcții critice sau importante, entitățile financiare, înainte de încheierea acordurilor, țin seama în mod corespunzător de utilizarea de către furnizorii terți de servicii TIC a celor mai recente și de cea mai înaltă calitate standarde de securitate a informațiilor.

(6) În exercitarea drepturilor de acces, de inspecție și de audit cu privire la furnizorul terț de servicii TIC, entitățile financiare stabilesc în prealabil, utilizând o abordare bazată pe riscuri, frecvența auditurilor și a inspecțiilor, precum și domeniile care urmează să fie auditate prin aderarea la standardele de audit acceptate de comun acord, în concordanță cu instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde de audit.

În cazul în care acordurile contractuale încheiate cu furnizori terți de servicii TIC privind utilizarea unor servicii TIC prezintă o complexitate tehnică ridicată, entitatea financiară verifică dacă auditorii, atât cei interni, cât și cei externi, sau un grup de auditori, dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.

(7) Entitățile financiare se asigură că acordurile contractuale privind utilizarea serviciilor TIC pot fi reziliate în oricare dintre următoarele circumstanțe:

(a) încălcarea semnificativă de către furnizorul terț de servicii TIC a actelor cu putere de lege, a reglementărilor sau a clauzelor contractuale aplicabile;

(b) circumstanțe identificate pe parcursul monitorizării riscurilor TIC generate de părți terțe care sunt considerate capabile să modifice îndeplinirea funcțiilor oferite prin acordul contractual, inclusiv modificările semnificative care afectează acordul sau situația furnizorului terț de servicii TIC;

(c) deficiențe demonstrate ale furnizorului terț de servicii TIC legate de gestionarea sa generală a riscurilor TIC și, în special, legate de modul în care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, fie date cu caracter personal sau date sensibile din alt punct de vedere, ori a datelor fără caracter personal;

(d) în cazul în care autoritatea competentă nu mai poate supraveghea în mod eficace entitatea financiară ca urmare a condițiilor acordului contractual respectiv sau a unor circumstanțe legate de acesta.

(8) Pentru serviciile TIC care sprijină funcții critice sau importante, entitățile financiare instituie strategii de ieșire. Strategiile de ieșire țin seama de riscurile care pot apărea la nivelul furnizorilor terți de servicii TIC, în special o posibilă deficiență din partea acestora, o deteriorare a calității serviciilor TIC oferite, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor TIC sau orice riscuri semnificative care decurg din utilizarea adecvată și continuă a serviciului TIC respectiv ori încetarea acordurilor contractuale cu furnizorii terți de servicii TIC în oricare dintre situațiile enumerate la alineatul (7).

Entitățile financiare se asigură că pot să se retragă din acordurile contractuale fără:

(a) perturbarea activităților lor comerciale;

(b) limitarea respectării cerințelor în materie de reglementare;

(c) afectarea continuității și calității serviciilor furnizate către clienți.

Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, în conformitate cu criteriile stabilite la articolul 4 alineatul (2), trebuie să fie testate în mod suficient și revizuite periodic.

Entitățile financiare identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine serviciile TIC contractate și datele relevante de la furnizorul terț de servicii TIC și să le transfere în condiții de siguranță și în integralitatea lor către furnizori alternativi sau să le reintegreze în sistemul propriu.

Entitățile financiare instituie măsuri adecvate pentru situații neprevăzute astfel încât să păstreze continuitatea activității în cazul apariției situațiilor menționate la primul paragraf.

(9) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de punere în aplicare pentru a stabili modelele standard pentru registrul de informații menționat la alineatul (3), inclusiv informații care sunt comune tuturor acordurilor contractuale privind utilizarea serviciilor TIC. AES transmit Comisiei aceste proiecte de standarde tehnice de punere în aplicare până la 17 ianuarie 2024.

Se conferă Comisiei competența de a adopta standardele tehnice de punere în aplicare menționate la primul paragraf în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

(10) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind conținutul detaliat al politicii menționate la alineatul (2) în legătură cu acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC.

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Articolul 29

Evaluarea preliminară a riscului de concentrare a serviciilor TIC

(1) La identificarea și evaluarea riscurilor menționate la articolul 28 alineatul (4) litera (c), entitățile financiare iau în considerare, de asemenea, dacă încheierea preconizată a unui acord contractual în legătură cu servicii TIC care sprijină funcții critice sau importante ar conduce la oricare dintre următoarele situații:

(a) stabilirea unei relații contractuale cu un furnizor terț de servicii TIC care nu este ușor de înlocuit; sau

(b) instituirea unor acorduri contractuale multiple cu privire la furnizarea de servicii TIC care sprijină funcții critice sau importante cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns conectați.

Entitățile financiare evaluează beneficiile și costurile soluțiilor alternative, cum ar fi utilizarea unor furnizori terți de servicii TIC diferiți, luând în considerare dacă și în ce mod soluțiile avute în vedere corespund nevoilor și obiectivelor operaționale stabilite în strategia lor privind reziliența digitală.

(2) În cazul în care acordurile contractuale privind utilizarea de servicii TIC care sprijină funcții critice sau importante includ posibilitatea ca un furnizor terț de servicii TIC să subcontracteze în continuare servicii TIC care sprijină o funcție critică sau importantă către alți furnizori terți de servicii TIC, entitățile financiare evaluează beneficiile și riscurile care pot apărea în legătură cu o astfel de subcontractare, în special în cazul unui subcontractant TIC stabilit într-o țară terță.

În cazul în care acordurile contractuale privesc servicii TIC care sprijină funcții critice sau importante, entitățile financiare iau în considerare în mod corespunzător dispozițiile din legislația privind insolvența care s-ar aplica în eventualitatea falimentului furnizorului terț de servicii TIC, precum și orice constrângere care ar putea apărea în legătură cu recuperarea urgentă a datelor entității financiare.

Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante sunt încheiate cu un furnizor terț de servicii TIC stabilit într-o țară terță, entitățile financiare iau în considerare, în afară de aspectele menționate la al doilea paragraf, și conformitatea cu normele Uniunii privind protecția datelor și asigurarea efectivă a respectării legii în respectiva țară terță.

Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante prevăd subcontractarea, entitățile financiare evaluează dacă și în ce mod lanțurile de subcontractare potențial lungi sau complexe pot avea un impact asupra capacității lor de a monitoriza pe deplin funcțiile contractate și asupra capacității autorității competente de a supraveghea efectiv entitatea financiară din acest punct de vedere.

Articolul 30

Dispoziții contractuale esențiale

(1) Drepturile și obligațiile care revin entității financiare și furnizorului terț de servicii TIC sunt clar atribuite și definite în scris. Contractul complet include acordurile privind nivelul serviciilor **și** este consemnat într-un document scris care se află la dispoziția părților pe suport de hârtie sau într-un document având un alt format durabil, accesibil și care poate fi descărcat.

(2) Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele elemente:

(a) o descriere clară și completă a tuturor funcțiilor și serviciilor TIC care urmează să fie furnizate de furnizorul terț de servicii TIC, indicând dacă este permisă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau părți semnificative ale acesteia și, în caz afirmativ, condițiile aplicabile acestei subcontractări;

(b) locurile, și anume regiunile sau țările, în care urmează să fie furnizate funcțiile și serviciile TIC contractate sau subcontractate și în care urmează să fie prelucrate datele, inclusiv locul stabilit pentru stocare, precum și cerința ca furnizorul terț de servicii TIC să informeze în prealabil entitatea financiară în cazul în care are în vedere modificarea acestor locuri;

(c) dispoziții privind disponibilitatea, autenticitatea, integritatea și confidențialitatea în ceea ce privește protecția datelor, inclusiv a datelor cu caracter personal;

(d) dispoziții privind asigurarea accesului, a recuperării și a returnării într-un format ușor accesibil a datelor cu caracter personal și a celor fără caracter personal prelucrate de entitatea financiară în caz de insolvență, de rezoluție sau de încetare a activității furnizorului terț de servicii TIC sau în cazul încetării acordurilor contractuale;

(e) descrieri la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora;

(f) obligația furnizorului terț de servicii TIC de a oferi asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante, atunci când survine un incident TIC care este legat de serviciul TIC furnizat entității financiare;

(g) obligația furnizorului terț de servicii TIC de a coopera pe deplin cu autoritățile competente și cu autoritățile de rezoluție ale entității financiare, inclusiv cu persoanele numite de acestea;

(h) drepturile de încetare și perioadele minime de preaviz aferente pentru încetarea acordurilor contractuale, în conformitate cu așteptările autorităților competente și ale autorităților de rezoluție;

(i) condițiile pentru participarea furnizorilor terți de servicii TIC la programele de conștientizare cu privire la securitatea TIC ale entităților financiare și la cursurile de formare în domeniul rezilienței operaționale digitale în conformitate cu articolul 13 alineatul (6).

(3) Acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante includ, în plus față de elementele menționate la alineatul (2), cel puțin următoarele:

(a) descrieri complete la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora, cu obiective cantitative și calitative precise privind performanța în limitele nivelurilor convenite ale serviciilor, pentru a permite monitorizarea eficace de către entitatea financiară a serviciilor TIC și adoptarea unor măsuri corective adecvate, fără întârzieri nejustificate, atunci când nu sunt asigurate nivelurile convenite ale serviciilor;

(b) perioade de preaviz și obligații de raportare către entitatea financiară pentru furnizorul terț de servicii TIC, inclusiv notificarea oricărei evoluții care ar putea avea un impact semnificativ asupra capacității furnizorului terț de servicii TIC de a furniza în mod eficace serviciile TIC în sprijinul funcțiilor critice sau importante, în concordanță cu nivelurile convenite ale serviciului;

(c) cerințe ca furnizorul terț de servicii TIC să pună în aplicare și să testeze planuri pentru situații neprevăzute și să dispună de măsuri, instrumente și politici în materie de securitate a TIC care să asigure un nivel adecvat de securitate în ceea ce privește furnizarea serviciilor de către entitatea financiară, în concordanță cu cadrul său de reglementare;

(d) obligația furnizorului terț de servicii TIC de a participa la TLPT ale entității financiare și de a coopera pe deplin în cadrul realizării acestora, astfel cum se menționează la articolele 26 și 27;

(e) dreptul de a monitoriza, în permanență, performanța furnizorului terț de servicii TIC, care presupune următoarele:

(i) drepturile nerestricționate de acces, de inspecție și de audit de către entitatea financiară sau o parte terță desemnată și de către autoritatea competentă, precum și dreptul de a produce copii ale documentelor relevante la fața locului, dacă acestea sunt esențiale pentru operațiunile furnizorului terț de servicii TIC, drepturi a căror exercitare efectivă nu este împiedicată sau limitată de alte acorduri contractuale sau politici de punere în aplicare;

(ii) dreptul de a conveni asupra unor niveluri de asigurare alternative în cazul în care sunt afectate drepturile altor clienți;

(iii) obligația furnizorului terț de servicii TIC de a coopera pe deplin în timpul inspecțiilor și auditurilor la fața locului efectuate de autoritățile competente, de supraveghetorul principal, de entitatea financiară sau de o parte terță desemnată; și

(iv) obligația de a transmite detalii privind domeniul de aplicare, procedurile care trebuie urmate și frecvența unor astfel de inspecții și audituri;

(f) strategiile de ieșire, în special stabilirea unei perioade de tranziție adecvate obligatorii:

(i) în cursul căreia furnizorul terț de servicii TIC va continua să furnizeze funcțiile sau serviciile TIC respective vizând să reducă riscul de perturbare în cadrul entității financiare sau să asigure rezoluția și restructurarea sa eficace;

(ii) care permite entității financiare să migreze către un alt furnizor terț de servicii TIC sau să treacă la soluții dezvoltate de aceasta pe plan intern, în conformitate cu complexitatea serviciului furnizat.

Prin derogare de la litera (e), furnizorul terț de servicii TIC și entitatea financiară care este o microîntreprindere pot conveni ca drepturile de acces, de inspecție și de audit ale entității financiare să poată fi delegate unui terț independent, numit de furnizorul terț de servicii TIC, și ca entitatea financiară să poată solicita în orice moment din partea terțului informații și asigurări cu privire la performanța furnizorului terț de servicii TIC.

(4) La negocierea acordurilor contractuale, entitățile financiare și furnizorii terți de servicii TIC țin seama de utilizarea clauzelor contractuale standard elaborate de autoritățile publice pentru servicii specifice.

(5) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare cu privire la elementele menționate la alineatul (2) litera (a), pe care o entitate financiară trebuie să le stabilească și să le evalueze atunci când subcontractează servicii TIC care sprijină funcții critice sau importante.

Atunci când elaborează aceste proiecte de standarde tehnice de reglementare, AES țin seama de dimensiunea și de profilul general de risc al entității financiare, precum și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Secțiunea II

Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC

Articolul 31

Desemnarea furnizorilor terți esențiali de servicii TIC

(1) AES, prin intermediul Comitetului comun și la recomandarea Forumului de supraveghere instituit în temeiul articolului 32 alineatul (1):

(a) desemnează furnizorii terți de servicii TIC care sunt esențiali pentru entitățile financiare, în urma unei evaluări care ține seama de criteriile menționate la alineatul (2);

(b) desemnează drept supraveghetor principal pentru fiecare furnizor terț esențial de servicii TIC acea AES care este responsabilă, în conformitate cu Regulamentul (UE) nr. 1093/2010, (UE) nr. 1094/2010 sau (UE) nr. 1095/2010, de entitățile financiare care dețin împreună cea mai mare parte a activelor totale din valoarea activelor totale ale tuturor entităților financiare care utilizează serviciile furnizorului terț esențial de servicii TIC relevant, astfel cum reiese din suma bilanțurilor individuale ale entităților financiare respective.

(2) Desemnarea prevăzută la alineatul (1) litera (a) se bazează pe toate criteriile următoare în ceea ce privește serviciile TIC furnizate de furnizorul terț de servicii TIC:

(a) impactul sistemic asupra stabilității, continuității sau calității furnizării serviciilor financiare în situația în care furnizorul terț de servicii TIC relevant s-ar confrunta cu o defecțiune operațională la scară largă în ceea ce privește furnizarea serviciilor sale, ținând seama de numărul de entități financiare și de valoarea totală a activelor entităților financiare cărora furnizorul terț de servicii TIC relevant le oferă servicii;

(b) caracterul sistemic sau importanța entităților financiare care se bazează pe furnizorul terț de servicii TIC relevant, evaluată în conformitate cu următorii parametri:

(i) numărul de instituții de importanță sistemică globală (G-SII) sau de alte instituții de importanță sistemică (O-SII) care se bazează pe respectivul furnizor terț de servicii TIC;

(ii) interdependența dintre G-SII sau O-SII menționate la punctul (i) și alte entități financiare, inclusiv situațiile în care G-SII sau O-SII furnizează servicii de infrastructură financiară altor entități financiare;

(c) dependența entităților financiare de serviciile furnizate de furnizorul terț de servicii TIC relevant în ceea ce privește funcțiile critice sau importante ale entităților financiare care implică, în ultimă instanță, același furnizor terț de servicii TIC, indiferent dacă entitățile financiare se bazează direct sau indirect pe aceste servicii, prin intermediul unor acorduri de subcontractare;

(d) gradul de substituibilitate a furnizorului terț de servicii TIC, ținând seama de următorii parametri:

(i) lipsa unor alternative reale, chiar și parțiale, având în vedere numărul limitat de furnizori terți de servicii TIC activi pe o anumită piață sau cota de piață deținută de furnizorul terț de servicii TIC relevant sau complexitatea tehnică ori gradul de sofisticare implicat, inclusiv în ceea ce privește orice tehnologie protejată, sau caracteristicile specifice ale modului de organizare sau ale activității furnizorului terț de servicii TIC;

(ii) dificultăți în ceea ce privește migrarea parțială sau integrală a datelor și a volumelor de lucru relevante de la furnizorul terț de servicii TIC relevant către un alt furnizor terț de servicii TIC, fie ca urmare a costurilor financiare semnificative, a timpului sau a altor resurse pe care le poate implica procesul de migrare, fie din cauza unor riscuri TIC sporite sau a altor riscuri operaționale la care poate fi expusă entitatea financiară prin intermediul unei astfel de migrări.

(3) În cazul în care furnizorul terț de servicii TIC face parte dintr-un grup, criteriile menționate la alineatul (2) sunt examinate în raport cu serviciile TIC furnizate de grup în ansamblul său.

(4) Furnizorii terți esențiali de servicii TIC care fac parte dintr-un grup desemnează o persoană juridică drept punct de coordonare pentru a asigura în mod adecvat reprezentarea și comunicarea cu supraveghetorul principal.

(5) Supraveghetorul principal notifică furnizorului terț de servicii TIC rezultatul evaluării care a dus la desemnarea menționată la alineatul (1) litera (a). În termen de șase săptămâni de la data notificării, furnizorul terț de servicii TIC îi poate transmite supraveghetorului principal o declarație motivată conținând orice informații relevante în scopul evaluării. Supraveghetorul principal analizează declarația motivată și poate solicita să îi fie furnizate informații suplimentare în termen de 30 de zile calendaristice de la primirea unei astfel de declarații.

După ce a desemnat un furnizor terț de servicii TIC ca fiind esențial, AES, prin intermediul Comitetului comun, informează furnizorul terț de servicii TIC cu privire la această desemnare și cu privire la data de la care va începe să facă efectiv obiectul activităților de supraveghere. Data respectivă trebuie să fie la cel mult o lună de la momentul notificării. Furnizorul terț de servicii TIC informează entitățile financiare cărora le furnizează servicii cu privire la desemnarea sa drept esențial.

(6) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 57 pentru a completa prezentul regulament prin precizarea mai în detaliu a criteriilor menționate la alineatul (2) de la prezentul articol, până la 17 iulie 2024.

(7) Nu se recurge la desemnarea menționată la alineatul (1) litera (a) decât după ce Comisia a adoptat un act delegat în conformitate cu alineatul (6).

(8) Desemnarea menționată la alineatul (1) litera (a) nu se aplică în ceea ce privește:

(i) entitățile financiare care furnizează servicii TIC altor entități financiare;

(ii) furnizorii terți de servicii TIC care fac obiectul unor cadre de supraveghere instituite cu scopul de a sprijini misiunile menționate la articolul 127 alineatul (2) din Tratatul privind funcționarea Uniunii Europene;

(iii) furnizorii de servicii TIC intragrup;

(iv) furnizorii terți de servicii TIC care furnizează servicii TIC numai într-un stat membru unor entități financiare care își desfășoară activitatea numai în statul membru respectiv.

(9) AES, prin intermediul Comitetului comun, elaborează, publică și actualizează anual lista furnizorilor terți esențiali de servicii TIC la nivelul Uniunii.

(10) În sensul alineatului (1) litera (a), autoritățile competente transmit, anual și agregat, Forumului de supraveghere instituit în temeiul articolului 32 rapoartele menționate la articolul 28 alineatul (3) al treilea paragraf. Forumul de supraveghere evaluează dependențele entităților financiare față de furnizorii terți de servicii TIC pe baza informațiilor primite de la autoritățile competente.

(11) Furnizorii terți de servicii TIC care nu sunt incluși în lista menționată la alineatul (9) pot solicita să fie desemnați ca fiind esențiali în conformitate cu alineatul (1) litera (a).

În scopul aplicării primului paragraf, furnizorul terț de servicii TIC transmite o cerere motivată către ABE, ESMA sau EIOPA care, prin intermediul Comitetului comun, decide dacă să desemneze respectivul furnizor terț de servicii TIC ca fiind esențial în conformitate cu alineatul (1) litera (a).

Decizia menționată la al doilea paragraf se adoptă și se notifică furnizorului terț de servicii TIC în termen de șase luni de la primirea cererii.

(12) Entitățile financiare utilizează serviciile unui furnizor terț de servicii TIC stabilit într-o țară terță și care a fost desemnat ca fiind esențial în conformitate cu alineatul (1) litera (a) numai în cazul în care acesta din urmă a înființat o filială în Uniune în termen de 12 luni de la desemnare.

(13) Furnizorul terț esențial de servicii TIC menționat la alineatul (12) informează supraveghetorul principal cu privire la orice modificare a structurii conducerii filialei înființate în Uniune.

Articolul 32

Structura cadrului de supraveghere

(1) Comitetul comun, în conformitate cu articolul 57 alineatul (1) din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, instituie Forumul de supraveghere ca subcomitet în scopul sprijinirii activității Comitetului comun și a supraveghetorului principal menționat la articolul 31 alineatul (1) litera (b) în domeniul riscurilor TIC generate de părți terțe în toate sectoarele financiare. Forumul de supraveghere pregătește proiectele de poziții comune și de acte comune ale Comitetului comun în acest domeniu.

Forumul de supraveghere discută periodic despre evoluțiile relevante cu privire la riscurile și vulnerabilitățile TIC și promovează o abordare consecventă în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe la nivelul Uniunii.

(2) Forumul de supraveghere efectuează anual o evaluare colectivă a rezultatelor și a constatărilor activităților de supraveghere desfășurate pentru toți furnizorii terți esențiali de servicii TIC și promovează măsuri de coordonare pentru a spori reziliența operațională digitală a entităților financiare, a încuraja cele mai bune practici în ceea ce privește abordarea riscurilor de concentrare a serviciilor TIC și a studia factorii de diminuare în cazul transferurilor riscurilor la nivel transsectorial.

(3) Forumul de supraveghere prezintă criterii de referință cuprinzătoare pentru furnizorii terți esențiali de servicii TIC, care urmează să fie adoptate de Comitetul comun ca poziții comune ale AES în conformitate cu articolul 56 alineatul (1) din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

(4) Forumul de supraveghere este compus din:

(a) președinții AES;

(b) un reprezentant la nivel înalt provenind din personalul actual al autorității competente relevante menționate la articolul 46 din fiecare stat membru;

(c) directorii executivi ai fiecărei AES și câte un reprezentant din partea Comisiei, CERS, BCE și ENISA, în calitate de observatori;

(d) după caz, un reprezentant suplimentar al unei autorități competente menționate la articolul 46 din fiecare stat membru, în calitate de observator;

(e) după caz, un reprezentant al autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC, în calitate de observator.

Forumul de supraveghere poate, după caz, să solicite avizul unor experți independenți numiți în conformitate cu alineatul (6).

(5) Fiecare stat membru desemnează autoritatea competentă relevantă din cadrul personalului căreia este numit reprezentantul la nivel înalt menționat la alineatul (4) primul paragraf litera (b) și informează supraveghetorul principal în acest sens.

AES publică pe site-ul lor lista reprezentanților la nivel înalt, provenind din personalul actual al autorității competente relevante, desemnați de statele membre.

(6) Experții independenți menționați la alineatul (4) al doilea paragraf sunt numiți de Forumul de supraveghere dintr-un grup de rezervă de experți selectați în urma unui proces de candidatură public și transparent.

Experții independenți sunt numiți pe baza cunoștințelor și experienței lor în materie de stabilitate financiară, reziliență operațională digitală și securitate TIC. Aceștia acționează independent și obiectiv în interesul exclusiv al Uniunii în ansamblul său și nu solicită și nu primesc instrucțiuni din partea instituțiilor sau a organelor Uniunii, din partea vreunui guvern al unui stat membru sau din partea vreunui alt organism public sau privat.

(7) În conformitate cu articolul 16 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES emit, până la 17 iulie 2024, în scopul aplicării prezentei secțiuni, orientări privind cooperarea dintre AES și autoritățile competente cuprinzând procedurile și condițiile detaliate pentru alocarea și executarea sarcinilor între autoritățile competente și AES, precum și detaliile privind schimburile de informații care sunt necesare pentru ca autoritățile competente să se asigure că recomandările adresate furnizorilor terți esențiali de servicii TIC în temeiul articolului 35 alineatul (1) litera (d) sunt urmate.

(8) Cerințele prevăzute în prezenta secțiune nu aduc atingere aplicării Directivei (UE) 2022/2555 și a altor norme ale Uniunii privind supravegherea aplicabilă furnizorilor de servicii de cloud computing.

(9) AES, prin intermediul Comitetului comun și pe baza lucrărilor pregătitoare desfășurate de Forumul de supraveghere, prezintă anual Parlamentului European, Consiliului și Comisiei un raport privind aplicarea prezentei secțiuni.

Articolul 33

Sarcinile supraveghetorului principal

(1) Supraveghetorul principal, numit în conformitate cu articolul 31 alineatul (1) litera (b), efectuează supravegherea furnizorilor terți esențiali de servicii TIC atribuiți și este, cu privire la toate aspectele legate de supraveghere, punctul de contact principal pentru respectivii furnizori terți esențiali de servicii TIC.

(2) În scopul aplicării alineatului (1), supraveghetorul principal evaluează dacă fiecare furnizor terț esențial de servicii TIC a instituit norme, proceduri, mecanisme și măsuri cuprinzătoare, solide și eficace de gestionare a riscurilor TIC pe care le poate genera pentru entitățile financiare.

Evaluarea menționată la primul paragraf se axează în principal pe serviciile TIC furnizate de furnizorul terț esențial de servicii TIC care sprijină funcțiile critice sau importante ale entităților financiare. Atunci când este necesar pentru a aborda toate riscurile relevante, evaluarea respectivă se extinde la serviciile TIC care sprijină alte funcții decât cele critice sau importante.

(3) Evaluarea prevăzută la alineatul (2) cuprinde:

(a) cerințele privind TIC pentru a asigura, în special, securitatea, disponibilitatea, continuitatea, scalabilitatea și calitatea serviciilor pe care furnizorul terț esențial de servicii TIC le furnizează entităților financiare, precum și capacitatea de a menține în permanență standarde înalte de disponibilitate, autenticitate, integritate sau confidențialitate a datelor;

(b) securitatea fizică ce contribuie la asigurarea securității TIC, inclusiv securitatea sediilor, a instalațiilor, a centrelor de date;

(c) procesele de gestionare a riscurilor, inclusiv politicile de gestionare a riscurilor TIC, politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC;

(d) mecanismele de guvernanță, inclusiv o structură organizatorică cu arii de responsabilitate și norme privind răspunderea clare, transparente și coerente, care permit gestionarea eficace a riscurilor TIC;

(e) identificarea, monitorizarea și raportarea promptă a incidentelor semnificative legate de TIC către entitățile financiare, gestionarea și soluționarea acestor incidente, în special a atacurilor cibernetice;

(f) mecanismele de portabilitate a datelor, de portabilitate a aplicațiilor și de interoperabilitate, care asigură exercitarea efectivă a drepturilor de încetare de către entitățile financiare;

(g) testarea sistemelor, a infrastructurii și a controalelor TIC;

(h) auditurile privind TIC;

(i) utilizarea standardelor naționale și internaționale relevante aplicabile furnizării serviciilor sale TIC către entitățile financiare.

(4) Pe baza evaluării prevăzute la alineatul (2) și în coordonare cu Rețeaua de supraveghere comună (RSC) menționată la articolul 34 alineatul (1), supraveghetorul principal adoptă un plan de supraveghere individual clar, detaliat și motivat care descrie obiectivele anuale de supraveghere și principalele acțiuni de supraveghere planificate pentru fiecare furnizor terț esențial de servicii TIC. Planul respectiv este comunicat în fiecare an furnizorului terț esențial de servicii TIC.

Înainte de adoptarea planului de supraveghere, supraveghetorul principal comunică proiectul planului de supraveghere furnizorului terț esențial de servicii TIC.

La primirea proiectului de plan de supraveghere, furnizorul terț esențial de servicii TIC poate prezenta, în termen de 15 zile calendaristice, o declarație motivată prin care să demonstreze impactul preconizat asupra clienților care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament și, după caz, să formuleze soluții pentru atenuarea riscurilor.

(5) Odată ce planurile de supraveghere anuale menționate la alineatul (4) au fost adoptate și notificate furnizorilor terți esențiali de servicii TIC, autoritățile competente pot lua măsuri privind acești furnizori terți esențiali de servicii TIC numai în acord cu supraveghetorul principal.

Articolul 34

Coordonarea operațională a supraveghetorilor principali

(1) Pentru a asigura o abordare coerentă a activităților de supraveghere și a permite coordonarea strategiilor generale de supraveghere și coeziunea abordărilor operaționale și a metodologiilor de lucru, cei trei supraveghetori principali numiți în conformitate cu articolul 31 alineatul (1) litera (b) instituie o RSC pentru a-și coordona acțiunile în cursul etapelor pregătitoare și al desfășurării activităților de supraveghere a furnizorilor terți esențiali de servicii TIC pe care îi supraveghează fiecare dintre ei, precum și în cursul oricărei acțiuni care ar putea fi necesară în temeiul articolului 42.

(2) În scopul aplicării alineatului (1), supraveghetorii principali elaborează un protocol de supraveghere comun în care precizează procedurile detaliate care trebuie urmate pentru realizarea coordonării curente și pentru asigurarea unor schimburi și reacții rapide. Protocolul este revizuit periodic pentru a reflecta nevoile operaționale, în special evoluția modalităților practice de supraveghere.

(3) Supraveghetorii principali pot solicita ad-hoc BCE și ENISA să ofere consiliere tehnică, să facă schimb de experiență practică sau să participe la anumite reuniuni de coordonare ale RSC.

Articolul 35

Competențele supraveghetorului principal

(1) În scopul îndeplinirii atribuțiilor care îi revin în temeiul prezentei secțiuni, supraveghetorul principal are următoarele competențe în ceea ce privește furnizorii terți esențiali de servicii TIC:

(a) de a solicita toate informațiile și documentele relevante în conformitate cu articolul 37;

(b) de a efectua investigații generale și inspecții în conformitate cu articolele 38 și, respectiv, 39;

(c) de a solicita, după încheierea activităților de supraveghere, rapoarte în care se specifică acțiunile întreprinse sau măsurile de remediere care au fost puse în aplicare de furnizorii terți esențiali de servicii TIC în legătură cu recomandările menționate la litera (d) de la prezentul alineat;

(d) de a emite recomandări privind domeniile menționate la articolul 33 alineatul (3), în special privind:

(i) utilizarea unor cerințe sau procese specifice de securitate și calitate în domeniul TIC, în special în ceea ce privește introducerea de corecții, actualizări, criptări și alte măsuri de securitate pe care supraveghetorul principal le consideră relevante pentru asigurarea securității din perspectiva TIC a serviciilor furnizate entităților financiare;

(ii) utilizarea termenelor și condițiilor, inclusiv punerea în aplicare tehnică a acestora, potrivit cărora furnizorii terți esențiali de servicii TIC furnizează servicii TIC entităților financiare, pe care supraveghetorul principal le consideră relevante pentru prevenirea generării unor puncte unice de defecțiune sau a amplificării acestora sau pentru reducerea la minimum a impactului sistemic potențial la nivelul sectorului financiar al Uniunii în cazul unor riscuri de concentrare a serviciilor TIC;

(iii) orice subcontractare planificată, în cazul în care supraveghetorul principal consideră că subcontractarea în continuare, inclusiv acordurile de subcontractare pe care furnizorii terți esențiali de servicii TIC intenționează să le încheie cu furnizori terți de servicii TIC sau cu subcontractanți de servicii TIC stabiliți într-o țară terță, poate genera riscuri pentru furnizarea de servicii de către entitatea financiară sau riscuri pentru stabilitatea financiară, pe baza examinării informațiilor colectate în conformitate cu articolele 37 și 38;

(iv) abținerea de la încheierea unui nou acord de subcontractare, în cazul în care sunt îndeplinite următoarele condiții cumulative:

— subcontractantul avut în vedere este un furnizor terț de servicii TIC sau un subcontractant de servicii TIC stabilit într-o țară terță;

— subcontractarea vizează funcții critice sau importante ale entității financiare; și

— supraveghetorul principal consideră că utilizarea unei astfel de subcontractări prezintă un risc clar și grav pentru stabilitatea financiară a Uniunii sau pentru entitățile financiare, inclusiv pentru capacitatea entităților financiare de a se conforma cerințelor de supraveghere.

În scopul aplicării punctului (iv) de la prezenta literă, furnizorii terți de servicii TIC transmit informațiile privind subcontractarea supraveghetorului principal, utilizând modelul prevăzut la articolul 41 alineatul (1) litera (b).

(2) Atunci când exercită competențele prevăzute la prezentul articol, supraveghetorul principal:

(a) asigură o coordonare regulată în cadrul RSC și, în special, urmărește aplicarea unor abordări coerente, după caz, în ceea ce privește supravegherea furnizorilor terți esențiali de servicii TIC;

(b) ține seama în mod corespunzător de cadrul instituit prin Directiva (UE) 2022/2555 și, atunci când este necesar, consultă autoritățile competente relevante desemnate sau instituite în conformitate cu directiva respectivă, pentru a evita suprapunerea măsurilor tehnice și organizatorice care s-ar putea aplica furnizorilor terți esențiali de servicii TIC în temeiul directivei respective;

(c) urmărește să reducă la minimum, în măsura posibilului, riscul de perturbare a serviciilor furnizate de furnizori terți esențiali de servicii TIC unor clienți care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament.

(3) Supraveghetorul principal consultă Forumul de supraveghere înainte de a exercita competențele menționate la alineatul (1).

Înainte de a emite recomandări în conformitate cu alineatul (1) litera (d), supraveghetorul principal îi oferă furnizorului terț de servicii TIC posibilitatea de a prezenta, în termen de 30 de zile calendaristice, informații relevante care să demonstreze impactul preconizat asupra clienților care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament și, după caz, să formuleze soluții pentru atenuarea riscurilor.

(4) Supraveghetorul principal informează RSC cu privire la rezultatul exercitării competențelor prevăzute la alineatul (1) literele (a) și (b). Supraveghetorul principal transmite fără întârzieri nejustificate rapoartele menționate la alineatul (1) litera (c) către RSC și către autoritățile competente ale entităților financiare care utilizează serviciile TIC ale respectivului furnizor terț esențial de servicii TIC.

(5) Furnizorii terți esențiali de servicii TIC cooperează cu bună credință cu supraveghetorul principal și îl asistă pe acesta în îndeplinirea sarcinilor sale.

(6) În cazul nerespectării totale sau parțiale a măsurilor care trebuie luate ca urmare a exercitării competențelor prevăzute la alineatul (1) literele (a), (b) și (c) și după expirarea unui termen de cel puțin 30 de zile calendaristice de la data la care furnizorul terț esențial de servicii TIC a fost notificat cu privire la măsurile respective, supraveghetorul principal adoptă o decizie prin care impune o penalitate cu titlu cominatoriu pentru a obliga furnizorul terț esențial de servicii TIC să se conformeze măsurilor respective.

(7) Penalitățile cu titlu cominatoriu prevăzute la alineatul (6) se impun pe zi de întârziere până când conformitatea este asigurată și pe o perioadă de maximum șase luni de la data notificării deciziei de impunere a unei penalități cu titlu cominatoriu furnizorului terț esențial de servicii TIC.

(8) Cuantumul penalității cu titlu cominatoriu, calculat de la data prevăzută în decizia de impunere a penalității cu titlu cominatoriu, este de până la 1 % din cifra de afaceri zilnică medie globală a furnizorului terț esențial de servicii TIC din exercițiul financiar precedent. La stabilirea cuantumului penalității cu titlu cominatoriu, supraveghetorul principal ține seama de următoarele criterii referitoare la nerespectarea măsurilor prevăzute la alineatul (6):

(a) gravitatea și durata neconformității;

(b) dacă neconformitatea a fost săvârșită în mod intenționat sau din neglijență;

(c) nivelul de cooperare al furnizorului terț de servicii TIC cu supraveghetorul principal.

În scopul aplicării primului paragraf, pentru a asigura o abordare coerentă, supraveghetorul principal efectuează consultări în cadrul RSC.

(9) Penalitățile cu titlu cominatoriu sunt de natură administrativă și sunt executorii. Executarea este reglementată de normele de procedură civilă în vigoare în statul membru pe teritoriul căruia au loc inspecțiile și este acordat accesul. Plângerile legate de neregulile survenite în cursul executării sunt de competența instanțelor judecătorești ale statului membru în cauză. Sumele aferente penalităților se alocă bugetului general al Uniunii Europene.

(10) Supraveghetorul principal face publice toate penalitățile cu titlu cominatoriu aplicate, cu excepția cazurilor în care publicarea lor ar perturba grav piețele financiare sau ar aduce un prejudiciu disproporționat părților implicate.

(11) Înainte de a impune o penalitate cu titlu cominatoriu în temeiul alineatului (6), supraveghetorul principal oferă reprezentanților furnizorului terț esențial de servicii TIC care face obiectul procedurii posibilitatea de a fi audiat cu privire la constatări și își întemeiază deciziile numai pe constatările asupra cărora furnizorul terț esențial de servicii TIC care face obiectul procedurii a avut ocazia să își prezinte observațiile.

Dreptul la apărare al persoanelor care fac obiectul procedurii se respectă pe deplin pe durata acesteia. Furnizorul terț esențial de servicii TIC care face obiectul procedurii are dreptul de a avea acces la dosar, sub rezerva interesului legitim al altor persoane de a-și proteja secretele comerciale. Dreptul de acces la dosar nu se extinde și la informațiile confidențiale sau la documentele interne de lucru ale supraveghetorului principal.

Articolul 36

Exercitarea competențelor supraveghetorului principal în afara Uniunii

(1) Atunci când obiectivele de supraveghere nu pot fi atinse prin intermediul interacțiunii cu filiala înființată potrivit dispozițiilor articolului 31 alineatul (12) sau prin exercitarea de activități de supraveghere la sedii situate în Uniune, supraveghetorul principal poate exercita competențele menționate la următoarele dispoziții, cu privire la orice sediu situat într-o țară terță care este deținut sau utilizat în orice mod în scopul furnizării de servicii către entități financiare din Uniune de către un furnizor terț esențial de servicii TIC, în legătură cu operațiunile, funcțiile sau serviciile sale comerciale, inclusiv orice birou, sediu, teren, clădire sau altă proprietate folosită cu scop administrativ, comercial sau operațional:

(a) la articolul 35 alineatul (1) litera (a); și

(b) la articolul 35 alineatul (1) litera (b), în conformitate cu articolul 38 alineatul (2) literele (a), (b) și (d) și articolul 39 alineatul (1) și alineatul (2) litera (a).

Competențele menționate la primul paragraf pot fi exercitate sub rezerva îndeplinirii tuturor condițiilor următoare:

(i) supraveghetorul principal consideră că efectuarea unei inspecții într-o țară terță este necesară pentru a-i permite să își îndeplinească pe deplin și în mod eficace sarcinile care îi revin în temeiul prezentului regulament;

(ii) inspecția într-o țară terță este direct legată de furnizarea de servicii TIC unor entități financiare din Uniune;

(iii) furnizorul terț esențial de servicii TIC în cauză este de acord cu efectuarea unei inspecții într-o țară terță; și

(iv) autoritatea relevantă din țara terță în cauză a fost notificată oficial de supraveghetorul principal și nu a formulat nicio obiecție cu privire la aceasta.

(2) Fără a aduce atingere competențelor instituțiilor Uniunii și, respectiv, ale statelor membre, în scopul aplicării alineatului (1), ABE, ESMA sau EIOPA încheie acorduri de cooperare administrativă cu autoritatea relevantă din țara terță pentru a permite buna desfășurare a inspecțiilor în țara terță în cauză de către supraveghetorul principal și echipa desemnată de acesta pentru misiunea sa în țara terță respectivă. Aceste acorduri de cooperare nu creează obligații juridice pentru Uniune și statele sale membre și nu împiedică statele membre și autoritățile lor competente să încheie acorduri bilaterale sau multilaterale cu țările terțe respective și cu autoritățile competente ale acestora.

Aceste acorduri de cooperare specifică cel puțin următoarele elemente:

(a) procedurile privind coordonarea activităților de supraveghere desfășurate în temeiul prezentului regulament și orice monitorizare analoagă a riscurilor TIC generate de părți terțe în sectorul financiar efectuată de autoritatea relevantă din țara terță în cauză, inclusiv detaliile privind transmiterea acordului acesteia din urmă pentru a permite efectuarea, de către supraveghetorul principal și echipa desemnată de acesta, a investigațiilor generale și a inspecțiilor la fața locului menționate la alineatul (1) primul paragraf pe teritoriul aflat sub jurisdicția sa;

(b) mecanismul de transmitere a oricăror informații relevante între ABE, ESMA sau EIOPA și autoritatea relevantă din țara terță în cauză, în special în legătură cu informațiile care pot fi solicitate de supraveghetorul principal în temeiul articolului 37;

(c) mecanismele prin care se realizează notificarea promptă de către autoritatea relevantă din țara terță în cauză a ABE, ESMA sau EIOPA cu privire la cazurile în care se consideră că un furnizor terț de servicii TIC stabilit într-o țară terță și desemnat ca fiind esențial în conformitate cu articolul 31 alineatul (1) litera (a) a încălcat cerințele pe care este obligat să le respecte în temeiul dreptului aplicabil al țării terțe în cauză atunci când furnizează servicii unor instituții financiare din țara terță respectivă, precum și măsurile corective și sancțiunile aplicate;

(d) transmiterea periodică de informații actualizate privind evoluțiile în materie de reglementare sau de supraveghere în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe ale instituțiilor financiare din țara terță în cauză;

(e) detaliile pentru a permite, dacă este necesar, participarea unui reprezentant al autorității competente din țara terță la inspecțiile efectuate de supraveghetorul principal și de echipa desemnată.

(3) În cazul în care supraveghetorul principal nu este în măsură să desfășoare activitățile de supraveghere în afara Uniunii menționate la alineatele (1) și (2), supraveghetorul principal:

(a) își exercită competențele prevăzute la articolul 35 pe baza tuturor faptelor și documentelor de care dispune;

(b) documentează și explică orice consecință a imposibilității sale de a desfășura activitățile de supraveghere preconizate la care se referă prezentul articol.

Consecințele potențiale menționate la litera (b) de la prezentul alineat sunt luate în considerare în cadrul recomandărilor emise de supraveghetorul principal în temeiul articolului 35 alineatul (1) litera (d).

Articolul 37

Solicitarea de informații

(1) Supraveghetorul principal poate, printr-o simplă cerere sau printr-o decizie, să solicite furnizorilor terți esențiali de servicii TIC să furnizeze toate informațiile necesare pentru ca supraveghetorul principal să își îndeplinească sarcinile care îi revin în temeiul prezentului regulament, inclusiv toate documentele comerciale sau operaționale relevante, contractele, documentele de politică, rapoartele de audit privind securitatea TIC, rapoartele privind incidentele legate de TIC, precum și orice informații legate de părțile cărora furnizorul terț esențial de servicii TIC le-a externalizat funcții sau activități operaționale.

(2) Atunci când trimite o simplă solicitare de informații în temeiul alineatului (1), supraveghetorul principal:

(a) face trimitere la prezentul articol ca temei juridic al solicitării sale;

(b) menționează scopul solicitării;

(c) specifică informațiile care sunt solicitate;

(d) stabilește un termen pentru furnizarea informațiilor;

(e) informează reprezentantul furnizorului terț esențial de servicii TIC de la care sunt solicitate informațiile cu privire la faptul că acesta nu este obligat să furnizeze informațiile, dar că, în cazul unui răspuns voluntar la solicitare, informațiile furnizate nu trebuie să fie incorecte sau să inducă în eroare.

(3) Atunci când solicită printr-o decizie furnizarea de informații în temeiul alineatului (1), supraveghetorul principal:

(a) face trimitere la prezentul articol ca temei juridic al solicitării sale;

(b) menționează scopul solicitării;

(c) specifică informațiile care sunt solicitate;

(d) stabilește un termen pentru furnizarea informațiilor;

(e) indică penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6) în cazul în care informațiile solicitate sunt furnizate incomplet sau dacă aceste informații nu sunt furnizate în termenul menționat la litera (d) de la prezentul alineat;

(f) indică dreptul de a contesta decizia în fața comisiei de apel a AES și de a solicita controlul legalității deciziei de către Curtea de Justiție a Uniunii Europene (denumită în continuare „Curtea de Justiție"), în conformitate cu articolele 60 și 61 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

(4) Reprezentanții furnizorilor terți esențiali de servicii TIC furnizează informațiile solicitate. Avocații autorizați în mod corespunzător să acționeze pot furniza informațiile în numele clienților lor. Furnizorii terți esențiali de servicii TIC au în continuare întreaga responsabilitate în cazul în care informațiile furnizate sunt incomplete, incorecte sau induc în eroare.

(5) Supraveghetorul principal transmite fără întârziere o copie a deciziei prin care se solicită furnizarea de informații autorităților competente ale entităților financiare care folosesc serviciile furnizorilor terți esențiali de servicii TIC relevanți și RSC.

Articolul 38

Investigații generale

(1) Pentru a-și îndeplini sarcinile care îi revin în temeiul prezentului regulament, supraveghetorul principal, asistat de echipa de examinare comună menționată la articolul 40 alineatul (1), poate, atunci când este necesar, să efectueze investigații cu privire la furnizorii terți esențiali de servicii TIC.

(2) Supraveghetorul principal este abilitat:

(a) să analizeze evidențele, datele, procedurile și orice alte materiale relevante pentru executarea atribuțiilor sale, indiferent de suportul pe care sunt stocate;

(b) să facă sau să obțină copii certificate ale unor astfel de evidențe, date, documente care prevăd proceduri și ale oricăror alte materiale, precum și extrase din acestea;

(c) să convoace reprezentanții furnizorului terț esențial de servicii TIC pentru explicații verbale sau scrise cu privire la fapte sau documente referitoare la obiectul și scopul investigației și să înregistreze răspunsurile;

(d) să pună întrebări oricărei alte persoane fizice sau juridice care acceptă să i se pună întrebări în scopul colectării de informații referitoare la obiectul unei investigații;

(e) să solicite înregistrări ale convorbirilor telefonice și ale traficului de date.

(3) Funcționarii și celelalte persoane autorizate de supraveghetorul principal în scopul efectuării investigației menționate la alineatul (1) își exercită competențele pe baza prezentării unei autorizații scrise în care se specifică obiectul și scopul investigației.

Autorizația respectivă indică, de asemenea, penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6) aplicabile în cazul în care evidențele, datele, documentele care prevăd proceduri sau orice alte materiale solicitate sau răspunsurile la întrebările adresate reprezentanților furnizorului terț de servicii TIC nu sunt furnizate sau sunt incomplete.

(4) Reprezentanții furnizorilor terți esențiali de servicii TIC sunt obligați să se supună investigațiilor pe baza unei decizii a supraveghetorului principal. Decizia specifică obiectul și scopul investigației, penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6), căile de atac disponibile în temeiul Regulamentelor (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, precum și dreptul de a solicita controlul legalității deciziei de către Curtea de Justiție.

(5) În timp util înainte de începerea investigației, supraveghetorul principal informează autoritățile competente ale entităților financiare care utilizează serviciile TIC ale respectivului furnizor terț esențial de servicii TIC cu privire la investigația preconizată și la identitatea persoanelor autorizate.

Supraveghetorul principal comunică RSC toate informațiile primite în temeiul primului paragraf.

Articolul 39

Inspecții

(1) Pentru a-și îndeplini sarcinile care îi revin în temeiul prezentului regulament, supraveghetorul principal, asistat de echipele de examinare comună menționate la articolul 40 alineatul (1), poate să aibă acces la orice sediu comercial, teren sau proprietate a furnizorilor terți de servicii TIC, cum ar fi sediile sociale, centrele de operațiuni sau sediile secundare, și poate să efectueze toate inspecțiile la fața locului necesare, precum și să efectueze inspecții la distanță.

În scopul exercitării competențelor menționate la primul paragraf, supraveghetorul principal consultă RSC.

(2) Funcționarii și celelalte persoane autorizate de supraveghetorul principal să efectueze o inspecție la fața locului sunt abilitați:

(a) să intre în orice astfel de sediu comercial, teren sau proprietate; și

(b) să sigileze orice astfel de sediu comercial**,** registre sau evidențe**,** pe perioada inspecției și în măsura în care acest lucru este necesar pentru inspecție.

Funcționarii și celelalte persoane autorizate de supraveghetorul principal își exercită competențele pe baza prezentării unei autorizații scrise în care se specifică obiectul și scopul inspecției, precum și penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6) în cazul în care reprezentanții furnizorilor terți esențiali de servicii TIC în cauză nu se supun inspecției.

(3) În timp util înainte de începerea inspecției, supraveghetorul principal informează autoritățile competente ale entităților financiare care utilizează respectivul furnizor terț de servicii TIC.

(4) Inspecțiile acoperă întreaga gamă de sisteme TIC, rețele, dispozitive, informații și date relevante care sunt utilizate sau contribuie la furnizarea de servicii TIC către entități financiare.

(5) Înainte de orice inspecție la fața locului planificată, supraveghetorul principal le dă un preaviz rezonabil furnizorilor terți esențiali de servicii TIC, cu excepția cazului în care un astfel de preaviz nu este posibil din cauza unei situații de urgență sau de criză sau în cazul în care acesta ar conduce la o situație în care inspecția sau auditul nu ar mai fi eficace.

(6) Furnizorul terț esențial de servicii TIC se supune inspecțiilor la fața locului dispuse prin decizia supraveghetorului principal. Decizia specifică obiectul și scopul inspecției, stabilește data la care va începe inspecția și indică penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6), căile de atac disponibile în temeiul Regulamentelor (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, precum și dreptul de a solicita controlul legalității deciziei de către Curtea de Justiție.

(7) În cazul în care funcționarii și celelalte persoane autorizate de supraveghetorul principal constată că un furnizor terț esențial de servicii TIC se opune unei inspecții dispuse în temeiul prezentului articol, supraveghetorul principal informează furnizorul terț esențial de servicii TIC cu privire la consecințele unei astfel de opoziții, inclusiv cu privire la posibilitatea ca autoritățile competente ale entităților financiare relevante să solicite entităților financiare să înceteze acordurile contractuale încheiate cu respectivul furnizor terț esențial de servicii TIC.

Articolul 40

Supravegherea permanentă

(1) Atunci când desfășoară activități de supraveghere, în special investigații generale sau inspecții, supraveghetorul principal este asistat de o echipă de examinare comună, instituită pentru fiecare furnizor terț esențial de servicii TIC.

(2) Echipa de examinare comună menționată la alineatul (1) este formată din membri ai personalului:

(a) AES;

(b) autorităților competente relevante care supraveghează entitățile financiare cărora furnizorul terț esențial de servicii TIC le oferă servicii TIC;

(c) autorității naționale competente menționate la articolul 32 alineatul (4) litera (e), pe bază de voluntariat;

(d) unei autorități naționale competente din statul membru în care este stabilit furnizorul terț esențial de servicii TIC, pe bază de voluntariat.

Membrii echipei de examinare comună au cunoștințe de specialitate în domeniul TIC și în ceea ce privește riscurile operaționale. Echipa de examinare comună lucrează sub coordonarea unui membru desemnat al personalului supraveghetorului principal („coordonatorul supraveghetorului principal”).

(3) În termen de trei luni de la încheierea unei investigații sau a unei inspecții, supraveghetorul principal, după consultarea Forumului de supraveghere, adoptă recomandări care urmează a fi adresate furnizorului terț esențial de servicii TIC în temeiul competențelor menționate la articolul 35.

(4) Recomandările menționate la alineatul (3) se comunică imediat furnizorului terț esențial de servicii TIC și autorităților competente ale entităților financiare cărora acesta le furnizează servicii TIC.

În scopul executării activităților de supraveghere, supraveghetorul principal poate lua în considerare certificările relevante ale unei părți terțe și rapoartele de audit TIC intern sau extern ale unei părți terțe puse la dispoziție de furnizorul terț esențial de servicii TIC.

Articolul 41

Armonizarea condițiilor care permit desfășurarea activităților de supraveghere

(1) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a preciza:

(a) informațiile care trebuie furnizate de un furnizor terț de servicii TIC în cererea prin care solicită în mod voluntar să fie desemnați ca fiind esențiali în temeiul articolului 31 alineatul (11);

(b) conținutul, structura și formatul informațiilor care trebuie transmise, comunicate sau raportate de furnizorii terți de servicii TIC în temeiul articolului 35 alineatul (1), inclusiv modelul pentru furnizarea informațiilor privind acordurile de subcontractare;

(c) criteriile privind stabilirea componenței echipei de examinare comune, asigurând o participare echilibrată a membrilor personalului AES și a membrilor personalului autorităților competente relevante, precum și modul de desemnare, sarcinile și acordurile de lucru ale acestora;

(d) detaliile evaluării efectuate de autoritățile competente cu privire la măsurile luate de furnizorii terți esențiali de servicii TIC pe baza recomandărilor supraveghetorului principal în conformitate cu articolul 42 alineatul (3).

(2) AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la alineatul (1), în conformitate cu procedura prevăzută la articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

Articolul 42

Acțiunile ulterioare întreprinse de autoritățile competente

(1) În termen de 60 de zile calendaristice de la primirea recomandărilor emise de supraveghetorul principal în temeiul articolului 35 alineatul (1) litera (d), furnizorii terți esențiali de servicii TIC fie informează supraveghetorul principal cu privire la intenția lor de a urma recomandările, fie oferă o explicație cu privire la motivele pentru care nu vor urma recomandările respective. Supraveghetorul principal transmite imediat aceste informații autorităților competente ale entităților financiare în cauză.

(2) Supraveghetorul principal face publice cazurile în care un furnizor terț esențial de servicii TIC nu informează supraveghetorul principal în conformitate cu alineatul (1) sau cazurile în care explicația furnizată de furnizorul terț esențial de servicii TIC nu este considerată suficientă. Informațiile publicate dezvăluie identitatea furnizorului terț esențial de servicii TIC, precum și informații privind tipul și natura neconformității. Aceste informații se limitează la ceea ce este pertinent și proporțional în scopul asigurării informării publicului, cu excepția cazului în care această publicare ar cauza prejudicii disproporționate părților implicate sau ar putea periclita grav buna funcționare și integritatea piețelor financiare sau stabilitatea întregului sistem financiar al Uniunii sau a unei părți a acestuia.

Supraveghetorul principal informează furnizorul terț de servicii TIC cu privire la respectiva informare publică.

(3) Autoritățile competente informează entitățile financiare relevante cu privire la riscurile identificate în cadrul recomandărilor adresate furnizorilor terți esențiali de servicii TIC în conformitate cu articolul 35 alineatul (1) litera (d).

Atunci când gestionează riscuri TIC generate de părți terțe, entitățile financiare țin seama de riscurile menționate la primul paragraf.

(4) În cazul în care o autoritate competentă consideră că o entitate financiară, în cadrul activității sale de gestionare a riscurilor TIC generate de părți terțe, nu ține seama de riscurile specifice identificate în cadrul recomandărilor sau nu le contracarează suficient, aceasta notifică entitatea financiară cu privire la posibilitatea adoptării unei decizii, în termen de 60 de zile calendaristice de la primirea unei astfel de notificări, în temeiul alineatului (6), în lipsa unor acorduri contractuale adecvate care să aibă drept scop contracararea acestor riscuri.

(5) La primirea rapoartelor menționate la articolul 35 alineatul (1) litera (c) și înainte de a lua o decizie astfel cum se menționează la alineatul (6) de la prezentul articol, autoritățile competente pot, în mod voluntar, să consulte autoritățile competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC.

(6) Autoritățile competente pot, ca măsură de ultimă instanță, în urma informării și, dacă este cazul, a consultării prevăzute la alineatele (4) și (5) din prezentul articol, în conformitate cu articolul 50, să adopte o decizie prin care să solicite entităților financiare să suspende temporar, parțial sau integral, utilizarea sau implementarea unui serviciu furnizat de furnizorul terț esențial de servicii TIC până la contracararea riscurilor identificate în cadrul recomandărilor adresate furnizorilor terți esențiali de servicii TIC. În cazul în care este necesar, acestea pot solicita entităților financiare să rezilieze parțial sau integral acordurile contractuale relevante încheiate cu furnizorii terți esențiali de servicii TIC.

(7) În cazul în care un furnizor terț esențial de servicii TIC refuză să accepte recomandările în baza unei abordări divergente față de cea recomandată de supraveghetorul principal, și o astfel de abordare divergentă ar putea avea un impact negativ asupra unui număr mare de entități financiare sau asupra unei părți semnificative a sectorului financiar, iar avertismentele individuale emise de autoritățile competente nu au avut drept rezultat abordări coerente care să atenueze riscul potențial la adresa stabilității financiare, supraveghetorul principal poate, după consultarea Forumului de supraveghere, să emită avize neobligatorii și fără caracter public adresate autorităților competente, pentru a promova măsuri ulterioare de supraveghere coerente și convergente, după caz.

(8) La primirea rapoartelor menționate la articolul 35 alineatul (1) litera (c), autoritățile competente, atunci când iau o decizie în conformitate cu alineatul (6) de la prezentul articol, țin seama de tipul și de amploarea riscului care nu a fost contracarat de furnizorul terț esențial de servicii TIC, precum și de gravitatea neconformității, având în vedere următoarele criterii:

(a) gravitatea și durata neconformității;

(b) dacă neconformitatea a evidențiat deficiențe grave în ceea ce privește procedurile, sistemele de gestionare, gestionarea riscurilor și controalele interne ale furnizorului terț esențial de servicii TIC;

(c) dacă prin neconformitate a fost facilitată sau ocazionată o infracțiune financiară sau dacă aceasta este imputabilă în alt mod neconformității;

(d) dacă neconformitatea a fost intenționată sau este rezultatul unei neglijențe;

(e) dacă suspendarea sau încetarea acordurilor contractuale dă naștere unui risc la adresa continuității activităților economice ale entității financiare în pofida eforturilor acesteia de a evita perturbarea furnizării serviciilor sale;

(f) după caz, avizul autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC, aviz solicitat în mod voluntar în conformitate cu alineatul (5) de la prezentul articol.

Autoritățile competente le acordă entităților financiare perioada de timp necesară pentru a le permite să adapteze acordurile contractuale cu furnizorii terți esențiali de servicii TIC pentru a evita apariția unor efecte negative asupra rezilienței lor operaționale digitale și pentru a le permite să implementeze strategiile de ieșire și planurile de tranziție, astfel cum sunt menționate la articolul 28.

(9) Decizia menționată la alineatul (6) de la prezentul articol se notifică membrilor Forumului de supraveghere menționat la articolul 32 alineatul (4) literele (a), (b) și (c) și RSC.

Furnizorii terți esențiali de servicii TIC vizați de deciziile prevăzute la alineatul (6) cooperează pe deplin cu entitățile financiare afectate, în special în contextul procesului de suspendare sau de încetare a acordurilor lor contractuale.

(10) Autoritățile competente informează periodic supraveghetorul principal cu privire la abordările urmate și măsurile luate în cadrul atribuțiilor lor de supraveghere în ceea ce privește entitățile financiare, precum și cu privire la acordurile contractuale încheiate de entitățile financiare în cazul în care furnizorii terți esențiali de servicii TIC nu au acceptat, parțial sau în întregime, recomandările adresate de supraveghetorul principal.

(11) Supraveghetorul principal poate, la cerere, să furnizeze clarificări suplimentare cu privire la recomandările emise pentru a îndruma autoritățile competente cu privire la măsurile ulterioare.

Articolul 43

Taxele de supraveghere

(1) În conformitate cu actul delegat menționat la alineatul (2) de la prezentul articol, supraveghetorul principal percepe de la furnizorii terți esențiali de servicii TIC taxe care acoperă integral cheltuielile necesare ale supraveghetorului principal în legătură cu îndeplinirea atribuțiilor de supraveghere în temeiul prezentului regulament, inclusiv rambursarea oricăror costuri care ar putea fi suportate ca urmare a activității desfășurate de echipa de examinare comună prevăzută la articolul 40, precum și a costurilor aferente consultanței furnizate de experții independenți menționați la articolul 32 alineatul (4) al doilea paragraf, în legătură cu aspecte care intră în sfera activităților de supraveghere directă.

Cuantumul unei taxe percepute de la un furnizor terț esențial de servicii TIC acoperă toate costurile care decurg din efectuarea sarcinilor stabilite în prezenta secțiune și este proporțional cu cifra sa de afaceri.

(2) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 57 pentru a completa prezentul regulament prin stabilirea cuantumului taxelor și a modalității de plată a acestora, până la 17 iulie 2024.

Articolul 44

Cooperarea internațională

(1) Fără a aduce atingere articolului 36, ABE, ESMA și EIOPA pot, în conformitate cu articolul 33 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010, să încheie acorduri administrative cu autorități de reglementare și de supraveghere din țări terțe pentru a încuraja cooperarea internațională cu privire la riscurile TIC generate de părți terțe în diferite sectoare financiare, în special prin elaborarea de bune practici pentru revizuirea practicilor de gestionare a riscurilor TIC și a controalelor aferente, a măsurilor de atenuare și a răspunsurilor la incidente.

(2) AES transmit, prin intermediul Comitetului comun, o dată la cinci ani, un raport confidențial comun Parlamentului European, Consiliului și Comisiei, în care sintetizează constatările discuțiilor relevante purtate cu autoritățile țărilor terțe menționate la alineatul (1), axându-se pe evoluția riscurilor TIC generate de părți terțe și pe implicațiile pentru stabilitatea financiară, integritatea pieței, protecția investitorilor și funcționarea pieței interne.

CAPITOLUL VI

Acorduri privind schimbul de informații

Articolul 45

Acorduri privind schimbul de informații referitoare la informații și date operative privind amenințările cibernetice

(1) Entitățile financiare pot face schimb reciproc de informații și date operative privind amenințările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în măsura în care aceste schimburi de informații și date operative:

(a) vizează sporirea rezilienței operaționale digitale a entităților financiare, în special prin creșterea gradului de conștientizarea cu privire la amenințările cibernetice, limitarea sau împiedicarea capacității de propagare a amenințărilor cibernetice, sprijinirea capacităților de apărare, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare;

(b) au loc în cadrul unor comunități de încredere ale entităților financiare;

(c) sunt puse în aplicare prin intermediul unor acorduri privind schimbul de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin secretul comercial, protecția datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 și orientările privind politica în domeniul concurenței.

(2) În scopul aplicării alineatului (1) litera (c), acordurile privind schimbul de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea autorităților publice și calitatea în care acestea pot fi asociate la acordurile privind schimbul de informații, implicarea furnizorilor terți de servicii TIC și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.

(3) Entitățile financiare informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații menționate la alineatul (1), în momentul validării sau, după caz, al încetării participării lor, odată ce aceasta începe să producă efecte.

CAPITOLUL VII

Autoritățile competente

Articolul 46

Autoritățile competente

Fără a aduce atingere dispozițiilor privind cadrul de supraveghere pentru furnizorii terți esențiali de servicii TIC menționat în capitolul V secțiunea II din prezentul regulament, respectarea prezentului regulament este asigurată de următoarele autorități competente în conformitate cu prerogativele conferite prin actele juridice respective:

(a) pentru instituțiile de credit și pentru instituțiile exceptate în temeiul Directivei 2013/36/UE, autoritatea competentă desemnată în conformitate cu articolul 4 din directiva respectivă, iar pentru instituțiile de credit clasificate ca fiind semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, BCE, în conformitate cu competențele și atribuțiile conferite prin regulamentul respectiv;

(b) pentru instituțiile de plată, inclusiv instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366, instituțiile emitente de monedă electronică, inclusiv cele exceptate în temeiul Directivei 2009/110/CE, și prestatorii de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366, autoritatea competentă desemnată în conformitate cu articolul 22 din Directiva (UE) 2015/2366;

(c) pentru firmele de investiții, autoritatea competentă desemnată în conformitate cu articolul 4 din Directiva (UE) 2019/2034 a Parlamentului European și a Consiliului ([38]);

(d) pentru furnizorii de servicii de criptoactive autorizați în temeiul Regulamentului privind piețele criptoactivelor și pentru emitenții de tokenuri raportate la active, autoritatea competentă desemnată în conformitate cu dispozițiile relevante din regulamentul respectiv;

(e) pentru depozitarii centrali de titluri de valoare, autoritatea competentă desemnată în conformitate cu articolul 11 din Regulamentul (UE) nr. 909/2014;

(f) pentru contrapărțile centrale, autoritatea competentă desemnată în conformitate cu articolul 22 din Regulamentul (UE) nr. 648/2012;

(g) pentru locurile de tranzacționare și furnizorii de servicii de raportare a datelor, autoritatea competentă desemnată în conformitate cu articolul 67 din Directiva 2014/65/UE și autoritatea competentă definită la articolul 2 alineatul (1) punctul 18 din Regulamentul (UE) nr. 600/2014;

(h) pentru registrele centrale de tranzacții, autoritatea competentă desemnată în conformitate cu articolul 22 din Regulamentul (UE) nr. 648/2012;

(i) pentru administratorii de fonduri de investiții alternative, autoritatea competentă desemnată în conformitate cu articolul 44 din Directiva 2011/61/UE;

(j) pentru societățile de administrare, autoritatea competentă desemnată în conformitate cu articolul 97 din Directiva 2009/65/CE;

(k) pentru întreprinderile de asigurare și de reasigurare, autoritatea competentă desemnată în conformitate cu articolul 30 din Directiva 2009/138/CE;

(l) pentru intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare, autoritatea competentă desemnată în conformitate cu articolul 12 din Directiva (UE) 2016/97;

(m) pentru instituțiile pentru furnizarea de pensii ocupaționale, autoritatea competentă desemnată în conformitate cu articolul 47 din Directiva (UE) 2016/2341;

(n) pentru agențiile de rating de credit, autoritatea competentă desemnată în conformitate cu articolul 21 din Regulamentul (CE) nr. 1060/2009;

(o) pentru administratorii de indici de referință critici, autoritatea competentă desemnată în conformitate cu articolele 40 și 41 din Regulamentul (UE) 2016/1011;

([38]) Directiva (UE) 2019/2034 a Parlamentului European și a Consiliului din 27 noiembrie 2019 privind supravegherea prudențială a firmelor de investiții și de modificare a Directivelor 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE și 2014/65/UE (JO L 314, 5.12.2019, p. 64).

(p) pentru furnizorii de servicii de finanțare participativă, autoritatea competentă desemnată în conformitate cu articolul 29 din Regulamentul (UE) 2020/1503;

(q) pentru registrele centrale de securitizări, autoritatea competentă desemnată în conformitate cu articolul 10 și cu articolul 14 alineatul (1) din Regulamentul (UE) 2017/2402.

Articolul 47

Cooperarea cu structurile și autoritățile înființate prin Directiva (UE) 2022/2555

(1) Pentru a încuraja cooperarea și a permite schimburile de informații în scopuri de supraveghere între autoritățile competente desemnate în temeiul prezentului regulament și Grupul de cooperare instituit prin articolul 14 din Directiva (UE) 2022/2555, AES și autoritățile competente pot participa la activitățile Grupului de cooperare în ceea ce privește chestiuni care privesc activitățile lor de supraveghere în legătură cu entitățile financiare. AES și autoritățile competente pot solicita să fie invitate să participe la activitățile Grupului de cooperare cu privire la chestiuni legate de entitățile esențiale sau importante cărora li se aplică Directiva (UE) 2022/2555 și care au fost, de asemenea, desemnate drept furnizori terți esențiali de servicii TIC în temeiul articolului 31 din prezentul regulament.

(2) După caz, autoritățile competente se pot consulta și pot face schimb de informații cu punctele unice de contact și cu echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.

(3) După caz, autoritățile competente pot solicita orice tip de consultanță și asistență tehnică relevantă din partea autorităților competente desemnate sau stabilite în conformitate cu Directiva (UE) 2022/2555 și pot stabili acorduri de cooperare pentru a permite crearea unor mecanisme de coordonare eficace și rapide.

(4) Acordurile menționate la alineatul (3) de la prezentul articol pot specifica, printre altele, procedurile pentru coordonarea activităților de supraveghere și, respectiv, de control în ceea ce privește entitățile esențiale sau importante cărora li se aplică Directiva (UE) 2022/2555 și care au fost desemnate drept furnizori terți esențiali de servicii TIC în temeiul articolului 31 din prezentul regulament, inclusiv pentru efectuarea, în conformitate cu dreptul intern, a investigațiilor și a inspecțiilor la fața locului, precum și pentru mecanismele privind schimbul de informații dintre autoritățile competente în temeiul prezentului regulament și autoritățile competente desemnate sau stabilite în conformitate cu directiva respectivă, care include accesul la informațiile solicitate de autoritățile din urmă.

Articolul 48

Cooperarea între autorități

(1) Autoritățile competente cooperează îndeaproape între ele și, după caz, cu supraveghetorul principal.

(2) Autoritățile competente și supraveghetorul principal își transmit reciproc, în timp util, toate informațiile relevante privind furnizorii terți esențiali de servicii TIC care sunt necesare pentru îndeplinirea sarcinilor care le revin în temeiul prezentului regulament, în special în legătură cu riscurile identificate, cu abordările și cu măsurile adoptate în cadrul sarcinilor de supraveghere ale supraveghetorului principal.

Articolul 49

Exerciții, comunicare și cooperare transsectoriale în domeniul financiar

(1) AES, prin intermediul Comitetului comun și în colaborare cu autoritățile competente, cu autoritățile de rezoluție menționate la articolul 3 din Directiva 2014/59/UE, cu BCE, cu Comitetul unic de rezoluție în ceea ce privește informațiile referitoare la entitățile care intră sub incidența Regulamentului (UE) nr. 806/2014**,** cu CERS și cu ENISA, după caz, pot stabili mecanisme care să permită schimbul de practici eficace între sectoarele financiare în vederea îmbunătățirii gradului de conștientizare a situației și a identificării vulnerabilităților și riscurilor cibernetice comune la nivelul tuturor sectoarelor.

Acestea pot elabora exerciții de gestionare a crizelor și pentru situații neprevăzute care implică scenarii de atacuri cibernetice, cu scopul de a dezvolta canale de comunicare și de a permite treptat un răspuns coordonat eficace la nivelul UE în cazul unui incident transfrontalier major legat de TIC sau al unei amenințări conexe cu un impact sistemic asupra sectorului financiar al Uniunii în ansamblu.

Exercițiile respective pot, după caz, să testeze și dependențele sectorului financiar de alte sectoare economice.

(2) Autoritățile competente, AES și BCE cooperează strâns și fac schimb de informații pentru a-și îndeplini atribuțiile prevăzute la articolele 47-54. Acestea își coordonează îndeaproape activitățile de supraveghere pentru a identifica și a remedia cazurile de nerespectare a prezentului regulament, pentru a elabora și a promova bune practici, a facilita colaborarea, a stimula consecvența interpretării și a furniza evaluări interjurisdicționale în cazul oricăror neînțelegeri.

Articolul 50

Sancțiuni administrative și măsuri de remediere

(1) Autoritățile competente dispun de toate competențele de supraveghere, de investigare și de sancționare necesare pentru a-și îndeplini atribuțiile în conformitate cu prezentul regulament.

(2) Competențele menționate la alineatul (1) includ cel puțin următoarele:

(a) competența de a avea acces la orice document sau date deținute sub orice formă pe care autoritatea competentă le consideră relevante pentru îndeplinirea sarcinilor sale și competența de a primi sau de a face o copie a acestora;

(b) competența de a efectua inspecții la fața locului sau investigații, incluzând, printre altele, următoarele activități:

(i) convocarea reprezentanților entităților financiare pentru explicații verbale sau scrise cu privire la fapte sau documente referitoare la obiectul și scopul investigației și înregistrarea răspunsurilor;

(ii) punerea de întrebări oricărei alte persoane fizice sau juridice care acceptă să i se pună întrebări în scopul colectării de informații referitoare la obiectul unei investigații;

(c) competența de a solicita măsuri corective și de remediere pentru încălcările cerințelor prezentului regulament.

(3) Fără a aduce atingere dreptului statelor membre de a impune sancțiuni penale în conformitate cu articolul 52, statele membre prevăd norme de stabilire a sancțiunilor administrative și a măsurilor de remediere corespunzătoare pentru încălcările prezentului regulament și asigură punerea lor efectivă în aplicare.

Aceste sancțiuni și măsuri sunt eficace, proporționale și disuasive.

(4) Statele membre conferă autorităților competente competența de a aplica cel puțin următoarele sancțiuni administrative sau măsuri de remediere în cazul încălcării prezentului regulament:

(a) emiterea unei dispoziții prin care i se cere persoanei fizice sau juridice să înceteze comportamentul care încalcă prezentul regulament și să se abțină de la repetarea comportamentului respectiv;

(b) solicitarea încetării temporare sau permanente a oricărei practici sau a oricărui comportament în legătură cu care autoritatea competentă consideră că contravine dispozițiilor prezentului regulament și prevenirea repetării practicii sau a comportamentului în cauză;

(c) adoptarea oricărui tip de măsură, inclusiv de natură pecuniară, pentru a asigura că entitățile financiare respectă în continuare cerințele legale;

(d) solicitarea, în măsura în care dreptul intern permite acest lucru, a unor înregistrări existente ale schimburilor de date deținute de un operator de telecomunicații, atunci când există o suspiciune rezonabilă privind o încălcare a prezentului regulament și atunci când aceste înregistrări pot fi relevante pentru o investigație referitoare la încălcări ale prezentului regulament; și

(e) emiterea unor anunțuri publice, inclusiv a unor declarații publice care indică identitatea persoanei fizice sau juridice și natura încălcării.

(5) Atunci când alineatul (2) litera (c) și alineatul (4) se aplică unor persoane juridice, statele membre conferă autorităților competente competența de a aplica sancțiunile administrative și măsurile de remediere, sub rezerva condițiilor prevăzute în dreptul intern, membrilor organului de conducere, precum și altor persoane care, în temeiul dreptului intern, sunt responsabile de încălcare.

(6) Statele membre se asigură că orice decizie de impunere a unor sancțiuni administrative sau a unor măsuri de remediere prevăzute la alineatul (2) litera (c) este justificată în mod corespunzător și face obiectul unei căi de atac.

Articolul 51

Exercitarea competenței de a impune sancțiuni administrative și măsuri de remediere

(1) Autoritățile competente își exercită competențele de a impune sancțiunile administrative și măsurile de remediere menționate la articolul 50 în conformitate cu cadrele lor juridice naționale, dacă este cazul, după cum urmează:

(a) în mod direct;

(b) în colaborare cu alte autorități;

(c) sub responsabilitate proprie prin delegare către alte autorități; sau

(d) prin sesizarea autorităților judiciare competente.

(2) La stabilirea tipului și a nivelului unei sancțiuni administrative sau al unei măsuri de remediere care urmează să fie impuse în temeiul articolului 50, autoritățile competente iau în considerare măsura în care încălcarea este intenționată sau rezultă din neglijență și toate celelalte circumstanțe relevante, inclusiv, după caz, următoarele elemente:

(a) importanța semnificativă, gravitatea și durata încălcării;

(b) gradul de responsabilitate al persoanei fizice sau juridice responsabile de încălcare;

(c) soliditatea financiară a persoanei fizice sau juridice responsabile;

(d) importanța profiturilor obținute sau a pierderilor evitate de către persoana fizică sau juridică responsabilă, în măsura în care acestea pot fi determinate;

(e) pierderile suferite de terți în urma respectivei încălcări, în măsura în care acestea pot fi determinate;

(f) nivelul de cooperare cu autoritatea competentă a persoanei fizice sau juridice responsabile, fără a aduce atingere necesității de a asigura confiscarea profiturilor obținute sau a pierderilor evitate de persoana fizică sau juridică respectivă;

(g) încălcările anterioare comise de persoana fizică sau juridică responsabilă.

Articolul 52

Sancțiuni penale

(1) Statele membre pot decide să nu stabilească norme privind sancțiunile administrative sau măsurile de remediere în cazul încălcărilor care fac obiectul sancțiunilor penale în dreptul lor intern.

(2) În cazul în care statele membre au ales să prevadă sancțiuni penale pentru încălcările prezentului regulament, acestea se asigură că sunt instituite măsuri adecvate astfel încât autoritățile competente să dispună de toate competențele necesare pentru a asigura legătura cu autoritățile judiciare, de urmărire penală sau autoritățile judiciare penale din jurisdicția lor pentru a primi informații specifice referitoare la anchete sau proceduri penale inițiate pentru încălcarea prezentului regulament, precum și pentru a furniza aceleași informații altor autorități competente, precum și ABE, ESMA sau EIOPA astfel încât să își îndeplinească obligațiile de cooperare în scopul aplicării prezentului regulament.

Articolul 53

Obligații de notificare

Statele membre notifică actele cu putere de lege și actele administrative de punere în aplicare a prezentului capitol, inclusiv orice dispoziții relevante de drept penal, Comisiei, ESMA, ABE și EIOPA până la 17 ianuarie 2025. Statele membre înștiințează fără întârzieri nejustificate Comisia, ESMA, ABE și EIOPA cu privire la orice modificare ulterioară a acestor acte.

Articolul 54

Publicarea sancțiunilor administrative

(1) Autoritățile competente publică pe site-urile lor internet oficiale, fără întârzieri nejustificate, orice decizie de impunere a unei sancțiuni administrative care nu face obiectul niciunei căi de atac după notificarea destinatarului sancțiunii cu privire la decizia respectivă.

(2) Publicarea menționată la alineatul (1) include informații privind tipul și natura încălcării, identitatea persoanelor responsabile și sancțiunile impuse.

(3) În cazul în care autoritatea competentă, în urma unei evaluări de la caz la caz, consideră că publicarea identității, în cazul persoanelor juridice, sau a identității și a datelor cu caracter personal, în cazul persoanelor fizice, ar fi disproporționată, comportând riscuri cu privire la protecția datelor cu caracter personal, ar pune în pericol stabilitatea piețelor financiare sau desfășurarea unei anchete penale în curs sau ar cauza, în măsura în care acestea pot fi determinate, prejudicii disproporționate persoanei implicate, aceasta adoptă una dintre următoarele soluții în ceea ce privește decizia de impunere a unei sancțiuni administrative:

(a) amână publicarea sa până când toate motivele pentru nepublicare încetează;

(b) publică decizia menținând anonimatul persoanei în cauză, în conformitate cu dreptul intern; sau

(c) se abține de la publicarea acesteia, în cazul în care opțiunile prevăzute la literele (a) și (b) sunt considerate insuficiente pentru a garanta lipsa oricărui pericol pentru stabilitatea piețelor financiare sau în cazul în care o astfel de publicare nu ar fi proporțională cu clemența sancțiunii impuse.

(4) În cazul unei decizii de a publica sancțiunea administrativă menținând anonimatul persoanei în cauză în conformitate cu alineatul (3) litera (b), publicarea datelor relevante poate fi amânată.

(5) Dacă o autoritate competentă publică o decizie de impunere a unei sancțiuni administrative care face obiectul unei căi de atac în fața autorităților judiciare relevante, autoritățile competente includ imediat pe site-ul lor internet oficial această informație și, ulterior, orice informații conexe ulterioare cu privire la rezultatul căii de atac. Se publică, de asemenea, hotărârile judecătorești care anulează deciziile de impunere a unei sancțiuni administrative.

(6) Autoritățile competente se asigură că orice publicare menționată la alineatele (1)-(4) rămâne pe site-ul lor internet oficial numai pe perioada care este necesară pentru ca prezentul articol să își producă efectele. Această perioadă nu poate depăși cinci ani de la data publicării.

Articolul 55

Secretul profesional

(1) Informațiile confidențiale primite, schimbate sau transmise în temeiul prezentului regulament fac obiectul condițiilor privind respectarea secretului profesional prevăzute la alineatul (2).

(2) Obligația de păstrare a secretului profesional se aplică tuturor persoanelor care lucrează sau care au lucrat pentru autoritățile competente în temeiul prezentului regulament sau pentru orice autoritate, întreprindere de pe piață sau persoană fizică ori juridică căreia respectivele autorități competente i-au delegat competențele lor, inclusiv auditorilor și experților contractați de acestea.

(3) Informațiile care fac obiectul secretului profesional, inclusiv schimbul de informații între autoritățile competente în temeiul prezentului regulament și autoritățile competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555, nu se comunică niciunei alte persoane sau autorități, cu excepția cazului în care acest lucru este prevăzut de dreptul Uniunii sau de dreptul intern.

(4) Toate informațiile care fac obiectul unor schimburi între autoritățile competente în temeiul prezentului regulament și care privesc condițiile comerciale sau operaționale și alte chestiuni economice sau personale sunt considerate confidențiale și intră sub incidența obligației referitoare la secretul profesional, cu excepția cazului în care autoritatea competentă precizează, la momentul comunicării, că informațiile respective pot fi divulgate sau a cazului în care divulgarea acestora este necesară pentru desfășurarea unei proceduri judiciare.

Articolul 56

Protecția datelor

(1) AES și autoritățile competente sunt autorizate să prelucreze date cu caracter personal numai în cazul în care acest lucru este necesar în scopul îndeplinirii obligațiilor și sarcinilor care le revin în temeiul prezentului regulament, în special în ceea ce privește investigarea, realizarea de inspecții, solicitarea de informații, comunicarea, publicarea, evaluarea, verificarea, evaluarea și elaborarea de planuri de supraveghere. Datele cu caracter personal se prelucrează în conformitate cu Regulamentul (UE) 2016/679 sau cu Regulamentul (UE) 2018/1725, în funcție de care dintre acestea este aplicabil.

(2) Cu excepția cazului în care se prevede altfel în alte acte sectoriale, datele cu caracter personal menționate la alineatul (1) se păstrează până la îndeplinirea atribuțiilor de supraveghere aplicabile și, în orice caz, pentru o perioadă maximă de 15 ani, cu excepția cazului în care o procedură judiciară în curs necesită păstrarea acestor date pentru o perioadă mai lungă.

CAPITOLUL VIII

Acte delegate

Articolul 57

Exercitarea delegării de competențe

(1) Se conferă Comisiei competența de a adopta acte delegate, cu respectarea condițiilor stabilite la prezentul articol.

(2) Competența de a adopta acte delegate menționată la articolul 31 alineatul (6) și la articolul 43 alineatul (2) se conferă Comisiei pe o perioadă de cinci ani de la 17 ianuarie 2024. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată la articolul 31 alineatul (6) și la articolul 43 alineatul (2) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării competenței specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 31 alineatul (6) și al articolului 43 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de trei luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.

CAPITOLUL IX

Dispoziții tranzitorii și finale

Secțiunea I

Articolul 58

Clauza de reexaminare

(1) Până la 17 ianuarie 2028, după ce se consultă cu AES și CERS, după caz, Comisia efectuează o reexaminare și prezintă un raport Parlamentului European și Consiliului, însoțit, dacă este cazul, de o propunere legislativă. Reexaminarea include cel puțin următoarele aspecte:

(a) criteriile pentru desemnarea furnizorilor terți esențiali de servicii TIC în conformitate cu articolul 31 alineatul (2);

(b) caracterul voluntar al notificării amenințărilor cibernetice semnificative menționat la articolul 19;

(c) regimul menționat la articolul 31 alineatul (12) și competențele supraveghetorului principal prevăzute la articolul 35 alineatul (1) litera (d) punctul (iv) prima liniuță, în vederea evaluării eficacității dispozițiilor respective în ceea ce privește asigurarea unei supravegheri eficace a furnizorilor terți esențiali de servicii TIC stabiliți într-o țară terță și necesitatea de a înființa o filială în Uniune.

În scopul aplicării primului paragraf de la prezenta literă, reexaminarea include o analiză a regimului menționat la articolul 31 alineatul (12), inclusiv a condițiilor de acces al entităților financiare din Uniune la servicii din țări terțe și a disponibilității unor astfel de servicii pe piața Uniunii, și ține seama de evoluția piețelor serviciilor care fac obiectul prezentului regulament, de experiența practică a entităților financiare și a supraveghetorilor financiari în ceea ce privește aplicarea și, respectiv, supravegherea regimului respectiv, precum și de orice evoluții relevante în materie de reglementare și de supraveghere care au loc la nivel internațional;

(d) oportunitatea includerii în domeniul de aplicare al prezentului regulament a entităților financiare menționate la articolul 2 alineatul (3) litera (e) care recurg la sisteme de vânzări automatizate, ținând seama de evoluțiile viitoare ale pieței în ceea ce privește utilizarea unor astfel de sisteme;

(e) funcționarea și eficacitatea RSC în ceea ce privește sprijinirea coerenței supravegherii și a eficienței schimbului de informații în interiorul cadrului de supraveghere.

(2) În contextul reexaminării Directivei (UE) 2015/2366, Comisia evaluează necesitatea unei mai mari reziliențe cibernetice a sistemelor de plăți și a activităților de prelucrare a plăților, precum și oportunitatea extinderii domeniului de aplicare al prezentului regulament la operatorii sistemelor de plată și la entitățile implicate în activitățile de prelucrare a plăților. În lumina acestei evaluări, Comisia prezintă Parlamentului European și Consiliului, în cadrul reexaminării Directivei (UE) 2015/2366, un raport până cel târziu la 17 iulie 2023.

Pe baza respectivului raport de reexaminare și după consultarea AES, BCE și CERS, Comisia poate prezenta, dacă este cazul și ca parte a propunerii legislative pe care o poate adopta în temeiul articolului 108 al doilea paragraf din Directiva (UE) 2015/2366, o propunere urmărind să asigure faptul că toți operatorii sistemelor de plată și entitățile implicate în activitățile de prelucrare a plăților fac obiectul unei supravegheri adecvate, ținând seama în același timp de supravegherea existentă din partea băncilor centrale.

(3) Până la 17 ianuarie 2026, după consultarea AES și a Comitetului Organismelor Europene de Supraveghere a Auditului, Comisia efectuează o reexaminare și prezintă Parlamentului European și Consiliului un raport, însoțit, după caz, de o propunere legislativă, cu privire la oportunitatea unor cerințe mai stricte pentru auditorii statutari și firmele de audit în ceea ce privește reziliența operațională digitală, prin includerea auditorilor statutari și a firmelor de audit în domeniul de aplicare al prezentului regulament sau prin intermediul unor modificări ale Directivei 2006/43/CE a Parlamentului European și a Consiliului ([39]).

Secțiunea II

Modificări

Articolul 59

Modificarea Regulamentului (CE) nr. 1060/2009

Regulamentul (CE) nr. 1060/2009 se modifică după cum urmează:

1. În anexa I secțiunea A punctul 4, primul paragraf se înlocuiește cu următorul text:

„Agenția de rating de credit dispune de proceduri contabile și administrative sigure, de mecanisme de control intern, de tehnici eficiente de evaluare a riscurilor și de dispozitive eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

2. În anexa III, punctul 12 se înlocuiește cu următorul text:

„12. Agenția de rating de credit încalcă articolul 6 alineatul (2), coroborat cu punctul 4 din anexa I secțiunea A, prin faptul că nu dispune de proceduri contabile sau administrative sigure, de mecanisme de control intern, de proceduri eficiente de evaluare a riscurilor sau de dispozitive eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 sau prin faptul că nu pune în aplicare sau nu menține proceduri decizionale ori structuri organizaționale în conformitate cu punctul respectiv.”

Articolul 60

Modificarea Regulamentului (UE) nr. 648/2012

Regulamentul (UE) nr. 648/2012 se modifică după cum urmează:

1. Articolul 26 se modifică după cum urmează:

(a) alineatul (3) se înlocuiește cu următorul text:

„(3) CPC mențin și utilizează o structură organizatorică adecvată pentru a le asigura continuitatea și funcționarea corespunzătoare în cursul prestării serviciilor și al desfășurării activităților. Ele utilizează sisteme, resurse și proceduri adecvate și proporționale, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”;

([39]) Directiva 2006/43/CE a Parlamentului European și a Consiliului din 17 mai 2006 privind auditul legal al conturilor anuale și al conturilor consolidate, de modificare a Directivelor 78/660/CEE și 83/349/CEE ale Consiliului și de abrogare a Directivei 84/253/CEE a Consiliului (JO L 157, 9.6.2006, p. 87).

(b) alineatul (6) se elimină.

2. Articolul 34 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) CPC prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite și puse în aplicare în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura conservarea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor.";

(b) la alineatul (3), primul paragraf se înlocuiește cu următorul text:

„(3) Pentru a asigura aplicarea consecventă a prezentului articol, ESMA, după consultarea membrilor SEBC, elaborează proiecte de standarde tehnice de reglementare în care precizează conținutul și cerințele minime ale politicii de continuitate a activității și ale planului de recuperare în caz de dezastru, excluzând politica de continuitate a activității TIC și planurile de recuperare în caz de dezastru în domeniul TIC."

3. La articolul 56 alineatul (3), primul paragraf se înlocuiește cu următorul text:

„(3) Pentru a asigura aplicarea consecventă a prezentului articol, ESMA elaborează proiecte de standarde tehnice de reglementare în care precizează detaliile, altele decât cele pentru cerințele legate de gestionarea riscurilor TIC, ale cererii de înregistrare menționate la alineatul (1)."

4. La articolul 79, alineatele (1) și (2) se înlocuiesc cu următorul text:

„(1) Registrele centrale de tranzacții identifică sursele de risc operațional și le reduc la minimum și prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554.

(2) Registrele centrale de tranzacții prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura menținerea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor."

5. La articolul 80, alineatul (1) se elimină.

6. În anexa I, secțiunea II se modifică după cum urmează:

(a) literele (a) și (b) se înlocuiesc cu următorul text:

„(a) un registru central de tranzacții încalcă articolul 79 alineatul (1) dacă nu identifică sursele de risc operațional și nu reduce la minimum riscurile respective prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554;

(b) un registru central de tranzacții încalcă articolul 79 alineatul (2) dacă nu prevede, nu aplică sau nu menține o politică adecvată de continuitate a activității și un plan adecvat de redresare în caz de dezastru instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura menținerea funcțiilor sale, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor;";

(b) litera (c) se elimină.

7. Anexa III se modifică după cum urmează:

(a) secțiunea II se modifică după cum urmează:

(i) litera (c) se înlocuiește cu următorul text:

„(c) CPC de nivel 2 încalcă articolul 26 alineatul (3) dacă nu mențin sau nu utilizează o structură organizatorică care să asigure continuitatea și funcționarea corespunzătoare în cursul prestării serviciilor și al desfășurării activităților lor sau dacă nu utilizează sisteme, resurse sau proceduri adecvate și proporționale, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554";

(ii) litera (f) se elimină;

(b) în secțiunea III, litera (a) se înlocuiește cu următorul text:

„(a) CPC de nivel 2 încalcă articolul 34 alineatul (1) dacă nu prevăd, aplică sau mențin o politică adecvată de continuitate a activității și un plan adecvat de răspuns și de recuperare instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura conservarea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor CPC, care să permită cel puțin reluarea tuturor tranzacțiilor aflate în curs în momentul întreruperii, astfel încât CPC să poată continua să funcționeze în condiții de certitudine și să efectueze decontarea la data stabilită;”.

Articolul 61

Modificarea Regulamentului (UE) nr. 909/2014

Articolul 45 din Regulamentul (UE) nr. 909/2014 se modifică după cum urmează:

1. Alineatul (1) se înlocuiește cu următorul text:

„(1) CSD-urile identifică sursele de riscuri operaționale, atât interne, cât și externe, și reduc la minimum impactul acestora și prin implementarea unor instrumente, procese și politici TIC adecvate, instituite și gestionate în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*), precum și prin orice alte instrumente, mecanisme de control și proceduri adecvate relevante pentru alte tipuri de riscuri operaționale, inclusiv pentru toate sistemele de decontare a titlurilor de valoare pe care le exploatează.

_____

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

2. Alineatul (2) se elimină.

3. Alineatele (3) și (4) se înlocuiesc cu următorul text:

„(3) Pentru serviciile pe care le prestează, precum și pentru fiecare sistem de decontare a titlurilor de valoare pe care îl exploatează, CSD-urile prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura continuitatea serviciilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor CSD-urilor în cazul unor evenimente care prezintă un risc semnificativ de perturbare a operațiunilor.

(4) Planul menționat la alineatul (3) prevede reluarea tuturor tranzacțiilor și pozițiilor participanților în momentul perturbării, pentru a permite participanților la un CSD să continue să funcționeze în condiții de siguranță și să efectueze decontarea la data stabilită, inclusiv prin garantarea faptului că sistemele IT esențiale pot relua operațiunile aflate în curs în momentul perturbării, astfel cum se prevede la articolul 12 alineatele (5) și (7) din Regulamentul (UE) 2022/2554.”

4. Alineatul (6) se înlocuiește cu următorul text:

„(6) CSD-urile identifică, monitorizează și gestionează riscurile pe care le pot prezenta pentru operațiunile lor participanții principali la sistemele de decontare a titlurilor de valoare pe care le exploatează, precum și furnizorii de servicii și utilități, dar și alte CSD-uri sau alte infrastructuri ale piețelor. La cerere, CSD-urile furnizează autorităților competente și relevante informații cu privire la orice astfel de riscuri identificate. De asemenea, acestea informează autoritatea competentă și autoritățile relevante, fără întârziere, cu privire la orice incident operațional, altul decât cele legate de riscurile TIC, care rezultă din astfel de riscuri.”

5. La alineatul (7), primul paragraf se înlocuiește cu următorul text:

„(7) ESMA elaborează, în strânsă cooperare cu membrii SEBC, proiecte de standarde tehnice de reglementare care să precizeze riscurile operaționale menționate la alineatele (1) și (6), altele decât riscurile TIC, metodele de testare, abordare și reducere la minimum a riscurilor respective, inclusiv politicile de continuitate a activității și planurile de recuperare în caz de dezastru menționate la alineatele (3) și (4), precum și modalitățile de evaluare a acestora.”

Articolul 62

Modificarea Regulamentului (UE) nr. 600/2014

Regulamentul (UE) nr. 600/2014 se modifică după cum urmează:

1. Articolul 27g se modifică după cum urmează:

   (a) alineatul (4) se înlocuiește cu următorul text:

   „(4) APA respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

   _____

   (*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).";

   (b) la alineatul (8), litera (c) se înlocuiește cu următorul text:

   „(c) cerințele organizatorice concrete prevăzute la alineatele (3) și (5)."

2. Articolul 27h se modifică după cum urmează:

   (a) alineatul (5) se înlocuiește cu următorul text:

   „(5) CTP respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554.";

   (b) la alineatul (8), litera (e) se înlocuiește cu următorul text:

   „(e) cerințele organizatorice concrete prevăzute la alineatul (4)."

3. Articolul 27i se modifică după cum urmează:

   (a) alineatul (3) se înlocuiește cu următorul text:

   „(3) ARM respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554.";

   (b) la alineatul (5), litera (b) se înlocuiește cu următorul text:

   „(b) cerințele organizatorice concrete prevăzute la alineatele (2) și (4)."

Articolul 63

Modificarea Regulamentului (UE) 2016/1011

La articolul 6 din Regulamentul (UE) 2016/1011 se adaugă următorul alineat:

„(6) Pentru indicii de referință critici, administratorul dispune de proceduri administrative și contabile sigure, de mecanisme de control intern, de proceduri eficace de evaluare a riscurilor și de mecanisme eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

_____

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1)."

Articolul 64

Intrarea în vigoare și aplicarea

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la 17 ianuarie 2025.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Strasbourg, 14 decembrie 2022.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	M. BEK

DIRECTIVE

DIRECTIVA (UE) 2022/2555 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 14 decembrie 2022

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Băncii Centrale Europene ([1]),

având în vedere avizul Comitetului Economic și Social European ([2]),

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară ([3]),

întrucât:

(1) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([4]) viza consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, atenuarea amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente, contribuind astfel la securitatea Uniunii și la funcționarea eficace a economiei și a societății sale.

(2) De la intrarea în vigoare a Directivei (UE) 2016/1148, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență cibernetică în Uniune. Reexaminarea directivei respective a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă a mentalității. Directiva respectivă a asigurat finalizarea cadrelor naționale privind securitatea rețelelor și a sistemelor informatice prin elaborarea unor strategii naționale referitoare la securitatea rețelelor și a sistemelor informatice și prin crearea de capacități naționale, precum și prin punerea în aplicare a unor măsuri de reglementare care să vizeze infrastructurile și entitățile esențiale identificate de fiecare stat membru. De asemenea, Directiva (UE) 2016/1148 a contribuit la cooperarea la nivelul Uniunii prin instituirea Grupului de cooperare și a rețelei de echipe naționale de intervenție în caz de incidente de securitate informatică. În pofida acestor realizări, reexaminarea Directivei (UE) 2016/1148 a evidențiat deficiențe inerente care o împiedică să soluționeze în mod eficace provocările actuale și cele emergente în materie de securitate cibernetică.

(3) Rețelele și sistemele informatice au devenit o componentă centrală a vieții de zi cu zi, odată cu transformarea digitală rapidă și interconectarea societății, inclusiv în cadrul schimburilor transfrontaliere. Această transformare a condus la o extindere a peisajului amenințărilor la adresa securității cibernetice, generând noi provocări, care necesită răspunsuri adaptate, coordonate și inovatoare în toate statele membre. Incidentele sunt tot mai numeroase, mai ample, mai sofisticate, mai frecvente și cu un impact tot mai mare, acestea reprezentând o amenințare gravă la adresa funcționării rețelelor și a sistemelor informatice. Prin urmare, incidentele pot împiedica desfășurarea

([1]) JO C 233, 16.6.2022, p. 22.
([2]) JO C 286, 16.7.2021, p. 170.
([3]) Poziția Parlamentului European din 10 noiembrie 2022 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 28 noiembrie 2022.
([4]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

activităților economice pe piața internă, pot genera pierderi financiare, pot submina încrederea utilizatorilor și pot provoca pagube majore economiei și societății Uniunii. Prin urmare, pregătirea și eficacitatea în materie de securitate cibernetică sunt acum mai importante ca niciodată pentru buna funcționare a pieței interne. În plus, securitatea cibernetică este un factor-cheie pentru ca multe sectoare critice să adopte cu succes transformarea digitală și să profite pe deplin de beneficiile economice, sociale și durabile ale digitalizării.

(4) Temeiul juridic al Directivei (UE) 2016/1148 este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), al cărui obiectiv este instituirea și funcționarea pieței interne prin consolidarea măsurilor de apropiere a normelor naționale. Cerințele în materie de securitate cibernetică impuse entităților care furnizează servicii sau desfășoară activități care sunt semnificative din punct de vedere economic variază considerabil de la un stat membru la altul în ceea ce privește tipul de cerință, nivelul lor de detaliere și metoda de supraveghere. Disparitățile respective implică costuri suplimentare și creează dificultăți pentru entitățile care oferă bunuri sau servicii la nivel transfrontalier. Cerințele impuse de un stat membru care sunt diferite sau chiar în conflict cu cele impuse de un alt stat membru pot afecta în mod substanțial astfel de activități transfrontaliere. În plus, posibilitatea ca cerințele de securitate să fie concepute sau puse în aplicare în mod necorespunzător într-un stat membru este probabil să aibă repercusiuni asupra nivelului de securitate cibernetică din alte state membre, în special având în vedere intensitatea schimburilor transfrontaliere. Revizuirea Directivei (UE) 2016/1148 a arătat că punerea sa în aplicare diferă foarte mult de la un stat membru la altul, inclusiv în ceea ce privește domeniul său de aplicare, a cărui delimitare a fost lăsată în mare măsură la latitudinea statelor membre. Directiva (UE) 2016/1148 a acordat, de asemenea, statelor membre o marjă de apreciere foarte largă în ceea ce privește punerea în aplicare a obligațiilor de raportare privind securitatea și incidentele pe care le prevede aceasta. Prin urmare, obligațiile respective au fost puse în aplicare în moduri foarte diferite la nivel național. Există divergențe similare în ceea ce privește punerea în aplicare a dispozițiilor Directivei (UE) 2016/1148 privind supravegherea și asigurarea respectării legii.

(5) Toate aceste divergențe implică o fragmentare a pieței interne și pot avea un efect negativ asupra funcționării acesteia, afectând în special furnizarea transfrontalieră de servicii și nivelul de reziliență cibernetică din cauza aplicării unor măsuri diferite. În cele din urmă, divergențele respective ar putea duce la o vulnerabilitate mai mare a unor state membre la amenințările cibernetice, cu potențiale efecte de propagare în întreaga Uniune. Prezenta directivă urmărește să elimine astfel de divergențe marcante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace între autoritățile responsabile din fiecare stat membru, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și măsuri de asigurare a respectării legii eficace care sunt esențiale pentru asigurarea efectivă a respectării acestor obligații. Prin urmare, Directiva (UE) 2016/1148 ar trebui să fie abrogată și înlocuită cu prezenta directivă.

(6) Odată cu abrogarea Directivei (UE) 2016/1148, domeniul de aplicare pe sectoare ar trebui să fie extins la o parte mai mare a economiei pentru a oferi o acoperire cuprinzătoare a sectoarelor și a serviciilor de importanță vitală pentru activitățile societale și economice esențiale din cadrul pieței interne. În special, prezenta directivă vizează depășirea deficiențelor legate de diferențierea dintre operatorii de servicii esențiale și furnizorii de servicii digitale, care s-a dovedit a fi caducă, deoarece nu reflectă importanța sectoarelor sau a serviciilor pentru activitățile societale și economice din cadrul pieței interne.

(7) În temeiul Directivei (UE) 2016/1148, statele membre erau responsabile de identificarea entităților ce îndeplineau criteriile pentru a se califica ca operatori de servicii esențiale. Pentru a elimina divergențele mari dintre statele membre în această privință și pentru a asigura securitatea juridică în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un criteriu uniform pentru a determina entitățile care intră în domeniul de aplicare al prezentei directive. Criteriul respectiv ar trebui să constea în aplicarea unei norme de plafonare a dimensiunii, potrivit căreia toate entitățile care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE a Comisiei ([5]), sau depășesc plafoanele aferente întreprinderilor mijlocii prevăzute la alineatul (1) din

([5]) Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

respectivul articol, și care își desfășoară activitatea în sectoarele și furnizează tipurile de servicii sau desfășoară activitățile reglementate de prezenta directivă intră în domeniul său de aplicare. Statele membre ar trebui, de asemenea, să prevadă ca anumite întreprinderi mici și microîntreprinderi, astfel cum sunt definite la articolul 2 alineatele (2) și (3) din respectiva anexă, care îndeplinesc criterii specifice ce indică un rol esențial pentru societate, pentru economie sau pentru anumite sectoare sau tipuri de servicii, să intre în domeniul de aplicare al prezentei directive.

(8) Excluderea entităților administrației publice din domeniul de aplicare al prezentei directive ar trebui să se aplice entităților ale căror activități se desfășoară predominant în domeniile securității naționale, securității publice, apărării sau aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor. Cu toate acestea, entitățile administrației publice ale căror activități au doar o legătură redusă cu aceste domenii nu ar trebui să fie excluse din domeniul de aplicare al prezentei directive. În sensul prezentei directive, entitățile cu competențe de reglementare nu sunt considerate a desfășura activități în domeniul aplicării legii și, prin urmare, nu sunt excluse din acel motiv din domeniul de aplicare al prezentei directive. Entitățile administrației publice care sunt înființate în comun cu o țară terță în conformitate cu un acord internațional sunt excluse din domeniul de aplicare al prezentei directive. Prezenta directivă nu se aplică misiunilor diplomatice și consulare ale statelor membre în țări terțe sau rețelelor și sistemelor informatice ale acestora, în măsura în care aceste sisteme se află la sediul misiunii sau sunt utilizate pentru utilizatori dintr-o țară terță.

(9) Statele membre ar trebui să fie în măsură să ia măsurile necesare pentru a asigura protecția intereselor vitale de securitate națională, a apăra ordinea publică și siguranța publică și a permite prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor. În acest scop, statele membre ar trebui să poată exonera anumite entități care desfășoară activități în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, de anumite obligații prevăzute în prezenta directivă în ceea ce privește activitățile respective. În cazul în care o entitate prestează servicii exclusiv unei entități a administrației publice care este exclusă din domeniul de aplicare al prezentei directive, statele membre ar trebui să poată exonera entitatea respectivă de anumite obligații prevăzute în prezenta directivă în ceea ce privește serviciile în cauză. De asemenea, niciun stat membru nu ar trebui să aibă obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale securității naționale, siguranței publice sau apărării sale. Normele Uniunii sau cele naționale privind protecția informațiilor clasificate, acordurile de nedivulgare și acordurile de nedivulgare informale, cum ar fi protocolul de schimb de informații „*Traffic Light Protocol*”, ar trebui luate în considerare în respectivul context. Protocolul de schimb de informații „*Traffic Light Protocol*” trebuie înțeles ca un mijloc de a furniza informații cu privire la orice limitări în ce privește răspândirea ulterioară a informațiilor. Acesta este utilizat în aproape toate echipele de intervenție în caz de incidente de securitate informatică (denumite în continuare „echipe CSIRT”) și în unele centre de analiză și de schimb de informații.

(10) Deși prezenta directivă se aplică entităților care desfășoară activități de producere a energiei electrice în centrale nucleare, unele dintre respectivele activități pot fi legate de securitatea națională. Într-un astfel de caz, un stat membru ar trebui să își poată exercita responsabilitatea de protejare a securității naționale în ceea ce privește activitățile respective, inclusiv activitățile din cadrul lanțului valoric nuclear, în conformitate cu tratatele.

(11) Unele entități desfășoară activități în domeniul securității naționale, al securității publice, al apărării sau al aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, prestând în același timp servicii de încredere. Prestatorii de servicii de încredere care intră în domeniul de aplicare al Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([6]) ar trebui să intre în domeniul de aplicare al prezentei directive pentru a asigura același nivel de cerințe de securitate și de supraveghere ca cel prevăzut anterior în regulamentul respectiv în ceea ce privește prestatorii de servicii de încredere. În concordanță cu excluderea anumitor servicii specifice din Regulamentul (UE) nr. 910/2014, prezenta directivă nu ar trebui să se aplice prestării de servicii de încredere care sunt utilizate exclusiv în cadrul unor sisteme închise care decurg din dreptul intern sau din acorduri între un grup definit de participanți.

([6]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).

(12) Furnizorii de servicii poștale astfel cum sunt definiți în Directiva 97/67/CE a Parlamentului European și a Consiliului ([7]), inclusiv furnizorii de servicii de curierat ar trebui să intre în domeniul de aplicare al prezentei directive în cazul în care asigură cel puțin una dintre etapele lanțului de distribuție poștală, în special colectarea, sortarea, transportul sau distribuirea trimiterilor poștale, inclusiv serviciile de preluare, ținând seama totodată de gradul lor de dependență de rețele și de sistemele informatice. Serviciile de transport care nu sunt efectuate împreună cu una dintre aceste etape ar trebui să fie excluse din domeniul de aplicare al serviciilor poștale.

(13) Având în vedere intensificarea și gradul sporit de sofisticare a amenințărilor cibernetice, statele membre ar trebui să depună eforturi pentru a se asigura că entitățile care sunt excluse din domeniul de aplicare al prezentei directive ating un nivel ridicat de securitate cibernetică și pentru a sprijini punerea în aplicare a unor măsuri echivalente de gestionare a riscurilor în materie de securitate cibernetică care să reflecte natura sensibilă a entităților respective.

(14) Dreptul Uniunii privind protecția datelor și dreptul Uniunii privind protejarea confidențialității se aplică oricărei forme de prelucrare a datelor cu caracter personal în temeiul prezentei directive. În special, prezenta directivă nu aduce atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([8]) și Directivei 2002/58/CE a Parlamentului European și a Consiliului ([9]). Prin urmare, prezenta directivă nu ar trebui să aducă atingere, printre altele, sarcinilor și competențelor autorităților competente să monitorizeze respectarea dreptului aplicabil al Uniunii în materie de protecție a datelor și a dreptului aplicabil al Uniunii privind protejarea confidențialității.

(15) Entitățile care intră în domeniul de aplicare al prezentei directive în scopul respectării măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare ar trebui clasificate în două categorii, entități esențiale și entități importante, reflectând măsura în care acestea sunt critice în ceea ce privește sectorul lor sau tipul de serviciu pe care îl prestează, precum și dimensiunea lor. În acest sens, ar trebui să se țină seama în mod corespunzător de orice evaluări ale riscurilor sau de orice orientări specifice unui sector relevante emise de către autoritățile competente, după caz. Regimurile de supraveghere și de asigurare a respectării legii corespunzătoare acestor două categorii de entități ar trebui să fie diferențiate pentru a asigura un echilibru corect între cerințele și obligațiile bazate pe riscuri, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte.

(16) Pentru a evita ca entitățile care au întreprinderi partenere sau care sunt întreprinderi afiliate să fie considerate entități esențiale sau entități importante în cazul în care acest lucru ar fi disproporționat, statele membre pot ține seama de gradul de independență de care se bucură o entitate în raport cu întreprinderile sale partenere sau afiliate atunci când aplică articolul 6 alineatul (2) din anexa la Recomandarea 2003/361/CE. În special, statele membre sunt în măsură să ia în considerare faptul că o entitate este independentă de întreprinderile sale partenere sau afiliate în ceea ce privește rețelele și sistemele informatice pe care le utilizează pentru furnizarea serviciilor sale și în ceea ce privește serviciile pe care le prestează entitatea. Pe această bază, dacă este cazul, statele membre sunt în măsură să considere că o astfel de entitate nu se califică drept o întreprindere mijlocie în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau nu depășește plafoanele pentru o întreprindere mijlocie prevăzute la alineatul (1) din respectivul articol dacă, după luarea în considerare a gradului de independență a entității respective, nu s-ar fi considerat că acea entitate se califică drept o întreprindere mijlocie sau că depășește plafoanele respective în cazul în care ar fi fost luate în considerare numai propriile date. Acest lucru nu aduce atingere obligațiilor prevăzute în prezenta directivă ale întreprinderilor partenere și afiliate care intră în domeniul de aplicare al prezentei directive.

(17) Statele membre ar trebui să poată decide că entitățile identificate înainte de intrarea în vigoare a prezentei directive ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 trebuie să fie considerate entități esențiale.

([7]) Directiva 97/67/CE a Parlamentului European și a Consiliului din 15 decembrie 1997 privind normele comune pentru dezvoltarea pieței interne a serviciilor poștale ale Comunității și îmbunătățirea calității serviciului (JO L 15, 21.1.1998, p. 14).

([8]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([9]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

(18) Pentru a asigura o imagine de ansamblu clară a entităților care intră în domeniul de aplicare al prezentei directive, statele membre ar trebui să stabilească o listă a entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii. În acest scop, statele membre ar trebui să solicite entităților să transmită autorităților competente cel puțin următoarele informații, și anume denumirea, adresa și datele de contact actualizate, inclusiv adresele de e-mail, seriile IP și numerele de telefon ale entității și, după caz, sectorul și subsectorul pertinente menționate în anexe, precum și, după caz, o listă a statelor membre în care prestează servicii care intră în domeniul de aplicare al prezentei directive. În acest scop, Comisia, cu sprijinul Agenției pentru Securitate Cibernetică a Uniunii Europene (ENISA), ar trebui să ofere, fără întârzieri nejustificate, orientări și modele privind obligația de a prezenta informații. Pentru a înlesni întocmirea și actualizarea listei entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii, statele membre ar trebui să poată institui mecanisme naționale care să le permită entităților să se înregistreze ele însele. În cazul în care există registre la nivel național, statele membre pot decide cu privire la mecanismele adecvate care să permită identificarea entităților care intră în domeniul de aplicare al prezentei directive.

(19) Statele membre ar trebui să fie responsabile de transmiterea către Comisie cel puțin a numărului de entități esențiale și entități importante pentru fiecare sector și subsector menționat în anexe, precum și a informațiilor pertinente cu privire la numărul entităților identificate și dispoziția, dintre cele prevăzute în prezenta directivă, pe baza cărora au fost identificate, precum și tipul de serviciu pe care îl furnizează. Statele membre sunt încurajate să facă schimb de informații cu Comisia cu privire la entitățile esențiale și entitățile importante și, în cazul unui incident de securitate cibernetică de mare amploare, de informații pertinente, cum ar fi denumirea entității în cauză.

(20) Comisia, în cooperare cu Grupul de cooperare și după consultarea părților interesate pertinente, ar trebui să ofere orientări privind punerea în aplicare a criteriilor aplicabile microîntreprinderilor și întreprinderilor mici pentru a evalua dacă acestea intră în domeniul de aplicare al prezentei directive. Comisia ar trebui, de asemenea, să asigure faptul că se oferă orientări adecvate microîntreprinderilor și întreprinderilor mici care intră în domeniul de aplicare al prezentei directive. Comisia ar trebui, cu sprijinul statelor membre, să le pună la dispoziție microîntreprinderilor și întreprinderilor mici informații în acest sens.

(21) Comisia ar putea oferi orientări pentru a sprijini statele membre în punerea în aplicare a dispozițiilor prezentei directive privind domeniul de aplicare și în evaluarea proporționalității măsurilor care trebuie luate în temeiul prezentei directive, în special în ceea ce privește entitățile cu modele de afaceri sau medii de funcționare complexe, în care o entitate poate îndeplini simultan criteriile atribuite entităților esențiale și celor importante sau poate desfășura simultan activități, dintre care unele se încadrează în domeniul de aplicare al prezentei directive, iar altele nu se încadrează.

(22) Prezenta directivă stabilește nivelul de referință pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare în toate sectoarele care intră în domeniul său de aplicare. Pentru a evita fragmentarea dispozițiilor privind securitatea cibernetică din actele juridice ale Uniunii, în cazul în care se consideră a fi necesare alte acte juridice sectoriale ale Uniunii referitoare la măsurile de gestionare a riscurilor în materie de securitate cibernetică și la obligațiile de raportare pentru a asigura un nivel ridicat de securitate cibernetică în întreaga Uniune, Comisia ar trebui să evalueze dacă astfel de dispoziții suplimentare ar putea fi stipulate într-un act de punere în aplicare în temeiul prezentei directive. În cazul în care un astfel de act de punere în aplicare nu este adecvat scopului respectiv, actele juridice sectoriale ale Uniunii ar putea contribui la asigurarea unui nivel ridicat de securitate cibernetică în întreaga Uniune, ținând seama pe deplin de particularitățile și de complexitatea sectoarelor în cauză. În acest scop, prezenta directivă nu împiedică adoptarea altor acte juridice sectoriale ale Uniunii care abordează măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare care iau în considerare în mod corespunzător necesitatea unui cadru de securitate cibernetică cuprinzător și coerent. Prezenta directivă nu aduce atingere competențelor de executare existente care i-au fost conferite Comisiei într-o serie de sectoare, inclusiv în domeniul transporturilor și în cel al energiei.

(23) În cazul în care un act juridic sectorial al Uniunii cuprinde dispoziții care impun entităților esențiale sau entităților importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele semnificative, și în cazul în care cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute

în prezenta directivă, dispozițiile respective, inclusiv cele privind supravegherea și aplicarea legii, ar trebui să se aplice acestor entități. În cazul în care un act juridic sectorial al Uniunii nu include toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive ar trebui să se aplice în continuare entităților care nu fac obiectul dispozițiilor actului respectiv.

(24) În cazul în care dispozițiile unui act juridic sectorial al Uniunii impun entităților esențiale sau entităților importante să respecte obligațiile de raportare care au un efect cel puțin echivalent cu cel al obligațiilor de raportare prevăzute în prezenta directivă, ar trebui să se asigure coerența și eficacitatea gestionării notificărilor incidentelor. În acest scop, dispozițiile privind notificarea incidentelor din actul juridic sectorial al Uniunii ar trebui, în temeiul prezentei directive, să ofere echipelor CSIRT, autorităților competente sau punctelor unice de contact privind securitatea cibernetică (denumite în continuare „puncte unice de contact") un acces imediat la notificările incidentelor transmise în conformitate cu actul juridic sectorial al Uniunii. În special, un astfel de acces imediat poate fi asigurat dacă notificările incidentelor sunt înaintate fără întârzieri nejustificate către echipa CSIRT, autoritatea competentă sau punctul unic de contact în temeiul prezentei directive. După caz, statele membre ar trebui să instituie un mecanism de raportare automată și directă care să asigure schimbul sistematic și imediat de informații cu echipele CSIRT, cu autoritățile competente sau cu punctele unice de contact cu privire la gestionarea unor astfel de notificări ale incidentelor. În scopul simplificării informării și al punerii în aplicare a mecanismului de raportare automată și directă, statele membre ar putea, în concordanță cu actul juridic sectorial al Uniunii, să utilizeze un punct de intrare unic.

(25) Actele juridice sectoriale ale Uniunii care prevăd măsuri de gestionare a riscurilor în materie de securitate cibernetică sau obligații de raportare care au un efect cel puțin echivalent cu cele prevăzute în prezenta directivă ar putea prevedea ca autoritățile competente în temeiul respectivelor acte să își exercite competențele de supraveghere și de aplicare a legii în raport cu respectivele măsuri sau obligații, cu sprijinul autorităților competente desemnate în temeiul prezentei directive. Autoritățile competente în cauză ar putea încheia acorduri de cooperare în acest scop. Astfel de acorduri de cooperare ar putea specifica, printre altele, procedurile privind coordonarea activităților de supraveghere, inclusiv procedurile de investigare și de inspecție la fața locului în conformitate cu dreptul intern, precum și un mecanism pentru schimbul de informații relevante privind supravegherea și aplicarea legii între autoritățile competente, inclusiv accesul la informațiile legate de domeniul cibernetic solicitate de autoritățile competente în temeiul prezentei directive.

(26) În cazul în care actele juridice sectoriale ale Uniunii impun entităților sau oferă stimulente acestora pentru ca acestea să notifice amenințările cibernetice semnificative, statele membre ar trebui, de asemenea, să încurajeze schimbul de informații cu privire la amenințările cibernetice semnificative cu echipele CSIRT, cu autoritățile competente sau cu punctele unice de contact în temeiul prezentei directive, pentru a asigura un nivel sporit de conștientizare a organismelor respective cu privire la contextul amenințărilor cibernetice și pentru a le permite să răspundă în mod eficace și în timp util în cazul în care amenințările cibernetice semnificative se materializează.

(27) Viitoarele acte juridice sectoriale ale Uniunii ar trebui să țină seama în mod corespunzător de definițiile și de cadrul de supraveghere și de asigurare a respectării legii prevăzute în prezenta directivă.

(28) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului ([10]) ar trebui considerat a fi un act juridic sectorial al Uniunii în legătură cu prezenta directivă în ce privește entitățile financiare. Dispozițiile Regulamentului (UE) 2022/2554 referitoare la gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC), la gestionarea incidentelor legate de TIC și, în special, la raportarea incidentelor majore legate de TIC, precum și la testarea rezilienței operaționale digitale, la acordurile privind schimbul de informații și la riscurile TIC generate de părți terțe ar trebui să se aplice în locul celor prevăzute în prezenta directivă. Prin urmare, statele membre nu ar trebui să aplice dispozițiile prezentei directive privind gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare, supraveghere și aplicarea legii, entităților financiare care fac obiectul Regulamentului (UE) 2022/2554. În același timp, este important ca, în temeiul prezentei directive, să se mențină o relație puternică cu sectorul financiar și să se facă un schimb de informații cu acesta. În acest scop, Regulamentul (UE) 2022/2554 permite autorităților europene de supraveghere (AES) și autorităților competente în temeiul respectivului regulament să participe la activitățile Grupului de cooperare și să facă schimb de informații și să coopereze cu punctele unice de contact, precum și cu echipele CSIRT și cu autoritățile competente în temeiul prezentei directive. Autoritățile competente în temeiul Regulamentului (UE) 2022/2554 ar trebui, de asemenea, să transmită detaliile

([10]) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (a se vedea pagina 1 din prezentul Jurnal Oficial).

incidentelor majore legate de TIC și, după caz, ale amenințărilor cibernetice semnificative echipelor CSIRT, autorităților competente sau punctelor unice de contact în temeiul prezentei directive. Acest lucru se poate realiza prin asigurarea accesului imediat la notificările privind incidentele și prin înaintarea acestora fie în mod direct, fie prin intermediul unui punct de intrare unic. În plus, statele membre ar trebui să includă în continuare sectorul financiar în strategiile lor de securitate cibernetică, iar echipele CSIRT pot include sectorul financiar în activitățile lor.

(29) Pentru a evita lacunele și suprapunerile obligațiilor în materie de securitate cibernetică impuse entităților din sectorul aviației, autoritățile naționale desemnate în temeiul Regulamentului (CE) nr. 300/2008 ([11]) și Regulamentului (UE) 2018/1139 ([12]) ale Parlamentului European și ale Consiliului și autoritățile competente desemnate în temeiul prezentei directive ar trebui să coopereze în ceea ce privește punerea în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și supravegherea conformării cu aceste măsuri la nivel național. Respectarea de către o entitate a cerințelor de securitate prevăzute în Regulamentul (CE) nr. 300/2008 și Regulamentul (UE) 2018/1139 și în actele delegate și de punere în aplicare relevante adoptate în temeiul regulamentelor respective ar putea fi considerată de către autoritățile competente în temeiul prezentei directive ca reprezentând conformarea cu cerințele corespunzătoare prevăzute în prezenta directivă.

(30) Având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a entităților, ar trebui să se asigure o abordare coerentă între Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului ([13]) și prezenta directivă. Pentru a realiza acest lucru, entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557 ar trebui să fie considerate a fi entități esențiale în temeiul prezentei directive. Mai mult, fiecare stat membru ar trebui să se asigure că strategia sa națională de securitate cibernetică oferă un cadru de politică pentru o coordonare consolidată în statul membru respectiv între autoritățile sale competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 în contextul schimbului de informații privind riscurile, amenințările cibernetice și incidentele, precum și privind riscurile, amenințările și incidentele de altă natură decât cibernetică și cel al exercitării sarcinilor de supraveghere. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui să coopereze și să facă schimb de informații fără întârzieri nejustificate, în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în legătură cu riscurile, amenințările și incidentele de altă natură decât cibernetică ce afectează entitățile critice, inclusiv măsurile în materie de securitate cibernetică și măsurile fizice adoptate de entitățile critice precum și rezultatele activităților de supraveghere desfășurate în legătură cu astfel de entități.

În plus, pentru a raționaliza activitățile de supraveghere între autoritățile competente în temeiul prezentei directive și al Directivei (UE) 2022/2557 și pentru a reduce la minimum sarcina administrativă pentru entitățile în cauză, autoritățile competente ar trebui să depună eforturi pentru a armoniza modelele de notificare a incidentelor și procesele de supraveghere. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 ar trebui să poată solicita autorităților competente în temeiul prezentei directive să își exercite competențele de supraveghere și de asigurare a respectării legii în legătură cu o entitate care este identificată drept o entitate critică în temeiul Directivei (UE) 2022/2557. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui, atunci când este posibil în timp real, să coopereze și să facă schimb de informații în acest scop.

(31) Entitățile care aparțin sectorului infrastructurii digitale se bazează, în esență, pe rețele și sisteme informatice și, prin urmare, obligațiile impuse acestor entități în temeiul prezentei directive ar trebui să abordeze în mod cuprinzător securitatea fizică a acestor sisteme, ca parte a măsurilor lor de gestionare a riscurilor și a obligațiilor de raportare în materie de securitate cibernetică. Întrucât aceste aspecte sunt reglementate de prezenta directivă, obligațiile prevăzute în capitolele III, IV și VI din Directiva (UE) 2022/2557 nu se aplică acestor entități.

([11]) Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72).

([12]) Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1).

([13]) Directiva (UE) 2022/2557 a Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (a se vedea pagina 164 din prezentul Jurnal Oficial).

(32) Sprijinirea și menținerea unui sistem fiabil, rezilient și sigur de nume de domenii (DNS) reprezintă factori-cheie pentru menținerea integrității internetului și sunt esențiali pentru funcționarea sa continuă și stabilă, de care depind economia digitală și societatea. Prin urmare, prezenta directivă ar trebui să se aplice registrelor de nume de domenii de prim nivel (TLD) și prestatorilor de servicii DNS care trebuie înțelese ca fiind entități care furnizează servicii de rezolvare recursivă a numelor de domenii accesibile publicului pentru utilizatorii finali de internet sau ca servicii de rezolvare a numelor de domenii cu autoritate pentru utilizarea de către terți. Prezenta directivă nu ar trebui să se aplice serverelor pentru numele primare.

(33) Serviciile de *cloud computing* ar trebui să cuprindă serviciile digitale care permit administrarea la cerere și accesul amplu de la distanță la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun, inclusiv atunci când aceste resurse sunt distribuite în mai multe locuri. Resursele informatice includ resurse precum rețelele, serverele sau alte infrastructuri, sistemele de operare, programele informatice (software), stocarea, aplicațiile și serviciile. Modelele de servicii de *cloud computing* includ, printre altele, infrastructura ca serviciu (IaaS), platforma ca serviciu (PaaS), software-ul ca serviciu (SaaS) și rețeaua ca serviciu (NaaS). Modelele de implementare a *cloud computingului* ar trebui să includă tehnologiile de tip *cloud* private, comunitare, publice și hibride. Modelele de servicii și de implementare de *cloud computing* au același înțeles ca și termenii modelelor de servicii și de implementare definiți în standardul ISO/IEC 17788:2014. Capacitatea utilizatorului de *cloud computing* de a furniza în mod unilateral capacități de calcul autonome, cum ar fi ora serverului sau stocarea în rețea, fără nicio interacțiune umană din partea furnizorului de servicii de *cloud computing*, ar putea fi descrisă ca administrare la cerere.

Termenul „acces amplu de la distanță” este utilizat pentru a descrie faptul că capacitățile de *cloud* sunt furnizate prin rețea și accesate prin mecanisme care promovează utilizarea unor platforme eterogene, subțiri sau groase, pentru clienți, inclusiv telefoane mobile, tablete, laptopuri și stații de lucru. Termenul „redimensionabil” se referă la resursele informatice care sunt alocate în mod flexibil de către furnizorul de servicii de *cloud*, indiferent de localizarea geografică a resurselor, pentru a face față fluctuațiilor cererii. Termenul „bazin elastic” se referă la resursele informatice care sunt furnizate și puse la dispoziție în funcție de cerere, pentru a amplifica și a reduce rapid resursele disponibile în conformitate cu volumul de lucru. Expresia „care pot fi puse în comun” este utilizată pentru a descrie acele resurse informatice care sunt furnizate mai multor utilizatori care au acces comun la serviciu, dar tratamentul se efectuează separat pentru fiecare utilizator, deși serviciul este prestat de același echipament electronic. Termenul „distribuit” se referă la resursele informatice care sunt situate pe diferite calculatoare sau dispozitive în rețea și care comunică și se coordonează între ele prin transmiterea de mesaje.

(34) Având în vedere apariția unor tehnologii inovatoare și a unor noi modele de afaceri, se preconizează că pe piața internă vor apărea noi servicii de *cloud computing* și noi modele de implementare ca răspuns la nevoile în continuă evoluție ale clienților. În acest context, serviciile de *cloud computing* pot fi prestate într-o formă foarte distribuită, chiar mai aproape de locul în care datele sunt generate sau colectate, trecând astfel de la modelul tradițional la unul foarte distribuit („tehnica de calcul la margine” – *edge computing*).

(35) Este posibil ca serviciile oferite de prestatorii de servicii de centre de date să nu fie întotdeauna prestate sub formă de servicii de *cloud computing*. În consecință, este posibil ca centrele de date să nu constituie întotdeauna o parte a infrastructurii de *cloud computing*. Pentru a gestiona toate riscurile la adresa securității rețelelor și a sistemelor informatice, prezenta directivă ar trebui să vizeze, prin urmare, furnizorii de servicii de centre de date care nu sunt servicii de *cloud computing*. În sensul prezentei directive, termenul „serviciu de centre de date” ar trebui să includă prestarea unui serviciu care cuprinde structuri sau grupuri de structuri destinate instalării centralizate, interconectării și funcționării tehnologiei informației (IT) și echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului. Termenul „serviciu de centru de date” nu ar trebui să se aplice centrelor de date corporative interne, deținute și exploatate de entitatea în cauză, în scopuri proprii.

(36) Activitățile de cercetare joacă un rol esențial în dezvoltarea de noi produse și procese. Multe dintre respectivele activități sunt desfășurate de entități care partajează, diseminează sau exploatează rezultatele cercetării lor în scopuri comerciale. Prin urmare, aceste entități pot fi actori importanți în lanțurile valorice, ceea ce face ca securitatea rețelelor și a sistemelor lor informatice să fie parte integrantă din securitatea cibernetică globală a pieței interne. Organizațiile de cercetare ar trebui înțelese ca incluzând entitățile care își concentrează partea esențială a

activităților pe desfășurarea de cercetare aplicată sau dezvoltare experimentală, în sensul Manualului Frascati 2015 al Organizației pentru Cooperare și Dezvoltare Economică: *Guidelines for Collecting and Reporting Data on Research and Experimental Development* (Orientări pentru colectarea și raportarea datelor privind cercetarea și dezvoltarea experimentală), în vederea exploatării rezultatelor acestora în scopuri comerciale, cum ar fi fabricarea sau dezvoltarea unui produs sau a unui proces, furnizarea unui serviciu sau comercializarea acestora.

(37) Interdependențele din ce în ce mai mari sunt rezultatul unei rețele din ce în ce mai transfrontaliere și interdependente de prestare de servicii care utilizează infrastructuri-cheie din întreaga Uniune în sectoare precum energia, transporturile, infrastructura digitală, apa potabilă și apele uzate, sănătatea, anumite aspecte ale administrației publice, precum și spațiul, în măsura în care furnizarea anumitor servicii în funcție de infrastructurile terestre care sunt deținute, gestionate și exploatate fie de statele membre, fie de părți private, nu cuprinde, prin urmare, infrastructurile deținute, gestionate sau exploatate de Uniune sau în numele acesteia, ca parte a programului său spațial. Aceste interdependențe înseamnă că orice perturbare, chiar dacă inițial este limitată la o singură entitate sau la un singur sector, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea efecte negative de amploare și de lungă durată asupra furnizării de servicii pe piața internă. Intensificarea atacurilor cibernetice în timpul pandemiei de COVID-19 a demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere.

(38) Având în vedere diferențele dintre structurile naționale de administrare și pentru a proteja acordurile specifice unui sector sau organismele de supraveghere și de reglementare ale Uniunii deja existente, statele membre ar trebui să fie în măsură să desemneze sau să instituie una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere în temeiul prezentei directive.

(39) Pentru a facilita cooperarea și comunicarea transfrontalieră între autorități și pentru a permite punerea în aplicare efectivă a prezentei directive, este necesar ca fiecare stat membru să desemneze un punct unic de contact responsabil cu coordonarea aspectelor legate de securitatea rețelelor și a sistemelor informatice și cu cooperarea transfrontalieră la nivelul Uniunii.

(40) Punctele unice de contact ar trebui să asigure o cooperare transfrontalieră eficace cu autoritățile competente din alte state membre și, după caz, cu Comisia și cu ENISA. Punctele unice de contact ar trebui, prin urmare, să fie însărcinate cu înaintarea notificărilor incidentelor semnificative cu impact transfrontalier către punctele unice de contact ale altor state membre afectate, la cererea echipei CSIRT sau a autorității competente. La nivel național, punctele unice de contact ar trebui să înlesnească o bună cooperare transsectorială cu alte autorități competente. Punctele unice de contact ar putea fi, de asemenea, destinatarii informațiilor relevante privind incidentele referitoare la entitățile financiare transmise de autoritățile competente în temeiul Regulamentului (UE) 2022/2554 pe care ele ar trebui să le poată înainta, după caz, echipelor CSIRT sau autorităților competente în temeiul prezentei directive.

(41) Statele membre ar trebui să fie dotate în mod adecvat, din punctul de vedere al capacității atât tehnice, cât și organizatorice, pentru a preveni, a detecta, a răspunde și a se redresa de pe urma incidentelor și a riscurilor, precum și a atenua impactul acestora. Prin urmare, statele membre ar trebui să instituie sau să desemneze una sau mai multe echipe CSIRT în temeiul prezentei directive și să se asigure că acestea dispun de resurse și capacități tehnice adecvate. Echipele CSIRT ar trebui să respecte cerințele stabilite în prezenta directivă pentru a garanta existența unor capacități efective și compatibile de gestionare a incidentelor și a riscurilor și pentru a asigura o cooperare eficientă la nivelul Uniunii. Statele membre ar trebui să poată desemna în calitate de echipe CSIRT echipe existente de intervenție în caz de urgență informatică („CERT”). În vederea consolidării relației de încredere dintre entități și echipe CSIRT, în cazurile în care o echipe CSIRT face parte din autoritatea competentă, statele membre ar trebui să poată avea în vedere separarea funcțională a sarcinilor operaționale furnizate de echipele CSIRT, în special în ceea ce privește schimbul de informații și sprijinul acordat entităților, și activitățile de supraveghere ale autorităților competente.

(42) Echipele CSIRT au sarcina de a administra incidentele. Aceasta include prelucrarea unor volume mari de date uneori sensibile. Statele membre ar trebui să se asigure că echipele CSIRT dispun de o infrastructură pentru schimbul de informații și prelucrarea acestora, precum și de personal bine echipat, care asigură confidențialitatea și credibilitatea operațiunilor lor. Echipele CSIRT ar putea adopta, de asemenea, coduri de conduită în acest sens.

(43) În ceea ce privește datele cu caracter personal, echipele CSIRT ar trebui să poată furniza, în concordanță cu Regulamentul (UE) 2016/679, la cererea unei entități esențiale sau a unei entități importante, o scanare proactivă a rețelelor și a sistemelor informatice utilizate pentru prestarea serviciilor lor. Atunci când este cazul, statele membre ar trebui să vizeze asigurarea unui nivel egal de capacități tehnice pentru toate echipele CSIRT specifice unui sector. Statele membre ar trebui să poată solicita asistența ENISA pentru instituirea echipelor lor CSIRT.

(44) Echipele CSIRT ar trebui să aibă capacitatea, la cererea unei entități esențiale sau a unei entități importante, de a monitoriza resursele conectate la internet ale entității, atât la locurile în care își desfășoară activitatea, cât și în exteriorul acestora, pentru identifica, a înțelege și a gestiona riscurile organizaționale generale ale entității cu privire la compromisurile sau vulnerabilitățile critice nou-identificate din lanțul de aprovizionare. Entitatea ar trebui să fie încurajată să comunice echipei CSIRT dacă utilizează o interfață de gestionare privilegiată, deoarece acest lucru ar putea afecta viteza de desfășurare a unor acțiuni de atenuare.

(45) Având în vedere importanța cooperării internaționale în privința securității cibernetice, echipele CSIRT ar trebui să aibă posibilitatea de a participa la rețele de cooperare internațională, în plus față de rețeaua CSIRT instituită prin prezenta directivă. Prin urmare, în scopul îndeplinirii sarcinilor care le revin, echipele CSIRT și autoritățile competente ar trebui să poată face schimb de informații, inclusiv de date cu caracter personal, cu echipele naționale de intervenție în caz de incidente de securitate informatică sau cu autoritățile competente din țări terțe, cu condiția să fie îndeplinite condițiile prevăzute de dreptul Uniunii privind protecția datelor pentru transferurile de date cu caracter personal către țări terțe, printre altele cele prevăzute la articolul 49 din Regulamentul (UE) 2016/679.

(46) Este esențial să se asigure resurse adecvate pentru îndeplinirea obiectivelor prevăzute în prezenta directivă și pentru a facilita îndeplinirea de către autoritățile competente și echipele CSIRT a sarcinilor prevăzute în prezenta directivă. Statele membre pot institui la nivel național un mecanism de finanțare care să acopere cheltuielile necesare în legătură cu îndeplinirea sarcinilor entităților publice responsabile cu securitatea cibernetică în statul membru în temeiul prezentei directive. Un astfel de mecanism ar trebui să respecte dreptul Uniunii și ar trebui să fie proporțional și nediscriminatoriu și ar trebui să țină seama de diferitele abordări în ceea ce privește prestarea de servicii sigure.

(47) Rețeaua CSIRT ar trebui să contribuie în continuare la consolidarea încrederii și la promovarea unei cooperări operaționale rapide și eficace între statele membre. Pentru a consolida cooperarea operațională la nivelul Uniunii, rețeaua CSIRT ar trebui să aibă în vedere invitarea organelor și agențiilor Uniunii implicate în politica de securitate cibernetică, cum ar fi Europol, să participe la activitatea sa.

(48) În scopul atingerii și menținerii unui nivel ridicat de securitate cibernetică, strategiile naționale de securitate cibernetică necesare în temeiul prezentei directive ar trebui să constea în cadre coerente care să ofere obiective și priorități strategice în domeniul securității cibernetice și administrarea necesară pentru realizarea acestora. Aceste strategii pot fi compuse dintr-unul sau mai multe instrumente legislative sau fără caracter legislativ.

(49) Politicile de igienă cibernetică asigură baza pentru protecția infrastructurilor de rețele și sisteme informatice, pentru securitatea hardware, software și a aplicațiilor online, precum și pentru protecția datelor întreprinderilor sau ale utilizatorilor finali pe care se bazează entitățile. Politicile de igienă cibernetică care cuprind un set de practici de referință comun, inclusiv actualizări de software și hardware, modificări ale parolelor, gestionarea noilor instalări, limitarea conturilor cu acces la nivel de administrator și copierea de rezervă a datelor, permit un cadru proactiv de pregătire și de siguranță și securitate generale în caz de incidente sau amenințări cibernetice. ENISA ar trebui să monitorizeze și să analizeze politicile de igienă cibernetică ale statelor membre.

(50) Sensibilizarea cu privire la securitatea cibernetică și igiena cibernetică sunt esențiale pentru a crește nivelul de securitate cibernetică în Uniune, în special având în vedere numărul crescând de dispozitive conectate care sunt utilizate din ce în ce mai mult în atacurile cibernetice. Ar trebui depuse eforturi pentru a crește nivelul general de conștientizare a riscurilor legate de astfel de dispozitive, în timp ce evaluările la nivelul Uniunii ar putea contribui la asigurarea unei înțelegeri comune a acestor riscuri în cadrul pieței interne.

(51) Statele membre ar trebui să încurajeze utilizarea oricărei tehnologii inovatoare, inclusiv a inteligenței artificiale, a cărei utilizare ar putea îmbunătăți detectarea și prevenirea atacurilor cibernetice, permițând deturnarea resurselor către atacuri cibernetice într-un mod mai eficace. Prin urmare, statele membre ar trebui să încurajeze, în cadrul strategiei lor naționale de securitate cibernetică, activitățile de cercetare și dezvoltare pentru a înlesni utilizarea unor astfel de tehnologii, în special a celor legate de instrumentele automatizate sau semi automatizate în materie de securitate cibernetică și, după caz, schimbul de date necesare pentru formarea utilizatorilor unei astfel de tehnologii și pentru îmbunătățirea acesteia. Utilizarea oricărei tehnologii inovatoare, inclusiv a inteligenței artificiale, ar trebui să respecte dreptul Uniunii în materie de protecție a datelor, inclusiv principiile de protecție a datelor, și anume acuratețea, reducerea la minimum a datelor, echitatea și transparența, precum și securitatea datelor, cum ar fi criptarea de ultimă generație. Cerințele privind protecția datelor începând cu momentul conceperii și protecția implicită a datelor prevăzute în Regulamentul (UE) 2016/679 ar trebui să fie exploatate pe deplin.

(52) Instrumentele și aplicațiile de securitate cibernetică cu sursă deschisă pot contribui la un grad mai ridicat de deschidere și pot avea un impact pozitiv asupra eficienței inovării industriale. Standardele deschise înlesnesc interoperabilitatea dintre instrumentele de securitate, aducând beneficii securității părților interesate din industrie. Instrumentele și aplicațiile de securitate cibernetică cu sursă deschisă pot stimula comunitatea mai largă a dezvoltatorilor, permițând diversificarea furnizorilor. Sursa deschisă poate duce la un proces mai transparent de verificare a instrumentelor legate de securitatea cibernetică și la un proces de descoperire a vulnerabilităților bazat pe comunitate. Prin urmare, statele membre ar trebui să fie în măsură să promoveze utilizarea de software cu sursă deschisă și de standarde deschise prin aplicarea de politici privind utilizarea datelor deschise și a surselor deschise ca parte a securității prin transparență. Politicile care promovează introducerea și utilizarea durabilă a instrumentelor de securitate cibernetică cu sursă deschisă sunt de o importanță deosebită pentru întreprinderile mici și mijlocii care se confruntă cu costuri semnificative pentru punerea în aplicare, care ar putea fi reduse prin reducerea nevoii de aplicații sau instrumente specifice.

(53) Utilitățile sunt din ce în ce mai conectate la rețelele digitale din orașe, în scopul îmbunătățirii rețelelor de transport urban, al modernizării instalațiilor de alimentare cu apă și de eliminare a deșeurilor și al creșterii eficienței iluminatului și a încălzirii clădirilor. Respectivele utilități digitalizate sunt vulnerabile la atacurile cibernetice și riscă, în cazul unui atac cibernetic reușit, să prejudicieze cetățenii la scară largă din cauza interconectării lor. Statele membre ar trebui să elaboreze o politică care să abordeze dezvoltarea unor astfel de orașe conectate sau inteligente și efectele lor potențiale asupra societății, ca parte a strategiei lor naționale de securitate cibernetică.

(54) În ultimii ani, Uniunea s-a confruntat cu o creștere exponențială a atacurilor de tip *ransomware*, în care programele malware criptează date și sisteme și solicită o plată de răscumpărare pentru a le decripta. Frecvența și gravitatea tot mai mare a atacurilor de tip *ransomware* pot fi determinate de mai mulți factori, cum ar fi modele diferite de atac, modele de afaceri infracționale în jurul „*ransomware* ca serviciu" (*ransomware as a service*) și criptomonedele, cererile de răscumpărare și intensificarea atacurilor asupra lanțului de aprovizionare. Statele membre ar trebui să elaboreze o politică care să abordeze creșterea numărului de atacuri de tip *ransomware* ca parte a strategiei lor naționale de securitate cibernetică.

(55) Parteneriatele public-private (PPP) în domeniul securității cibernetice pot asigura un cadru adecvat pentru schimbul de cunoștințe, de bune practici și pentru stabilirea unui nivel comun de înțelegere între părțile interesate. Statele membre ar trebui să promoveze politici care stau la baza instituirii unor PPP specifice securității cibernetice. Respectivele politici ar trebui să clarifice, printre altele, domeniul de aplicare și părțile interesate implicate, modelul de administrare, opțiunile de finanțare disponibile, precum și interacțiunea dintre părțile interesate participante în ceea ce privește PPP. PPP pot valorifica cunoștințele specializate ale entităților din sectorul privat pentru a ajuta autoritățile competente în dezvoltarea unor servicii și procese de ultimă generație, inclusiv în schimbul de informații, alertele timpurii, exercițiile pentru amenințări cibernetice și incidente, gestionarea crizelor și planificarea rezilienței.

(56) În strategiile lor naționale de securitate cibernetică, statele membre ar trebui să abordeze nevoile specifice în materie de securitate cibernetică ale întreprinderilor mici și mijlocii. La nivelul Uniunii, întreprinderile mici și mijlocii reprezintă un procentaj ridicat din piața industrială și de afaceri și adesea se luptă să se adapteze la noile practici comerciale într-o lume mai conectată și la mediul digital, în care angajații lucrează de acasă, iar activitățile de afaceri se desfășoară tot mai mult online. Unele întreprinderi mici și mijlocii se confruntă cu provocări specifice în materie de securitate cibernetică, cum ar fi un nivel scăzut de sensibilizare în domeniul cibernetic, lipsa securității informatice de la distanță, costul ridicat al soluțiilor de securitate cibernetică și un nivel crescut de amenințare, cum ar fi programele de tip *ransomware*, pentru care ar trebui să primească îndrumări și ajutor. Întreprinderile mici și mijlocii devin din ce în ce mai mult ținta atacurilor asupra lanțului de aprovizionare, din cauza măsurilor lor mai puțin riguroase de gestionare a riscurilor în materie de securitate cibernetică și a gestionării atacurilor, precum și din cauza faptului că au resurse de securitate limitate. Astfel de atacuri asupra lanțului de aprovizionare nu numai că au

un impact asupra întreprinderilor mici și mijlocii și asupra operațiunilor acestora în mod izolat, ci pot avea, de asemenea, un efect în cascadă rezultând în atacuri mai ample asupra entităților pe care le-au aprovizionat. Prin intermediul strategiilor lor naționale de securitate cibernetică, statele membre ar trebui să ajute întreprinderile mici și mijlocii să abordeze provocările cu care se confruntă în lanțurile lor de aprovizionare. Statele membre ar trebui să aibă un punct de contact pentru întreprinderile mici și mijlocii la nivel național sau regional, care fie să ofere orientări și asistență întreprinderilor mici și mijlocii, fie să le direcționeze către organele corespunzătoare pentru orientare și asistență în ceea ce privește aspectele legate de securitatea cibernetică. Statele membre sunt încurajate, de asemenea, să ofere servicii precum configurarea de site-uri web și înlesnirea jurnalizării pentru microîntreprinderile și întreprinderile mici care nu dispun de aceste capacități.

(57) Ca parte a strategiilor lor naționale de securitate cibernetică, statele membre ar trebui să adopte politici privind promovarea unei protecții cibernetice active ca parte a unei strategii defensive mai ample. În loc să răspundă reactiv, protecția cibernetică activă constă în prevenirea, detectarea, monitorizarea, analizarea și atenuarea în mod activ ale încălcărilor securității rețelei, combinată cu utilizarea capacităților desfășurate în interiorul și în afara rețelei afectate. Aceasta ar putea include oferirea de către statele membre a unor servicii sau instrumente gratuite anumitor entități, inclusiv verificări în regim de autoservire, instrumente de detectare și servicii de retragere. Capacitatea de a partaja și a înțelege rapid și automat informații și analize privind amenințările, alertele privind activitățile cibernetice și acțiunile de răspuns este esențială pentru a permite unitatea eforturilor în prevenirea, detectarea, abordarea și blocarea cu succes a atacurilor împotriva rețelelor și a sistemelor informatice. Protecția cibernetică activă se bazează pe o strategie defensivă care exclude măsurile ofensive.

(58) Întrucât exploatarea vulnerabilităților din cadrul rețelelor și al sistemelor informatice poate provoca perturbări și prejudicii semnificative, identificarea și remedierea rapidă a unor astfel de vulnerabilități constituie un factor important în reducerea riscului. Entitățile care dezvoltă sau administrează rețele și sisteme informatice ar trebui, prin urmare, să stabilească proceduri adecvate de gestionare a vulnerabilităților atunci când acestea sunt descoperite. Întrucât vulnerabilitățile sunt adesea descoperite și divulgate de părți terțe, producătorul sau furnizorul de produse TIC sau servicii TIC ar trebui, de asemenea, să instituie procedurile necesare pentru a primi de la terți informații privind vulnerabilitatea. În acest sens, standardele internaționale ISO/IEC 30111 și ISO/IEC 29147 oferă orientări privind gestionarea și divulgarea vulnerabilităților. Întărirea coordonării dintre persoanele fizice și juridice raportoare și producătorii ori furnizorii de produse TIC sau servicii TIC este deosebit de importantă în scopul facilitării cadrului voluntar de divulgare a vulnerabilităților. Divulgarea coordonată a vulnerabilităților definește un proces structurat prin care informații privind vulnerabilitățile sunt transmise producătorului sau furnizorului de produse TIC sau de servicii TIC potențial vulnerabile într-o manieră care să îi permită acestuia să diagnosticheze și să remedieze vulnerabilitatea înainte ca informațiile detaliate privind vulnerabilitatea să fie dezvăluite unor terțe părți sau publicului. Divulgarea coordonată a vulnerabilităților ar trebui să includă, de asemenea, coordonarea dintre persoana fizică sau juridică raportoare și producătorul sau furnizorul de produse TIC sau de servicii TIC potențial vulnerabile în ceea ce privește calendarul de remediere și publicare a vulnerabilităților.

(59) Comisia, ENISA și statele membre ar trebui să continue să încurajeze alinierea la standardele internaționale și la bunele practici existente din sector în domeniul gestionării riscurilor în materie de securitate cibernetică, de exemplu în domeniul evaluărilor securității lanțului de aprovizionare, al schimbului de informații și al divulgării vulnerabilităților.

(60) Statele membre, în cooperare cu ENISA, ar trebui să ia măsuri pentru a înlesni divulgarea coordonată a vulnerabilităților prin stabilirea unei politici naționale relevante. Ca parte a politicii lor naționale, statele membre ar trebui să își propună să facă față, în măsura posibilului, încercărilor cu care se confruntă cercetătorii în domeniul vulnerabilității, inclusiv expunerea potențială a acestora la răspunderea penală, în conformitate cu dreptul intern. Având în vedere faptul că persoanele fizice și juridice care cercetează vulnerabilități ar putea fi expuse, în unele state membre, răspunderii penale și civile, statele membre sunt încurajate să adopte orientări în ceea ce privește neurmărirea penală a cercetătorilor în domeniul securității informațiilor și exonerarea de răspundere civilă pentru activitățile desfășurate de aceștia.

(61) Statele membre ar trebui să desemneze una din echipele sale CSIRT drept coordonator, acționând, dacă este necesar, ca intermediar de încredere între persoanele fizice sau juridice care raportează și producătorii sau furnizorii de produse TIC sau servicii TIC care ar putea fi afectați de vulnerabilitate. Sarcinile echipei CSIRT desemnate drept coordonator ar trebui să includă identificarea și contactarea entităților în cauză, asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate, negocierea calendarelor de divulgare și gestionarea vulnerabilităților care

afectează mai multe entități (divulgarea coordonată a vulnerabilităților de către mai multe părți). Atunci când vulnerabilitatea raportată ar putea avea un impact semnificativ asupra entităților în mai multe state membre, echipele CSIRT desemnate drept coordonatori ar trebui să coopereze în cadrul rețelei CSIRT, dacă este cazul.

(62) Accesul la informații corecte și în timp util cu privire la vulnerabilitățile care afectează produsele TIC și serviciile TIC contribuie la o mai bună gestionare a riscurilor în materie de securitate cibernetică. Sursele de informații accesibile publicului cu privire la vulnerabilități reprezintă un instrument important pentru entități și pentru utilizatorii serviciilor acestora, dar și pentru autoritățile competente și pentru echipele CSIRT. Din acest motiv, ENISA ar trebui să creeze o bază de date europeană a vulnerabilităților în care entitățile, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, și furnizorii lor de rețele și sisteme informatice, precum și autoritățile competente și echipele CSIRT să poată divulga și înregistra, în mod voluntar, vulnerabilități cunoscute publicului, pentru a permite utilizatorilor să ia măsuri adecvate de atenuare. Scopul acestei baze de date este de a răspunde provocărilor unice pe care le constituie riscurile pentru entitățile din Uniune. În plus, ENISA ar trebui să stabilească o procedură adecvată în ceea ce privește procesul de publicare, pentru a acorda entităților timpul necesar pentru a lua măsuri de atenuare a vulnerabilităților lor și pentru a utiliza măsuri de gestionare a riscului în materie de securitate cibernetică de ultimă generație, precum și seturi de date care pot fi citite automat și interfețele corespunzătoare. Pentru a încuraja o cultură a divulgării vulnerabilităților, divulgarea nu ar trebui să aibă efecte negative asupra persoanei fizice sau juridice raportoare.

(63) Deși există registre sau baze de date ale vulnerabilităților similare, ele sunt găzduite și întreținute de entități care nu sunt stabilite în Uniune. O bază de date europeană a vulnerabilităților întreținută de ENISA ar oferi o mai mare transparență în ceea ce privește procesul de publicare înainte de dezvăluirea oficială a vulnerabilității, precum și reziliență în cazul unei perturbări sau al unei întreruperi ale furnizării de servicii similare. Pentru a evita, în măsura posibilului, dublarea eforturilor și pentru a urmări complementaritatea, ENISA ar trebui să analizeze posibilitatea de a încheia acorduri de cooperare structurată cu registre sau baze de date similare care intră sub jurisdicția unei țări terțe. În special, ENISA ar trebui să analizeze posibilitatea unei cooperări strânse cu operatorii sistemului comun de vulnerabilități și expuneri (CVE).

(64) Grupul de cooperare ar trebui să sprijine și să înlesnească cooperarea strategică și schimbul de informații, precum și să întărească încrederea între statele membre. Grupul de cooperare ar trebui să elaboreze un program de lucru o dată la doi ani. Programul de lucru ar trebui să includă acțiunile ce urmează să fie întreprinse de Grupul de cooperare în vederea punerii în aplicare a obiectivelor și sarcinilor sale. Calendarul pentru instituirea primului program de lucru în temeiul prezentei directive ar trebui să fie aliniat la calendarul ultimului program de lucru stabilit în temeiul Directivei (UE) 2016/1148, pentru a se evita eventualele perturbări ale activității Grupului de cooperare.

(65) Atunci când elaborează documente de orientare, Grupul de cooperare ar trebui, în mod consecvent, să inventarieze soluțiile și experiențele naționale, să evalueze impactul rezultatelor Grupului de cooperare asupra abordărilor naționale, să discute provocările legate de punerea în aplicare și să formuleze recomandări specifice, în special în ceea ce privește înlesnirea alinierii în transpunerea prezentei directive în statele membre, care să fie abordată printr-o mai bună punere în aplicare a normelor existente. Grupul de cooperare ar putea, de asemenea, să inventarieze soluțiile naționale pentru a promova compatibilitatea soluțiilor de securitate cibernetică aplicate în fiecare sector specific din întreaga Uniune. Acest lucru este deosebit de relevant pentru sectoarele care au un caracter internațional sau transfrontalier.

(66) Grupul de cooperare ar trebui să rămână un forum flexibil și să poată reacționa la prioritățile și provocările noi și în schimbare în materie de politici, ținând seama, în același timp, de disponibilitatea resurselor. Acesta ar putea organiza reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta despre activitățile pe care le desfășoară Grupul de cooperare și a colecta date și informații cu privire la provocările emergente în materie de politici. În plus, Grupul de cooperare ar trebui să efectueze o evaluare periodică a situației amenințărilor sau incidentelor cibernetice, cum ar fi cele de tip *ransomware*. Pentru a întări cooperarea la nivelul Uniunii, Grupul de cooperare ar trebui să aibă în vedere invitarea instituțiilor, organelor, oficiilor și agențiilor

relevante ale Uniunii implicate în politica de securitate cibernetică, cum ar fi Parlamentul European, Europol, Comitetul european pentru protecția datelor, Agenția Uniunii Europene pentru Siguranța Aviației, instituită prin Regulamentul (UE) 2018/1139, și Agenția Uniunii Europene pentru Programul Spațial, instituită prin Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului ([14]), să participe la lucrările sale.

(67) Autoritățile competente și echipele CSIRT ar trebui să aibă posibilitatea să participe la programe de schimb pentru funcționari din alte state membre, într-un cadru specific și, după caz, sub rezerva autorizării de securitate necesare a funcționarilor care participă la aceste programe de schimb, în vederea îmbunătățirii cooperării și a întăririi încrederii dintre statele membre. Autoritățile competente ar trebui să ia măsurile necesare ca funcționarii din alte state membre să poată juca un rol efectiv în activitățile autorității competente gazdă sau ale echipelor CSIRT gazdă.

(68) Statele membre ar trebui să contribuie la instituirea cadrului UE de răspuns la crizele de securitate cibernetică, astfel cum este prevăzut în Recomandarea (UE) 2017/1584 a Comisiei ([15]), prin intermediul rețelelor de cooperare existente, în special Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), rețeaua CSIRT și Grupul de cooperare. EU-CyCLONe și rețeaua CSIRT ar trebui să coopereze pe baza modalităților procedurale care precizează detaliile acestei cooperări și să evite orice suprapunere a sarcinilor. Regulamentul de procedură al EU-CyCLONe ar trebui să precizeze în detaliu modalitățile prin care ar trebui să funcționeze această rețea, inclusiv rolurile, mijloacele de cooperare, interacțiunile rețelei cu alți actori relevanți și modelele pentru schimbul de informații, precum și mijloacele de comunicare. Pentru gestionarea crizelor la nivelul Uniunii, părțile relevante ar trebui să se bazeze pe mecanismul integrat al UE pentru un răspuns politic la crize în temeiul Deciziei de punere în aplicare (UE) 2018/1993 a Consiliului ([16]) (mecanismul IPCR). În acest scop, Comisia ar trebui să utilizeze procesul ARGUS de coordonare transsectorială la nivel înalt în situații de criză. În cazul în care criza presupune o importantă dimensiune externă sau de politică de securitate și apărare comună, ar trebui activat mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă.

(69) În conformitate cu anexa la Recomandarea (UE) 2017/1584, un incident de securitate cibernetică de mare amploare ar trebui să însemne un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre. În funcție de cauza și de impactul lor, incidentele de securitate cibernetică de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne sau să prezinte riscuri grave pentru securitatea și siguranța publică, pentru entități sau cetățeni, în mai multe state membre sau în Uniune în ansamblul său. Având în vedere domeniul larg de aplicare și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele, oficiile și agențiile relevante ale Uniunii ar trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune.

(70) Incidentele de securitate cibernetică de mare amploare și crizele de la nivelul Uniunii necesită acțiuni coordonate pentru a asigura un răspuns rapid și eficace, din cauza gradului ridicat de interdependență dintre sectoare și statele membre. Disponibilitatea unor rețele și sisteme informatice reziliente din punct de vedere cibernetic, precum și disponibilitatea, confidențialitatea și integritatea datelor sunt vitale pentru securitatea Uniunii și pentru protecția cetățenilor, întreprinderilor și instituțiilor acesteia împotriva incidentelor și a amenințărilor cibernetice, precum și pentru consolidarea încrederii persoanelor și a organizațiilor în capacitatea Uniunii de a promova și de a proteja un spațiu cibernetic global, deschis, liber, stabil și sigur, bazat pe drepturile omului, libertățile fundamentale, democrație și statul de drept.

([14]) Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a Programului spațial al Uniunii și a Agenției Uniunii Europene pentru Programul spațial și de abrogare a Regulamentelor (UE) nr. 912/2010, (UE) nr. 1285/2013 și (UE) nr. 377/2014 și a Deciziei nr. 541/2014/UE (JO L 170, 12.5.2021, p. 69).

([15]) Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

([16]) Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize (JO L 320, 17.12.2018, p. 28).

(71) EU-CyCLONe ar trebui să acționeze ca intermediar între nivelul tehnic și cel politic în timpul incidentelor de securitate cibernetică de mare amploare și al crizelor și ar trebui să consolideze cooperarea la nivel operațional și să sprijine procesul decizional la nivel politic. În cooperare cu Comisia, având în vedere competența Comisiei în domeniul gestionării crizelor, EU-CyCLONe ar trebui să se bazeze pe constatările rețelei CSIRT și să își utilizeze propriile capacități pentru a crea o analiză a impactului incidentelor de securitate cibernetică de mare amploare și al crizelor.

(72) Atacurile cibernetice au un caracter transfrontalier, iar un incident semnificativ poate perturba și afecta infrastructurile critice de informații de care depinde buna funcționare a pieței interne. Recomandarea (UE) 2017/1584 abordează rolul tuturor actorilor relevanți. În plus, Comisia este responsabilă, în cadrul mecanismului de protecție civilă al Uniunii instituit prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului ([17]), de acțiunile generale în materie de pregătire, inclusiv de gestionarea Centrului de coordonare a răspunsului la situații de urgență și a sistemului comun de comunicare și informare în caz de urgență, de menținerea și dezvoltarea în continuare a capacității de conștientizare a situației și de analiză, precum și de instituirea și gestionarea capacității de a mobiliza și de a trimite echipe de experți în cazul unei cereri de asistență din partea unui stat membru sau a unei țări terțe. Comisia are, de asemenea, responsabilitatea de a furniza rapoarte analitice pentru mecanismul IPCR în temeiul Deciziei de punere în aplicare (UE) 2018/1993, inclusiv în ceea ce privește conștientizarea situației și pregătirea în materie de securitate cibernetică, precum și conștientizarea situației și răspunsul la situații de criză în domeniile agriculturii, condițiilor meteorologice nefavorabile, cartografierii și prognozelor privind conflictele, sistemelor de alertă timpurie în caz de dezastre naturale, urgențelor sanitare, supravegherii bolilor infecțioase, sănătății plantelor, incidentelor chimice, siguranței alimentelor și a hranei pentru animale, sănătății animalelor, migrației, vămilor, urgențelor nucleare și radiologice și energiei.

(73) După caz, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare, ale rețelei CSIRT, precum și ale EU-CyCLONe. Astfel de acorduri ar trebui să asigure interesele Uniunii și o protecție adecvată a datelor. Acest lucru nu ar trebui să excludă dreptul statelor membre de a coopera cu țări terțe în legătură cu gestionarea vulnerabilităților și a riscurilor în materie de securitate cibernetică, înlesnind raportarea și schimbul general de informații în conformitate cu dreptul Uniunii.

(74) Pentru a facilita punerea în aplicare eficace a prezentei directive în ceea ce privește, printre altele, gestionarea vulnerabilităților, măsurile de gestionare a riscurilor în materie de securitate cibernetică, obligațiile de raportare și acordurile privind schimbul de informații în materie de securitate cibernetică, statele membre pot coopera cu țări terțe și pot desfășura activități considerate a fi adecvate acestui scop, inclusiv schimburi de informații cu privire la amenințări cibernetice, incidente, vulnerabilități, instrumente și metode, tactici, tehnici și proceduri, pregătire și exerciții pentru gestionarea crizelor în materie de securitate cibernetică, formare, consolidare a încrederii și acorduri structurate privind schimbul de informații.

(75) Ar trebui introduse evaluări *inter pares* pentru a se putea învăța din experiențe comune, a consolida încrederea reciprocă și a atinge un nivel comun ridicat de securitate cibernetică. Evaluările *inter pares* pot conduce la idei și recomandări valoroase, consolidând capacitățile generale în materie de securitate cibernetică, creând o altă cale funcțională pentru schimbul de bune practici între statele membre și contribuind la îmbunătățirea nivelurilor de maturitate ale statelor membre în materie de securitate cibernetică. În plus, evaluările *inter pares* ar trebui să țină seama de rezultatele unor mecanisme similare, cum ar fi sistemul de evaluare *inter pares* al rețelei CSIRT, să aducă valoare adăugată și să evite suprapunerile. Implementarea sistemului de evaluări *inter pares* nu ar trebui să aducă atingere dreptului Uniunii sau dreptului intern privind protecția informațiilor confidențiale sau clasificate.

(76) Grupul de cooperare ar trebui să stabilească o metodologie de autoevaluare pentru statele membre, cu scopul de a acoperi factori precum nivelul de punere în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare, nivelul capacităților și eficacitatea exercitării sarcinilor autorităților competente, capacitățile operaționale ale echipelor CSIRT, nivelul de punere în aplicare a asistenței reciproce, nivelul de punere în aplicare a acordurilor privind schimbul de informații în materie de securitate cibernetică sau aspecte specifice de natură transfrontalieră sau transsectorială. Statele membre ar trebui să fie încurajate să efectueze autoevaluări în mod regulat și să prezinte și să discute rezultatele autoevaluării lor în cadrul Grupului de cooperare.

([17]) Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).

(77) Responsabilitatea de a asigura securitatea rețelelor și a sistemelor informatice revine în mare măsură entităților esențiale și entităților importante. Ar trebui să se promoveze și să se dezvolte o cultură a gestionării riscurilor, care să implice evaluări ale riscurilor și aplicarea unor măsuri de gestionare a riscurilor în materie de securitate cibernetică adecvate riscurilor întâmpinate.

(78) Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să țină seama de gradul de dependență al entității esențiale sau al entității importante de rețelele și sistemele informatice și să includă măsuri pentru identificarea oricăror riscuri de incidente, prevenirea și detectarea incidentelor, răspunsul la incidente și redresarea în urma acestora, precum și pentru atenuarea impactului lor. Securitatea rețelelor și a sistemelor informatice ar trebui să includă securitatea datelor stocate, transmise și prelucrate. Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să asigure o analiză sistemică, ținând seama de factorul uman, cu scopul de a obține o imagine completă privind securitatea rețelelor și a sistemelor informatice.

(79) Întrucât amenințările la adresa securității rețelelor și a sistemelor informatice pot avea origini diferite, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie bazate pe o abordare multirisc, care vizează protecția rețelelor și a sistemelor informatice și a mediului fizic al acestor sisteme împotriva unor evenimente cum ar fi furturile, incendiile, inundațiile, defecțiunile la nivelul telecomunicațiilor sau al alimentării cu energie, accesul fizic neautorizat și deteriorarea și interferența la nivelul informațiilor deținute de o entitate esențială sau de o entitate importantă sau al echipamentelor entității respective de prelucrare a informațiilor, care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora. Prin urmare, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să abordeze, de asemenea, securitatea fizică și a mediului în cazul rețelelor și al sistemelor informatice prin includerea unor măsuri pentru a le proteja împotriva defecțiunilor de sistem, a erorilor umane, a acțiunilor răuvoitoare sau a fenomenelor naturale, în conformitate cu standardele europene și internaționale, cum ar fi cele incluse în seria ISO/IEC 27000. În acest sens, entitățile esențiale și entitățile importante ar trebui, în cadrul măsurilor lor de gestionare a riscurilor în materie de securitate cibernetică, să abordeze și securitatea resurselor umane și să dispună de politici adecvate de control al accesului. Măsurile respective ar trebui să respecte Directiva (UE) 2022/2557.

(80) Pentru a dovedi respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică și în absența unor sisteme europene adecvate de certificare a securității cibernetice adoptate în conformitate cu Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului ([18]), statele membre ar trebui, cu consultarea Grupului de cooperare și a Grupului european pentru certificarea securității cibernetice, să promoveze utilizarea standardelor europene și internaționale relevante de către entitățile esențiale și entitățile importante sau pot solicita entităților să utilizeze produse TIC, servicii TIC și procese TIC certificate.

(81) Pentru a se evita impunerea unei sarcini financiare și administrative disproporționate asupra entităților esențiale și entităților importante, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri și, după caz, de standardele europene și internaționale relevante, precum și de costul punerii lor în aplicare.

(82) Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu gradul de expunere a entității esențiale sau a entității importante la riscuri și cu impactul societal și economic pe care un incident l-ar avea. Atunci când se stabilesc măsuri de gestionare a riscurilor în materie de securitate cibernetică adaptate entităților esențiale și entităților importante, ar trebui să se țină seama în mod corespunzător de expunerea divergentă la risc a entităților esențiale și a entităților importante, cum ar fi importanța critică a entității, riscurile, inclusiv riscurile societale, la care este expusă, dimensiunea entității și probabilitatea producerii incidentelor și gravitatea acestora, inclusiv impactul lor societal și economic.

([18]) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

(83) Entitățile esențiale și entitățile importante ar trebui să asigure securitatea rețelelor și a sistemelor informatice pe care le utilizează pentru a-și desfășura activitatea. Aceste sisteme sunt în principal rețele și sisteme informatice private, care sunt gestionate de către personalul IT intern al entităților esențiale și al entităților importante sau a căror securitate a fost externalizată. Măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare prevăzute în prezenta directivă ar trebui să li se aplice entităților esențiale și entităților importante relevante, indiferent dacă entitățile respective întrețin la nivel intern rețelele și sistemele lor informatice sau dacă externalizează întreținerea acestora.

(84) Având în vedere caracterul lor transfrontalier, furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de *cloud computing*, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere ar trebui să facă obiectul unui grad ridicat de armonizare la nivelul Uniunii. Prin urmare, implementarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică în ceea ce privește respectivele entități ar trebui facilitată printr-un act de punere în aplicare.

(85) Abordarea riscurilor care decurg din lanțul de aprovizionare al unei entități și din relația acesteia cu furnizorii săi, cum ar fi furnizorii de servicii de stocare și de prelucrare de date sau furnizorii de servicii de securitate gestionate și editorii de software, este deosebit de importantă, având în vedere prevalența incidentelor în care entitățile au fost victime ale atacurilor cibernetice și în care actori răuvoitori au fost în măsură să compromită securitatea rețelelor și a sistemelor informatice ale unei entități prin exploatarea vulnerabilităților care afectează produsele și serviciile unei părți terțe. Prin urmare, entitățile esențiale și entitățile importante ar trebui să evalueze și să țină seama de calitatea generală și de reziliența produselor și a serviciilor, de măsurile de gestionare a riscurilor în materie de securitate cibernetică integrate în acestea, precum și de practicile în materie de securitate cibernetică ale furnizorilor și ale prestatorilor lor de servicii, inclusiv de procedurile lor de dezvoltare sigure. Entitățile esențiale și entitățile importante ar trebui, în special, să fie încurajate să includă măsuri de gestionare a riscurilor în materie de securitate cibernetică în acordurile contractuale cu furnizorii lor direcți și cu prestatorii lor de servicii direcți. Entitățile respective ar putea lua în considerare riscurile generate de alte niveluri de furnizori și de prestatori de servicii.

(86) În rândul furnizorilor de servicii, furnizorii de servicii de securitate gestionate în domenii precum răspunsul în caz de incidente, testele de penetrare, auditurile de securitate și consultanța joacă un rol deosebit de important în sprijinirea entităților în eforturile lor de a preveni și de a detecta incidente, de a răspunde la acestea și de a se redresa după incidente. Totuși, și furnizorii de servicii de securitate gestionate au fost ținta atacurilor cibernetice și, din cauza integrării lor strânse în operațiunile entităților, prezintă un risc deosebit. Prin urmare, entitățile esențiale și entitățile importante ar trebui să dea dovadă de o diligență sporită în selectarea unui furnizor de servicii de securitate gestionate.

(87) Autoritățile competente, în contextul sarcinilor lor de supraveghere, pot beneficia, de asemenea, de servicii de securitate cibernetică, cum ar fi audituri de securitate, teste de penetrare sau răspunsuri la incidente.

(88) Entitățile esențiale și entitățile importante ar trebui, de asemenea, să abordeze riscurile care decurg din interacțiunile și din relațiile lor cu alte părți interesate în cadrul unui ecosistem mai larg, inclusiv în ceea ce privește combaterea spionajului industrial și protejarea secretelor comerciale. În special, entitățile respective ar trebui să ia măsurile adecvate pentru a se asigura că activitatea lor de cooperare cu instituțiile academice și de cercetare se desfășoară în conformitate cu politicile lor în materie de securitate cibernetică și respectă bunele practici în ceea ce privește accesul și diseminarea în condiții de siguranță a informațiilor, în general, și protecția proprietății intelectuale, în special. În mod similar, având în vedere importanța și valoarea datelor pentru activitățile pe care le desfășoară entitățile esențiale și entitățile importante, atunci când se bazează pe servicii de transformare și de analiză a datelor furnizate de terți, entitățile respective ar trebui să ia toate măsurile adecvate de gestionare a riscurilor în materie de securitate cibernetică.

(89) Entitățile esențiale și entitățile importante ar trebui să adopte o gamă largă de practici de bază în materie de igienă cibernetică, cum ar fi principii „încredere zero”, actualizări ale software-ului, configurarea dispozitivelor, segmentarea rețelelor, gestionarea identității și a accesului sau sensibilizarea utilizatorilor, să organizeze cursuri pentru personalul lor și să crească gradul de informare cu privire la amenințările cibernetice, *phishing* sau tehnici de inginerie socială. În plus, entitățile respective ar trebui să își evalueze propriile capacități în materie de securitate cibernetică și, atunci când este cazul, să urmărească integrarea tehnologiilor de îmbunătățire a securității cibernetice, cum ar fi sisteme de inteligență artificială sau de învățare automată pentru a consolida capacitățile proprii și securitatea rețelelor și a sistemelor informatice.

(90) Pentru a aborda în continuare principalele riscuri din cadrul lanțului de aprovizionare și pentru a oferi asistență entităților esențiale și entitățile importante care își desfășoară activitatea în sectoarele reglementate de prezenta directivă în privința gestionării adecvate a riscurilor legate de lanțul de aprovizionare și de furnizori, Grupul de cooperare ar trebui să efectueze, în cooperare cu Comisia și ENISA și, după caz, după consultarea părților interesate relevante, inclusiv din industrie, evaluări coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice, astfel cum s-a procedat deja în cazul rețelelor 5G ca urmare a Recomandării (UE) 2019/534 a Comisiei ([19]), cu scopul de a identifica, pentru fiecare sector în parte, serviciile TIC, sistemele TIC sau produsele TIC critice, amenințările și vulnerabilitățile relevante. Astfel de evaluări coordonate ale riscurilor de securitate ar trebui să identifice măsurile, planurile de atenuare și cele mai bune practici împotriva dependențelor critice, a potențialelor puncte unice de defecțiune, a amenințărilor, a vulnerabilităților și a altor riscuri asociate lanțului de aprovizionare și ar trebui să exploreze modalități de a încuraja adoptarea lor pe scară mai largă de către entități esențiale și entități importante. Printre factorii de risc potențiali fără caracter tehnic, cum ar fi influența nejustificată a unei țări terțe asupra furnizorilor și a prestatorilor de servicii, în special în cazul modelelor alternative de guvernanță, se numără vulnerabilitățile ascunse sau „ușile secrete” și eventualele întreruperi sistemice ale aprovizionării, în special în cazul blocajelor tehnologice sau al dependenței de furnizori.

(91) Evaluările coordonate ale riscurilor de securitate din cadrul lanțurilor de aprovizionare critice, având în vedere caracteristicile sectorului în cauză, ar trebui să țină seama atât de factori tehnici, cât și, după caz, de factori fără caracter tehnic, inclusiv de cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată de UE a riscurilor legate de securitatea cibernetică a rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică 5G convenit de Grupul de cooperare. Pentru a identifica lanțurile de aprovizionare care ar trebui să facă obiectul unei evaluări coordonate a riscurilor de securitate, ar trebui să se țină seama de următoarele criterii: (i) în ce măsură entitățile esențiale și entitățile importante utilizează și se bazează pe servicii TIC, sisteme TIC sau produse TIC critice specifice; (ii) relevanța serviciilor TIC, a sistemelor TIC sau a produselor TIC critice specifice pentru îndeplinirea funcțiilor critice sau sensibile, printre care se numără și prelucrarea datelor cu caracter personal; (iii) disponibilitatea unor servicii TIC, sisteme TIC sau produse TIC alternative; (iv) reziliența întregului lanț de aprovizionare cu servicii TIC, sisteme TIC sau produse TIC pe parcursul întregului lor ciclu de viață împotriva evenimentelor perturbatoare și (v) pentru serviciile TIC, sistemele TIC sau produsele TIC emergente, potențiala lor importanță viitoare pentru activitățile entităților. În plus, ar trebui să se pună un accent deosebit pe serviciile TIC, sistemele TIC sau produsele TIC care fac obiectul unor cerințe specifice impuse de țări terțe.

(92) Pentru a raționaliza obligațiile impuse furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului și prestatorilor de servicii de încredere în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, precum și pentru a permite acestor entități și autorităților competente în temeiul Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului ([20]) și, respectiv, al Regulamentului (UE) nr. 910/2014 să beneficieze de cadrul juridic instituit prin prezenta directivă, inclusiv desemnarea unei echipe CSIRT responsabile de gestionarea incidentelor, participarea autorităților competente în cauză la activitățile Grupului de cooperare și ale rețelei CSIRT, entitățile respective ar trebui să intre în domeniul de aplicare al prezentei directive. Prin urmare, dispozițiile corespunzătoare prevăzute în Regulamentul (UE) nr. 910/2014 și în Directiva (UE) 2018/1972 referitoare la impunerea de cerințe de securitate și de notificare pentru aceste tipuri de entități ar trebui eliminate. Normele privind obligațiile de raportare prevăzute în prezenta directivă nu ar trebui să aducă atingere nici Regulamentului (UE) 2016/679, nici Directivei 2002/58/CE.

(93) Obligațiile în materie de securitate cibernetică prevăzute în prezenta directivă ar trebui considerate a fi complementare cerințelor impuse prestatorilor de servicii de încredere în temeiul Regulamentului (UE) nr. 910/2014. Prestatorilor de servicii de încredere ar trebui să li se impună să ia toate măsurile adecvate și proporționale pentru a gestiona riscurile la care sunt expuse serviciile lor, inclusiv în ceea ce privește clienții și beneficiarii terți, și să raporteze incidentele în temeiul prezentei directive. Astfel de obligații în materie de securitate cibernetică și de raportare ar trebui să vizeze, de asemenea, protecția fizică a serviciilor prestate. Cerințele pentru prestatorii de servicii de încredere calificați prevăzute la articolul 24 din Regulamentul (UE) nr. 910/2014 continuă să se aplice.

([19]) Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 intitulată „Securitatea cibernetică a rețelelor 5G” (JO L 88, 29.3.2019, p. 42).

([20]) Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

(94) Statele membre pot atribui rolul autorităților competente pentru serviciile de încredere organismelor de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, pentru a asigura continuarea practicilor curente și pentru a valorifica cunoștințele și experiența dobândite odată cu aplicarea regulamentului respectiv. Într-un astfel de caz, autoritățile competente în temeiul prezentei directive ar trebui să coopereze îndeaproape și în timp util cu respectivele organisme de supraveghere prin schimburi de informații relevante, pentru a asigura supravegherea eficace și conformarea prestatorilor de servicii de încredere cu cerințele prevăzute în prezenta directivă și în Regulamentul (UE) nr. 910/2014. Dacă este cazul, echipa CSIRT sau autoritatea competentă în temeiul prezentei directive ar trebui să informeze imediat organismul de supraveghere în temeiul Regulamentului (UE) nr. 910/2014 cu privire la orice amenințare cibernetică semnificativă sau incident notificat care afectează serviciile de încredere, precum și cu privire la orice încălcare de către un prestator de servicii de încredere a prezentei directive. În scopul raportării, statele membre pot utiliza, după caz, punctul de intrare unic instituit pentru a realiza o raportare automată și comună a incidentelor atât către organismul de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, cât și către echipa CSIRT sau autoritatea competentă în temeiul prezentei directive.

(95) După caz și pentru a evita perturbările inutile, orientările naționale existente adoptate pentru transpunerea normelor referitoare la măsurile de securitate prevăzute la articolele 40 și 41 din Directiva (UE) 2018/1972 ar trebui să fie luate în considerare la transpunerea prezentei directive, valorificând astfel cunoștințele și competențele deja dobândite în temeiul Directivei (UE) 2018/1972 privind măsurile de securitate și notificarea incidentelor. ENISA poate, de asemenea, să elaboreze orientări privind cerințele în materie de securitate și obligațiile de raportare pentru furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, pentru a facilita armonizarea și tranziția și pentru a reduce la minimum perturbările. Statele membre pot atribui rolul de autorități competente pentru comunicațiile electronice autorităților de reglementare naționale în temeiul Directivei (UE) 2018/1972, pentru a asigura continuarea practicilor curente și pentru a valorifica cunoștințele și experiența dobândite ca rezultat al punerii în aplicare a respectivei directive.

(96) Având în vedere importanța crescândă a serviciilor de comunicații interpersonale care nu se bazează pe numere, astfel cum sunt definite în Directiva (UE) 2018/1972, este necesar să se asigure că astfel de servicii fac, de asemenea, obiectul unor cerințe corespunzătoare în materie de securitate, în conformitate cu natura lor specifică și cu importanța lor economică. Pe măsură ce suprafața de atac continuă să se extindă, serviciile de comunicații interpersonale care nu se bazează pe numere, cum ar fi serviciile de mesagerie, devin vectori de atac larg răspândiți. Actorii răuvoitori utilizează platformele pentru a comunica și a atrage victimele să deschidă pagini web compromise, crescând așadar probabilitatea unor incidente care implică exploatarea datelor cu caracter personal și, prin extensie, securitatea rețelelor și a sistemelor informatice. Furnizorii serviciilor de comunicații interpersonale care nu se bazează pe numere ar trebui să asigure un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscurilor prezentate. Având în vedere faptul că furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere nu exercită în mod normal un control efectiv asupra transmiterii semnalelor în rețea, gradul de risc aferent unor astfel de servicii poate fi considerat, în unele privințe, mai redus decât în cazul serviciilor tradiționale de comunicații electronice. Același lucru este valabil și pentru serviciile de comunicații interpersonale, astfel cum sunt definite în Directiva (UE) 2018/1972, care utilizează numere și care nu exercită un control efectiv asupra transmiterii semnalului.

(97) Piața internă depinde mai mult decât oricând de funcționarea internetului. Serviciile ale aproape tuturor entităților esențiale și entităților importante depind de serviciile furnizate pe internet. Pentru a asigura furnizarea fără probleme a serviciilor asigurate de entități esențiale și entități importante, este important ca toți furnizorii de rețele publice de comunicații electronice să dispună de măsuri adecvate în materie de securitate cibernetică și să raporteze incidentele semnificative legate de aceasta. Statele membre ar trebui să se asigure că securitatea rețelelor publice de comunicații electronice este menținută și că interesele lor vitale de securitate sunt protejate împotriva sabotajului și a spionajului. Întrucât conectivitatea internațională consolidează și accelerează digitalizarea competitivă a Uniunii și a economiei sale, incidentele care afectează cablurile de comunicații submarine ar trebui raportate echipei CSIRT sau, după caz, autorității competente. Strategia națională de securitate cibernetică ar trebui, după caz, să țină seama de securitatea cibernetică a cablurilor de comunicații submarine și să includă o inventariere a riscurilor potențiale în materie de securitate cibernetică și măsuri de atenuare pentru a asigura cel mai înalt nivel de protecție a acestora.

(98) Pentru a se garanta securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice accesibile publicului, ar trebui promovată utilizarea tehnologiilor de criptare, în special a criptării de la un capăt la altul, și a conceptelor de securitate centrate pe date, cum ar fi cartografierea, segmentarea, etichetarea, politica de acces și gestionarea accesului, precum și deciziile privind accesul automat. Atunci când este necesar, utilizarea criptării, în special a criptării de la un capăt la altul, ar trebui să fie obligatorie pentru furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, în conformitate cu principiile securității și confidențialității implicite și din momentul conceperii, în sensul prezentei directive. Utilizarea criptării de la un capăt la altul ar trebui să fie reconciliată cu competențele statelor membre de a asigura protecția intereselor lor esențiale în materie de securitate și de siguranță publică și de a permite prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor în conformitate cu dreptul Uniunii. Acest lucru nu ar trebui însă să slăbească criptarea de la un capăt la altul, care este o tehnologie esențială pentru protecția eficace a datelor și a confidențialității și pentru securitatea comunicațiilor.

(99) Pentru a proteja securitatea și a preveni abuzul și manipularea rețelelor publice de comunicații electronice și ale serviciilor de comunicații electronice accesibile publicului, ar trebui promovată utilizarea unor standarde de rutare sigure pentru a asigura integritatea și robustețea funcțiilor de rutare în întregul ecosistem al furnizorilor de servicii de acces la internet.

(100) Pentru a proteja funcționalitatea și integritatea internetului și pentru a promova securitatea și reziliența DNS, părțile interesate relevante, inclusiv entitățile din sectorul privat din Uniune, furnizorii de servicii de comunicații electronice accesibile publicului, în special furnizorii de servicii de acces la internet, și furnizorii de motoare de căutare online, ar trebui încurajate să adopte o strategie de diversificare a rezoluției DNS. În plus, statele membre ar trebui să încurajeze dezvoltarea și utilizarea unui serviciu european public și sigur de rezoluție a DNS.

(101) Prezenta directivă stabilește o abordare în mai multe etape a raportării incidentelor semnificative pentru a se ajunge la un echilibru adecvat între, pe de o parte, raportarea rapidă care contribuie la atenuarea unei eventuale răspândiri a incidentelor semnificative și le permite entităților esențiale și entităților importante să solicite asistență și, pe de altă parte, raportarea aprofundată, care permite extragerea unor învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența cibernetică a entităților individuale și a unor sectoare întregi. În acest sens, prezenta directivă ar trebui să includă raportarea incidentelor care, pe baza unei evaluări inițiale efectuate de entitatea în cauză, ar putea cauza entității respective perturbări operaționale ale serviciilor sau pierderi financiare substanțiale sau ar putea afecta alte persoane fizice sau juridice, provocând prejudicii materiale sau morale considerabile. O astfel de evaluare inițială ar trebui să ia în considerare, printre altele, rețeaua și sistemele informatice afectate, în special importanța acestora în furnizarea serviciilor entității, gravitatea și caracteristicile tehnice ale unei amenințări cibernetice și orice vulnerabilitate subiacentă care este exploatată, precum și experiența entității în ceea ce privește incidente similare. Indicatori precum măsura în care funcționarea serviciului este afectată, durata unui incident sau numărul de destinatari afectați ai serviciilor ar putea juca un rol important în identificarea gravității perturbării operaționale a serviciului.

(102) Dacă entitățile esențiale sau entitățile importante iau cunoștință de un incident semnificativ, acestea ar trebui să aibă obligația de a transmite o alertă timpurie fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore. Această alertă timpurie ar trebui să fie urmată de o notificare a incidentului. Entitățile în cauză ar trebui să transmită o notificare a incidentului fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, cu scopul, în special, de a actualiza informațiile transmise prin alerta timpurie și de a prezenta o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili. Un raport final ar trebui prezentat în termen de cel mult o lună de la notificarea incidentului. Alerta timpurie ar trebui să includă numai informațiile necesare pentru a aduce la cunoștința echipei CSIRT sau, după caz, a autorității competente incidentul semnificativ și pentru a permite entității în cauză să solicite asistență, dacă este necesar. O astfel de alertă timpurie, după caz, ar trebui să indice dacă se suspectează că incidentul semnificativ a fost cauzat de acte ilegale sau răuvoitoare și dacă este probabil să aibă un impact transfrontalier. Statele membre ar trebui să se asigure că obligația de a transmite respectiva alertă timpurie sau notificarea ulterioară a incidentului nu deviază resursele entității notificatoare de la activitățile legate de gestionarea incidentelor cărora ar trebui să li se acorde prioritate, pentru a preîntâmpina ca

obligațiile de raportare a incidentului fie să devieze resurse de la gestionarea răspunsului la incidente semnificative, fie să compromită în alt mod eforturile entității în acest sens. În cazul unui incident în desfășurare la momentul prezentării raportului final, statele membre ar trebui să se asigure că entitățile în cauză prezintă la momentul respectiv un raport privind progresele înregistrate și un raport final în termen de o lună de la gestionarea incidentului semnificativ.

(103) După caz, entitățile esențiale și entitățile importante ar trebui să comunice fără întârziere destinatarilor serviciilor lor orice măsură sau măsură corectivă pe care o pot lua pentru a atenua riscurile generate de o amenințare cibernetică semnificativă. Entitățile respective ar trebui, după caz și în special dacă este probabil ca amenințarea cibernetică semnificativă să se materializeze, să își informeze, de asemenea, destinatarii serviciilor cu privire la amenințarea în sine. Cerința de a informa destinatarii cu privire la amenințările cibernetice semnificative ar trebui îndeplinită cu maxima diligență posibilă, dar nu ar trebui să scutească entitățile respective de obligația de a lua, pe cheltuiala proprie, măsuri adecvate și imediate pentru a preveni sau remedia orice astfel de amenințare și pentru a restabili nivelul normal de securitate al serviciului. Furnizarea unor astfel de informații privind amenințările cibernetice semnificative la adresa securității destinatarilor serviciilor ar trebui să fie gratuită și informațiile ar trebui să fie redactate într-un limbaj ușor de înțeles.

(104) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului ar trebui să pună în aplicare securitatea din momentul conceperii și securitatea implicită și să își informeze destinatarii serviciilor cu privire la amenințările cibernetice semnificative și cu privire la măsurile pe care le pot lua pentru a-și proteja securitatea dispozitivelor și a comunicațiilor, de exemplu prin folosirea unor anumite tipuri de software sau de tehnologii de criptare.

(105) O abordare proactivă a amenințărilor cibernetice este o componentă vitală a măsurilor de gestionare a riscurilor în materie de securitate cibernetică, care ar trebui să permită autorităților competente să prevină în mod eficace materializarea amenințărilor cibernetice în incidente care pot cauza prejudicii materiale sau morale considerabile. În acest scop, notificarea amenințărilor cibernetice prezintă o importanță majoră. În acest sens, entitățile sunt încurajate să raporteze în mod voluntar amenințările cibernetice.

(106) Pentru a simplifica raportarea informațiilor solicitate în temeiul prezentei directive, precum și pentru a reduce sarcina administrativă pentru entități, statele membre ar trebui să pună la dispoziție mijloace tehnice, cum ar fi un punct de intrare unic, sisteme automatizate, formulare online, interfețe ușor de utilizat, modele, platforme specifice pentru utilizarea de către entități, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, pentru transmiterea informațiilor relevante care trebuie raportate. Finanțarea din partea Uniunii în sprijinul punerii în aplicare a prezentei directive, în special în cadrul programului Europa digitală instituit prin Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului ([21]), ar putea include sprijin pentru punctele de intrare unice. În plus, entitățile se află adesea într-o situație în care, din cauza caracteristicilor sale, un anumit incident trebuie raportat mai multor autorități ca urmare a obligațiilor de notificare incluse în diferite instrumente juridice. Astfel de cazuri creează o sarcină administrativă suplimentară și ar putea conduce, de asemenea, la incertitudini în ceea ce privește formatul unor asemenea notificări și procedurile aferente acestora. În cazul în care se instituie un punct de intrare unic, statele membre sunt încurajate, de asemenea, să utilizeze respectivul punct de intrare unic pentru notificarea incidentelor de securitate solicitată în temeiul altor acte legislative ale Uniunii, cum ar fi Regulamentul (UE) 2016/679 și Directiva 2002/58/CE. Utilizarea unui astfel de punct de intrare unic pentru raportarea incidentelor de securitate în temeiul Regulamentului (UE) 2016/679 și al Directivei 2002/58/CE nu ar trebui să afecteze aplicarea dispozițiilor Regulamentului (UE) 2016/679 și ale Directivei 2002/58/CE, în special a celor referitoare la independența autorităților menționate în acestea. ENISA, în cooperare cu Grupul de cooperare, ar trebui să elaboreze modele comune de notificare prin intermediul unor orientări pentru a simplifica și a raționaliza informațiile care trebuie raportate în temeiul dreptului Uniunii și a reduce sarcina administrativă impusă entităților notificatoare.

(107) Atunci când există suspiciuni că un incident ar fi legat de activități infracționale grave în temeiul dreptului Uniunii sau al dreptului intern, statele membre ar trebui să încurajeze entitățile esențiale și entitățile importante, pe baza normelor aplicabile în materie de proceduri penale în conformitate cu dreptul Uniunii, să raporteze autorităților de aplicare a legii incidentele despre care există suspiciuni că ar avea un caracter infracțional grav. După caz și fără a aduce atingere normelor de protecție a datelor cu caracter personal aplicabile Europol, este de dorit ca procesul de coordonare dintre autoritățile competente și autoritățile de aplicare a legii din diferite state membre să fie facilitat de Centrul european de combatere a criminalității informatice (EC3) și de ENISA.

([21]) Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului din 29 aprilie 2021 de instituire a programului „Europa digitală” și de abrogare a Deciziei (UE) 2015/2240 (JO L 166, 11.5.2021, p. 1).

(108) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile menționate în Regulamentul (UE) 2016/679 și Directiva 2002/58/CE.

(109) Menținerea unor baze de date exacte și complete conținând datele de înregistrare a numelor de domenii (date WHOIS) și furnizarea unui acces legal la astfel de date sunt aspecte esențiale pentru a asigura securitatea, stabilitatea și reziliența DNS, sistem care, la rândul său, contribuie la un nivel comun ridicat de securitate cibernetică în întreaga Uniune. În acest scop specific, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să aibă obligația de a prelucra anumite date necesare pentru atingerea acestui scop. O astfel de prelucrare ar trebui să constituie o obligație legală în sensul articolului 6 alineatul (1) litera (c) din Regulamentul (UE) 2016/679. Respectiva obligație nu aduce atingere posibilității de a colecta date privind înregistrarea numelor de domenii în alte scopuri, de exemplu pe baza unor dispoziții contractuale sau a unor cerințe juridice stabilite în alte acte legislative ale Uniunii sau naționale. Obligația respectivă vizează realizarea unui set complet și exact de date de înregistrare și nu ar trebui să conducă la colectarea acelorași date de mai multe ori. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să coopereze pentru a evita duplicarea acestei sarcini.

(110) Disponibilitatea și accesibilitatea în timp util a datelor de înregistrare a numelor de domenii pentru solicitanții legitimi de acces sunt esențiale pentru prevenirea și combaterea utilizării abuzive a DNS, precum și pentru prevenirea și detectarea incidentelor și răspunsul la acestea. Prin solicitanți legitimi de acces se înțelege orice persoană fizică sau juridică care formulează o cerere în temeiul dreptului Uniunii sau al dreptului intern. Printre acestea se pot număra autoritățile competente în temeiul prezentei directive și cele care sunt competente în temeiul dreptului Uniunii sau al dreptului intern pentru prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor, precum și CERT sau echipele CSIRT. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să aibă obligația de a permite accesul legal al solicitanților legitimi de acces la date specifice de înregistrare a numelor de domenii, care sunt necesare în scopul cererii de acces, în conformitate cu dreptul Uniunii și cu dreptul intern. Cererea solicitanților legitimi de acces ar trebui să fie însoțită de o expunere de motive care să permită evaluarea necesității accesului la date.

(111) Pentru a asigura disponibilitatea unor date exacte și complete de înregistrare a numelor de domeniu, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să colecteze și să garanteze integritatea și disponibilitatea datelor de înregistrare a numelor de domenii. În special, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru colectarea și păstrarea unor date de înregistrare a numelor de domenii exacte și complete, precum și pentru prevenirea și corectarea datelor de înregistrare inexacte, în conformitate cu dreptul Uniunii privind protecția datelor. Respectivele politici și proceduri ar trebui să țină seama, în măsura posibilului, de standardele elaborate de structurile de guvernanță multipartite la nivel internațional. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să adopte și să pună în aplicare proceduri proporționale pentru a verifica datele de înregistrare a numelor de domenii. Aceste proceduri ar trebui să reflecte cele mai bune practici utilizate în domeniu și, în măsura posibilului, progresele înregistrate în domeniul identificării electronice. Printre exemplele de proceduri de verificare se pot număra controalele *ex ante* efectuate în momentul înregistrării și controalele *ex post* efectuate după înregistrare. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui, în special, să verifice cel puțin un mijloc de contact al solicitantului înregistrării.

(112) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să aibă obligația de a pune la dispoziția publicului datele de înregistrare a numelor de domenii care nu intră în domeniul de aplicare al dreptului Uniunii privind protecția datelor, cum ar fi datele care se referă la persoanele juridice, în conformitate cu preambulul Regulamentului (UE) 2016/679. Pentru persoanele juridice, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să pună la dispoziția publicului cel puțin numele solicitantului înregistrării și numărul de telefon de contact. Adresa de e-mail de contact ar trebui, de asemenea, publicată, cu condiția să nu conțină date cu caracter personal cum ar fi în cazul pseudonimelor de e-mail sau al conturilor funcționale. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui, de asemenea, să le permită solicitanților legitimi de acces, în conformitate cu legislația Uniunii privind protecția datelor, accesul legal la date specifice de înregistrare a numelor de domenii privind persoanele fizice. Statele membre ar trebui să solicite registrelor de nume TLD și entităților care furnizează servicii de înregistrare a numelor de domenii să răspundă fără întârzieri nejustificate solicitărilor de divulgare a datelor de înregistrare a numelor de domenii formulate de solicitanții legitimi de acces. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru

publicarea și divulgarea datelor de înregistrare, inclusiv acorduri privind nivelul serviciilor pentru a trata cererile de acces din partea solicitanților legitimi de acces. Respectivele politici și proceduri ar trebui să țină seama, în măsura posibilului, de orice orientări și standarde elaborate de structurile de guvernanță multipartite la nivel internațional. Procedura de acces ar putea include, de asemenea, utilizarea unei interfețe, a unui portal sau a unui alt instrument tehnic, scopul fiind furnizarea unui sistem eficient de solicitare și accesare a datelor de înregistrare. În vederea promovării unor practici armonizate pe piața internă, Comisia poate, fără a aduce atingere competențelor Comitetului european pentru protecția datelor, să ofere orientări cu privire la astfel de proceduri, care să țină seama, în măsura posibilului, de standardele elaborate de structurile de guvernanță multipartite la nivel internațional. Statele membre ar trebui să se asigure că toate tipurile de acces la datele de înregistrare a numelor de domenii cu caracter personal și fără caracter personal sunt gratuite.

(113) Entitățile care intră în domeniul de aplicare al prezentei directive ar trebui considerate ca fiind sub jurisdicția statului membru în care sunt stabilite. Totuși, ar trebui să se considere că furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului intră sub jurisdicția statului membru în care își prestează serviciile. Ar trebui să se considere că furnizorii de servicii DNS, registrele de nume TLD, entitățile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii de *cloud computing*, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea se află sub jurisdicția statului membru în care își au sediul principal în Uniune. Entitățile administrației publice ar trebui să intre sub jurisdicția statului membru care le-a instituit. În cazul în care entitatea furnizează servicii sau își are sediul în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre respectivele state membre. Autoritățile competente din respectivele state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere. În cazul în care statele membre își exercită jurisdicția, acestea nu ar trebui să aplice măsuri de asigurare a respectării legii sau sancțiuni de mai multe ori pentru același comportament, în conformitate cu principiul ne bis in idem.

(114) Pentru a ține seama de caracterul transfrontalier al serviciilor și operațiunilor furnizorilor de servicii DNS, ale registrelor de nume TLD, ale entităților care furnizează servicii de înregistrare a numelor de domenii, ale furnizorilor de servicii de *cloud computing*, ale furnizorilor de servicii de centre de date, ale furnizorilor de rețele de furnizare de conținut, ale furnizorilor de servicii gestionate, ale furnizorilor de servicii de securitate gestionate, precum și ale furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, doar un stat membru ar trebui să aibă jurisdicție asupra entităților respective. Jurisdicția ar trebui să fie atribuită statului membru în care entitatea respectivă își are sediul principal în Uniune. Criteriul stabilirii în sensul prezentei directive implică exercitarea efectivă a activității prin intermediul unor forme de instalare stabilă. Forma juridică a unor astfel de instalări stabile, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință. Respectarea acestui criteriu nu ar trebui să depindă de localizarea fizică a rețelei și a sistemelor informatice într-un anumit loc; prezența și utilizarea unor astfel de sisteme nu constituie, în sine, un astfel de sediu principal și, prin urmare, acestea nu sunt criterii decisive pentru stabilirea sediului principal. Sediul principal ar trebui considerat a fi în statul membru în care sunt luate în mod predominant deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în Uniune. Acesta va corespunde, de regulă, locului în care se află administrația centrală a entităților din Uniune. Dacă un astfel de stat membru nu poate fi stabilit sau dacă astfel de decizii nu sunt luate în Uniune, sediul principal ar trebui considerat a fi în statul membru în care se desfășoară operațiunile de securitate cibernetică. Dacă un astfel de stat membru nu poate fi determinat, ar trebui să se considere că sediul principal se află în statul membru în care entitatea are sediul cu cel mai mare număr de angajați din Uniune. Dacă serviciile sunt prestate de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi.

(115) Dacă un serviciu DNS recurent accesibil publicului este furnizat de un furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului numai ca parte a serviciului de acces la internet, entitatea ar trebui să fie considerată a se afla sub jurisdicția tuturor statelor membre în care sunt furnizate serviciile sale.

(116) În cazul în care un furnizor de servicii DNS, un registru de nume TLD, o entitate care furnizează servicii de înregistrare a numelor de domenii, un furnizor de servicii de *cloud computing*, un furnizor de servicii de centru de date, un furnizor de rețele de furnizare de conținut, un furnizor de servicii gestionate, un furnizor de servicii de securitate gestionate sau un furnizor al unei piețe online, al unui motor de căutare online sau al unei platforme de servicii de socializare în rețea, care nu este stabilit în Uniune, oferă servicii în Uniune, acesta ar trebui să desemneze un reprezentant în Uniune. Pentru a determina dacă o astfel de entitate oferă servicii în cadrul Uniunii, ar trebui să se determine dacă entitatea intenționează să ofere servicii persoanelor din unul sau mai multe state membre. Simpla accesibilitate în Uniune a unui site al entității sau al unui intermediar ori disponibilitatea unei adrese de e-mail sau a altor date de contact sau utilizarea unei limbi folosite în general în țara terță în care este stabilită entitatea ar trebui să fie considerate insuficiente pentru a se confirma o astfel de intenție. Cu toate acestea, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda servicii în respectiva limbă ori menționarea unor clienți sau utilizatori din Uniune ar putea conduce la concluzia că entitatea intenționează să ofere servicii în Uniune. Reprezentantul ar trebui să acționeze în numele entității, iar autoritățile competente sau echipele CSIRT ar trebui să se poată adresa reprezentantului. Reprezentantul ar trebui să fie desemnat explicit printr-un mandat scris al entității pentru a acționa în numele acesteia în privința obligațiilor acesteia prevăzute în prezenta directivă, inclusiv în privința raportării incidentelor.

(117) Pentru a asigura o imagine de ansamblu clară asupra furnizorilor de servicii DNS, a registrelor de nume TLD, a entităților care furnizează servicii de înregistrare a numelor de domenii, a furnizorilor de servicii de *cloud computing*, a furnizorilor de servicii de centre de date, a furnizorilor de rețele de furnizare de conținut, a furnizorilor de servicii gestionate, a furnizorilor de servicii de securitate gestionate, precum și a furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, care furnizează servicii care intră în domeniul de aplicare al prezentei directive în întreaga Uniune, ENISA ar trebui să creeze și să mențină un registru al acestor entități, pe baza informațiilor primite de statele membre, dacă este cazul prin intermediul mecanismelor naționale instituite pentru ca entitățile să se poată înregistra. Punctele unice de contact ar trebui să înainteze către ENISA informațiile și orice modificare a acestora. Pentru a asigura acuratețea și exhaustivitatea informațiilor care urmează să fie incluse în acest registru, statele membre pot să transmită către ENISA informațiile disponibile în orice registru național cu privire la aceste entități. ENISA și statele membre ar trebui să ia măsuri pentru a facilita interoperabilitatea acestor registre, asigurând, în același timp, protecția informațiilor confidențiale sau clasificate. ENISA ar trebui să instituie protocoale adecvate de clasificare și gestionare a informațiilor pentru a asigura securitatea și confidențialitatea informațiilor divulgate și ar trebui să restricționeze accesul la informațiile respective, stocarea și transmiterea acestora către utilizatorii vizați.

(118) În cazul în care se face schimb de informații care sunt clasificate în conformitate cu dreptul Uniunii sau cu dreptul național ori astfel de informații sunt raportate sau partajate în alt mod în temeiul prezentei directive, ar trebui să se aplice normele corespunzătoare privind tratarea informațiilor clasificate. În plus, ENISA ar trebui să dispună de infrastructura, procedurile și normele în vigoare pentru a trata informațiile sensibile și clasificate în conformitate cu normele de securitate aplicabile pentru protecția informațiilor clasificate ale UE.

(119) Amenințările cibernetice devenind tot mai complexe și mai sofisticate, eficacitatea măsurilor de detectare a unor astfel de amenințări și prevenirea lor depinde în mare măsură de schimbul regulat de informații privind amenințările și vulnerabilitățile care are loc între entități. Schimbul de informații contribuie la creșterea gradului de sensibilizare cu privire la amenințările cibernetice, ceea ce, la rândul său, consolidează capacitatea entităților de a preveni materializarea unor astfel de amenințări în incidente și le permite entităților să controleze mai bine efectele incidentelor și să se redreseze mai eficient. În absența unor orientări la nivelul Uniunii, diverși factori par să fi împiedicat un astfel de schimb de informații, în special incertitudinea cu privire la compatibilitatea cu normele în materie de concurență și răspundere.

(120) Entitățile ar trebui încurajate și asistate de statele membre să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, pentru a-și consolida capacitățile de a preveni, a detecta, a furniza un răspuns în mod adecvat la incidente și de a se redresa în urma acestora sau de a diminua impactul lor. Prin urmare, este necesar să se permită apariția, la nivelul Uniunii, a unor acorduri privind schimbul voluntar de informații în materie de securitate cibernetică. În acest scop, statele membre ar trebui să sprijine și să încurajeze în mod activ entitățile, precum cele care furnizează servicii de securitate cibernetică și de cercetare, precum și cele relevante care nu intră în domeniul de aplicare al prezentei directive, să participe la astfel de acorduri privind schimbul de informații în materie de securitate cibernetică. Aceste mecanisme ar trebui să fie stabilite în conformitate cu normele Uniunii în materie de concurență și cu dreptul Uniunii în materie de protecție a datelor.

(121) Prelucrarea datelor cu caracter personal, în măsura necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor de către entități esențiale și entitățile importante, ar putea fi considerată legală pe baza faptului că o astfel de prelucrare respectă o obligație legală care îi revine operatorului, în conformitate cu cerințele de la articolul 6 alineatul (1) litera (c) și de la articolul 6 alineatul (3) din Regulamentul (UE) 2016/679. Prelucrarea datelor cu caracter personal ar putea fi, de asemenea, necesară pentru interesele legitime urmărite de entitățile esențiale și entitățile importante, precum și de furnizorii de tehnologii și servicii de securitate care acționează în numele acestor entități, în temeiul articolului 6 alineatul (1) litera (f) din Regulamentul (UE) 2016/679, inclusiv în cazul în care o astfel de prelucrare este necesară pentru acordurile privind schimbul de informații în materie de securitate cibernetică sau pentru notificarea voluntară a informațiilor relevante în conformitate cu prezenta directivă. Măsuri legate de prevenirea, detectarea, identificarea, limitarea, analizarea și combaterea incidentelor, măsuri de sensibilizare cu privire la amenințările cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilității și al divulgării coordonate a vulnerabilității, schimbul voluntar de informații cu privire la incidentele respective, precum și la amenințările și vulnerabilitățile cibernetice, indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare ar putea necesita prelucrarea anumitor categorii de date cu caracter personal, cum ar fi adrese IP, localizatoare uniforme de resurse (URL), nume de domenii, adrese de e-mail și, în cazul în care acestea dezvăluie date cu caracter personal, marcaje temporale. Prelucrarea datelor cu caracter personal de către autoritățile competente, punctele unice de contact și echipele CSIRT ar putea constitui o obligație legală sau ar putea fi considerată necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul de date în temeiul articolului 6 alineatul (1) litera (c) sau (e) și al articolului 6 alineatul (3) din Regulamentul (UE) 2016/679 sau pentru urmărirea unui interes legitim al entităților esențiale și al entităților importante, astfel cum se menționează la articolul 6 alineatul (1) litera (f) din respectivul regulament. În plus, dreptul național ar putea stabili norme care să permită autorităților competente, punctelor unice de contact și echipelor CSIRT, în măsura în care acest lucru este necesar și proporțional pentru a asigura securitatea rețelelor și a sistemelor informatice ale entităților esențiale și ale entităților importante, să prelucreze categorii speciale de date cu caracter personal în conformitate cu articolul 9 din Regulamentul (UE) 2016/679, în special prin prevederea unor măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanelor fizice, inclusiv limitări tehnice privind reutilizarea acestor date și utilizarea unor măsuri de ultimă generație de securitate și de protejare a confidențialității, cum ar fi pseudonimizarea sau criptarea, în cazul în care anonimizarea poate afecta în mod semnificativ scopul urmărit.

(122) Pentru a consolida competențele și măsurile de supraveghere care contribuie la asigurarea respectării efective, prezenta directivă ar trebui să prevadă o listă minimă de acțiuni și măsuri de supraveghere prin care autoritățile competente pot supraveghea entitățile esențiale și entitățile importante. În plus, prezenta directivă ar trebui să stabilească o diferențiere între regimul de supraveghere al entităților esențiale și cel al entităților importante, în vederea asigurării unui echilibru echitabil al obligațiilor pentru entitățile respective și pentru autoritățile competente. Prin urmare, entitățile esențiale ar trebui să fie supuse unui regim de supraveghere ex ante și ex post cuprinzător, în timp ce entitățile importante ar trebui să fie supuse unui regim de supraveghere simplificat, doar ex post. Entitățile importante nu ar trebui, așadar, să aibă obligația să documenteze în mod sistematic respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică, în timp ce autoritățile competente ar trebui să pună în aplicare o abordare reactivă ex post a supravegherii și, prin urmare, să nu aibă o obligație generală de a supraveghea entitățile respective. Supravegherea *ex post* a entităților importante poate fi declanșată de dovezi, indicii sau informații aduse la cunoștința autorităților competente, cu privire la care aceste autorități consideră că sugerează potențiale încălcări ale prezentei directive. De exemplu, astfel de dovezi, indicii sau informații ar putea fi de tipul celor furnizate autorităților competente de către alte autorități, de entități, cetățeni, mass-media sau alte surse, sau informații aflate la dispoziția publicului, sau ar putea rezulta din alte activități desfășurate de autoritățile competente în îndeplinirea sarcinilor lor.

(123) Executarea sarcinilor de supraveghere de către autoritățile competente nu ar trebui să împiedice în mod inutil activitățile comerciale ale entității în cauză. În cazul în care autoritățile competente își îndeplinesc sarcinile de supraveghere în legătură cu entitățile esențiale, inclusiv efectuarea de inspecții la fața locului și supravegherea *ex situ*, investigarea încălcărilor prezentei directive și efectuarea de audituri de securitate sau scanări de securitate, ar trebui să reducă la minimum impactul asupra activităților economice ale entității în cauză.

(124) În exercitarea supravegherii *ex ante*, autoritățile competente ar trebui să fie în măsură să decidă cu privire la ierarhizarea utilizării măsurilor și mijloacelor de supraveghere de care dispun, în mod proporțional. Acest lucru implică faptul că autoritățile competente pot decide cu privire la o astfel de ierarhizare a priorităților pe baza metodologiilor de supraveghere care ar trebui să urmeze o abordare bazată pe riscuri. Mai precis, astfel de metodologii ar putea include criterii sau valori de referință pentru clasificarea entităților esențiale în categorii de risc, alături de măsuri de supraveghere corespunzătoare și mijloace recomandate pentru fiecare categorie de risc, cum ar fi utilizarea, frecvența sau tipul inspecțiilor la fața locului, al auditurilor de securitate specifice sau al

scanărilor de securitate, tipul de informații care trebuie solicitate și nivelul de detaliere al informațiilor respective. Astfel de metodologii de supraveghere ar putea fi, de asemenea, însoțite de programe de lucru și pot fi evaluate și revizuite periodic, inclusiv cu privire la aspecte precum alocarea resurselor și nevoile. În ceea ce privește entitățile administrației publice, competențele de supraveghere ar trebui exercitate în conformitate cu cadrele legislative și instituționale naționale.

(125) Autoritățile competente ar trebui să se asigure că sarcinile lor de supraveghere în legătură cu entitățile esențiale și entitățile importante sunt îndeplinite de profesioniști cu formare în domeniu, care să dețină competențele necesare pentru a îndeplini sarcinile respective, în special în ceea ce privește efectuarea de inspecții la fața locului și supravegherea *ex situ*, inclusiv identificarea deficiențelor din bazele de date, de hardware, firewall-uri, de criptare și de rețele. Inspecțiile respective și supravegherea respectivă ar trebui să se desfășoare într-un mod obiectiv.

(126) În cazuri justificate în mod corespunzător în care are cunoștință de o amenințare cibernetică semnificativă sau de un risc iminent, autoritatea competentă ar trebui să fie în măsură să ia decizii imediate de executare cu scopul de a preveni un incident sau de a răspunde la acesta.

(127) Pentru ca asigurarea respectării legii să fie eficace, ar trebui stabilită o listă minimă de competențe de asigurare a respectării legii care pot fi exercitate pentru încălcarea măsurilor de gestionare a riscurilor de securitate cibernetică și a obligațiilor de raportare prevăzute în prezenta directivă, stabilind un cadru clar și coerent pentru asigurarea respectării legii în întreaga Uniune. Ar trebui să se țină seama în mod corespunzător de natura, gravitatea și durata încălcării prezentei directive, de prejudiciile materiale sau morale cauzate, de caracterul intenționat al încălcării sau de comiterea din neglijență a încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul material sau moral, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. Măsurile de asigurare a respectării legii, inclusiv amenzile administrative, ar trebui să fie proporționale, iar aplicarea lor ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), inclusiv dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.

(128) Prezenta directivă nu impune statelor membre să prevadă răspunderea penală sau civilă a persoanelor fizice care au responsabilitatea de a se asigura că o entitate respectă prezenta directivă pentru prejudiciile suferite de terți ca urmare a încălcării prezentei directive.

(129) Pentru a asigura respectarea efectivă a obligațiilor prevăzute în prezenta directivă, fiecare autoritate competentă ar trebui să aibă competența de a aplica sau de a solicita aplicarea de amenzi administrative.

(130) În cazul în care o amendă administrativă este aplicată unei entități esențiale sau unei entități importante care este o întreprindere, întreprinderea ar trebui înțeleasă ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE în aceste scopuri. În cazul în care o amendă administrativă se aplică unei persoane care nu este o întreprindere, autoritatea competentă ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Competența de a stabili dacă și în ce măsură autorităților publice ar trebui să li se poată aplica amenzi administrative ar trebui să revină statelor membre. Aplicarea unei amenzi administrative nu aduce atingere exercitării altor competențe de către autoritățile competente sau aplicarea altor sancțiuni prevăzute în normele naționale de transpunere a prezentei directive.

(131) Statele membre ar trebui să poată stabili norme privind sancțiunile penale pentru încălcarea normelor naționale de transpunere a prezentei directive. Cu toate acestea, aplicarea de sancțiuni penale pentru încălcări ale unor asemenea norme de drept intern și de sancțiuni administrative conexe nu ar trebui să ducă la încălcarea principiului *ne bis in idem*, astfel cum a fost interpretat de Curtea de Justiție a Uniunii Europene.

(132) În cazul în care prezenta directivă nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unei încălcări grave a prezentei directive, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni efective, proporționale și cu efect de descurajare. Natura unor astfel de sancțiuni și caracterul lor penal sau administrativ ar trebui stabilite de dreptul intern.

(133) Pentru a consolida și mai mult eficacitatea și efectul de descurajare al măsurilor de asigurare a respectării legii aplicabile în cazul încălcării prezentei directive, autoritățile competente ar trebui să fie împuternicite să suspende temporar sau să solicite suspendarea temporară a unei certificări sau a unei autorizații privind o parte din serviciile relevante furnizate de o entitate esențială sau privind ansamblul acestor servicii și să ceară impunerea unei interdicții temporare de a exercita funcții de conducere de către orice persoană fizică la nivel de director executiv sau de reprezentant legal. Având în vedere gravitatea și impactul lor asupra activităților entităților și, în cele din urmă, asupra utilizatorilor, aceste suspendări sau interdicții temporare ar trebui aplicate numai proporțional cu gravitatea încălcării și ținând seama de circumstanțele fiecărui caz individual, inclusiv de caracterul intenționat al încălcării sau de comiterea din neglijență a încălcării și de orice măsuri luate pentru a preveni sau a atenua prejudiciul material sau moral. Astfel de suspendări sau interdicții temporare ar trebui aplicate doar în ultimă instanță, adică numai după ce celelalte măsuri relevante de asigurare a respectării legii prevăzute de prezenta directivă au fost epuizate și numai până în momentul în care entitățile cărora li se aplică iau măsurile necesare pentru a remedia deficiențele sau pentru a se conforma cerințelor autorității competente pentru care au fost aplicate aceste suspendări sau interdicții temporare. Impunerea unor astfel de suspendări sau interdicții temporare ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.

(134) Pentru a asigura respectarea de către entități a obligațiilor lor prevăzute în prezenta directivă, statele membre ar trebui să coopereze și să își acorde asistență reciprocă în ceea ce privește măsurile de supraveghere și de asigurare a respectării legii, în special dacă o entitate furnizează servicii în mai multe state membre sau dacă rețelele și sistemele sale informatice sunt situate într-un alt stat membru decât cel în care furnizează servicii. Atunci când acordă asistență, autoritatea competentă căreia i se adresează solicitarea ar trebui să ia măsuri de supraveghere sau de asigurare a respectării legii în conformitate cu dreptul intern. Pentru a asigura buna funcționare a asistenței reciproce în temeiul prezentei directive, autoritățile competente ar trebui să utilizeze Grupul de cooperare ca forum pentru discutarea cazurilor și a cererilor specifice de asistență.

(135) Pentru a asigura eficacitatea supravegherii și a asigurării respectării legii, îndeosebi într-o situație cu o dimensiune transfrontalieră, un stat membru care a primit o cerere de asistență reciprocă ar trebui ca, în limitele cererii respective, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în legătură cu entitatea care face obiectul cererii respective și care furnizează servicii sau deține o rețea și un sistem informatic pe teritoriul statului membru respectiv.

(136) Prezenta directivă ar trebui să stabilească norme de cooperare între autoritățile competente și autoritățile de supraveghere în conformitate cu Regulamentul (UE) 2016/679 pentru tratarea cazurilor de încălcare a prezentei directive în materie de date cu caracter personal.

(137) Prezenta directivă ar trebui să vizeze asigurarea unui nivel ridicat de responsabilitate pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare la nivelul entităților esențiale și al entităților importante. Din aceste motive, organele de conducere ale entităților esențiale și ale entităților importante ar trebui să aprobe măsurile privind riscurile în materie de securitate cibernetică și să supravegheze punerea lor în aplicare.

(138) Pentru a asigura un nivel comun ridicat de securitate cibernetică în întreaga Uniune pe baza prezentei directive, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei în ceea ce privește completarea prezentei directive prin specificarea categoriilor de entități esențiale și entități importante care au obligația de a utiliza anumite produse TIC, servicii TIC și procese TIC certificate sau de a obține un certificat în cadrul unui sistem european de certificare a securității cibernetice. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([22]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

([22]) JO L 123, 12.5.2016, p. 1.

(139) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentei directive, Comisiei ar trebui să i se confere competențe de executare pentru a stabili dispozițiile procedurale necesare pentru funcționarea Grupului de cooperare și cerințele tehnice și metodologice, precum și cerințele sectoriale referitoare la măsurile de gestionare a riscurilor în materie de securitate cibernetică, precum și pentru a specifica mai în detaliu tipul de informații, formatul și procedura de notificare a incidentelor, a amenințărilor cibernetice și a incidentelor evitate la limită și a comunicărilor de amenințări cibernetice semnificative, precum și cazurile în care un incident trebuie considerat semnificativ. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([23]).

(140) Comisia ar trebui să revizuiască periodic prezenta directivă, consultându-se cu părțile interesate, în special pentru a stabili dacă este adecvat să propună modificări ca urmare a evoluției condițiilor societale, politice, tehnologice sau de piață. În cadrul acestor revizuiri, Comisia ar trebui să evalueze relevanța dimensiunii entităților vizate și a sectoarelor, a subsectoarelor și a tipurilor de entități menționate în anexele la prezenta directivă pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. Comisia ar trebui să evalueze, printre altele, dacă furnizorii care intră în domeniul de aplicare al prezentei directive și care sunt desemnați drept platforme online foarte mari în sensul articolului 33 din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului ([24]) ar putea fi identificați ca entități esențiale în temeiul prezentei directive.

(141) Prezenta directivă creează noi sarcini pentru ENISA, consolidând astfel rolul acesteia, și ar putea avea totodată drept rezultat o obligație a ENISA de a-și îndeplini sarcinile existente în temeiul Regulamentului (UE) 2019/881 la un nivel mai ridicat decât înainte. Pentru a se asigura că ENISA dispune de resursele financiare și umane necesare pentru a îndeplini sarcinile existente și cele noi, precum și pentru a îndeplini orice nivel mai ridicat de execuție a sarcinilor care rezultă din rolul său consolidat, bugetul său ar trebui majorat în consecință. În plus, pentru a asigura utilizarea eficientă a resurselor, ENISA ar trebui să beneficieze de o mai mare flexibilitate în ceea ce privește modul în care poate să aloce resurse la nivel intern pentru a-și îndeplini în mod eficace sarcinile și pentru a răspunde așteptărilor.

(142) Întrucât obiectivul prezentei directive, și anume obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, nu poate fi realizat în mod satisfăcător de către statele membre, dar, având în vedere efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivului respectiv.

(143) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de cartă, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare. Dreptul la o cale de atac eficientă se extinde la beneficiarii serviciilor furnizate de entități esențiale și de entități importante. Prezenta directivă ar trebui să fie pusă în aplicare în conformitate cu drepturile și principiile menționate.

(144) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([25]) și a emis un aviz la 11 martie 2021 ([26]),

---

([23]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([24]) Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale) (JO L 277, 27.10.2022 , p. 1).

([25]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

([26]) JO C 183, 11.5.2021, p. 3.

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiectul

(1) Prezenta directivă stabilește măsuri care vizează obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, cu scopul de a îmbunătăți funcționarea pieței interne.

(2) În acest scop, prezenta directivă stabilește:

(a) obligațiile statelor membre de a adopta strategii naționale de securitate cibernetică și de a desemna sau de a înființa autorități competente, autorități de gestionare a crizelor cibernetice, puncte unice de contact în materie de securitate cibernetică (denumite în continuare „puncte unice de contact") și echipe de intervenție în caz de incidente de securitate informatică (denumite în continuare „echipe CSIRT");

(b) măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru entitățile de tipul celor menționate în anexa I sau II, precum și pentru entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557;

(c) normele și obligațiile privind schimbul de informații în materie de securitate cibernetică;

(d) obligațiile în materie de supraveghere și de asigurare a respectării legii pentru statele membre.

Articolul 2

Domeniul de aplicare

(1) Prezenta directivă se aplică entităților publice sau private de tipul celor menționate în anexa I sau II, care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) din respectivul articol și care prestează servicii sau își desfășoară activitățile în cadrul Uniunii.

Articolul 3 alineatul (4) din anexa la recomandarea respectivă nu se aplică în sensul prezentei directive.

(2) Indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților de tipul celor menționate în anexa I sau II, în cazul în care:

(a) serviciile sunt furnizate de:

  (i) furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului;

  (ii) prestatorii de servicii de încredere;

  (iii) registrele de nume de domenii de prim nivel și de furnizorii de servicii de sistem de nume de domenii;

(b) entitatea este singurul furnizor dintr-un stat membru al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice;

(c) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranței publice, a securității publice sau a sănătății publice;

(d) perturbarea serviciului furnizat de entitate ar putea genera un risc sistemic semnificativ, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;

(e) entitatea este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente din statul membru;

(f) entitatea este o entitate a administrației publice:

(i) la nivel central, astfel cum este definită de un stat membru în conformitate cu dreptul intern;

(ii) la nivel regional, astfel cum este definită de un stat membru în conformitate cu dreptul intern, care, în urma unei evaluări bazate pe riscuri, furnizează servicii a căror întrerupere ar putea avea un impact semnificativ asupra activităților societale sau economice critice.

(3) Prezenta directivă se aplică entităților identificate ca fiind entități critice în temeiul Directivei (UE) 2022/2557, indiferent de dimensiunea lor.

(4) Prezenta directivă se aplică entităților care furnizează servicii de înregistrare a numelor de domenii, indiferent de dimensiunea lor.

(5) Statele membre pot prevedea ca prezenta directivă să se aplice:

(a) entităților administrației publice de la nivel local;

(b) instituțiilor de învățământ, în special în cazul în care acestea desfășoară activități critice de cercetare.

(6) Prezenta directivă nu aduce atingere responsabilității statelor membre de a proteja securitatea națională și competenței acestora de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale a statului și menținerea ordinii publice.

(7) Prezenta directivă nu se aplică entităților administrației publice care își desfășoară activitățile în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv prevenirii, investigării, depistării și urmăririi penale a infracțiunilor.

(8) Statele membre pot exonera anumite entități care desfășoară activități în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, sau care furnizează servicii exclusiv entităților administrației publice menționate la alineatul (7) de la prezentul articol, de obligațiile prevăzute la articolul 21 sau la articolul 23 în ceea ce privește activitățile sau serviciile respective. În astfel de cazuri, măsurile de supraveghere și de asigurare a respectării legii menționate în capitolul VII nu se aplică în legătură cu aceste activități sau servicii specifice. În cazul în care entitățile desfășoară activități sau prestează servicii exclusiv de tipul celor menționate în prezentul alineat, statele membre pot decide, de asemenea, să exonereze respectivele entități de obligațiile prevăzute la articolele 3 și 27.

(9) Alineatele (7) și (8) nu se aplică în cazul în care o entitate acționează ca prestator de servicii de încredere.

(10) Prezenta directivă nu se aplică entităților pe care statele membre le-au exclus din domeniul de aplicare al Regulamentului (UE) 2022/2554 în conformitate cu articolul 2 alineatul (4) din regulamentul respectiv.

(11) Obligațiile prevăzute în prezenta directivă nu implică furnizarea de informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

(12) Prezenta directivă se aplică fără a aduce atingere Regulamentului (UE) 2016/679, Directivei 2002/58/CE, Directivelor 2011/93/UE ([27]) și 2013/40/UE ([28]) ale Parlamentului European și ale Consiliului și Directivei (UE) 2022/2557.

(13) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii sau cu cele naționale, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante în conformitate cu prezenta directivă, numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații relevante pentru scopul urmărit și proporționale cu acesta. Schimbul de informații păstrează confidențialitatea respectivelor informații și protejează securitatea și interesele comerciale ale entităților în cauză.

([27]) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

([28]) Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

(14) Entitățile, autoritățile competente, punctele unice de contact și echipele CSIRT prelucrează datele cu caracter personal în măsura necesară pentru scopurile prezentei directive și în conformitate cu Regulamentul (UE) 2016/679; în special această prelucrare se bazează pe articolul 6 din respectivul regulament.

Prelucrarea datelor cu caracter personal în temeiul prezentei directive de către furnizorii de rețele publice de comunicații electronice sau de către furnizorii de servicii de comunicații electronice accesibile publicului se efectuează în conformitate cu dreptul Uniunii privind protecția datelor și cu dreptul Uniunii privind protejarea confidențialității, în special cu Directiva 2002/58/CE.

Articolul 3

Entități esențiale și entități importante

(1) În sensul prezentei directive, următoarele entități sunt considerate a fi entități esențiale:

(a) entitățile de tipul celor menționate în anexa I care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la articolul 2 alineatul (1) din anexa la Recomandarea 2003/361/CE;

(b) prestatorii de servicii de încredere calificați și registrele de nume de domenii de prim nivel, precum și prestatorii de servicii DNS, indiferent de dimensiunea lor;

(c) furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE;

(d) entitățile administrației publice menționate la articolul 2 alineatul (2) litera (f) punctul (i);

(e) orice alte entități de tipul celor menționate în anexa I sau II care sunt identificate de un stat membru drept entități esențiale în temeiul articolului 2 alineatul (2) literele (b)-(e);

(f) entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557, menționate la articolul 2 alineatul (3) din prezenta directivă;

(g) în cazul în care statul membru prevede acest lucru, entitățile pe care statul membru respectiv le-a identificat înainte de 16 ianuarie 2023 ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 sau cu dreptul intern.

(2) În sensul prezentei directive, entitățile de tipul celor menționate în anexa I sau II care nu se califică drept entități esențiale în temeiul alineatului (1) de la prezentul articol sunt considerate a fi entități importante. Sunt incluse aici entitățile identificate de statele membre ca fiind entități importante în temeiul articolului 2 alineatul (2) literele (b)-(e).

(3) Până la 17 aprilie 2025, statele membre întocmesc o listă a entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii. Statele membre revizuiesc lista în mod regulat, cel puțin o dată la doi ani, și o actualizează atunci când este cazul.

(4) În scopul întocmirii listei menționate la alineatul (3), statele membre solicită entităților menționate la respectivul alineat să prezinte autorităților competente cel puțin următoarele informații:

(a) denumirea entității;

(b) adresa și datele de contact actualizate, inclusiv adresele de e-mail, gama de IP-uri și numerele de telefon;

(c) dacă este cazul, sectorul și subsectorul relevante menționate în anexa I sau II; precum și

(d) după caz, o listă a statelor membre în care furnizează servicii care intră în domeniul de aplicare al prezentei directive.

Entitățile menționate la alineatul (3) notifică fără întârziere orice modificări ale detaliilor transmise în temeiul primului paragraf de la prezentul alineat și, în orice caz, în termen de două săptămâni de la data modificării.

Comisia, cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), oferă, fără întârzieri nejustificate, orientări și modele privind obligațiile prevăzute în prezentul alineat.

Statele membre pot institui mecanisme naționale prin care entitățile să se înregistreze.

(5) Până la 17 aprilie 2025 și, ulterior, o dată la doi ani, autoritățile competente notifică:

(a) Comisiei și Grupului de cooperare numărul entităților esențiale și al entităților importante enumerate în temeiul alineatului (3) pentru fiecare sector și subsector menționat în anexa I sau II; și

(b) Comisiei informațiile relevante privind numărul de entități esențiale și de entități importante identificate în temeiul articolului 2 alineatul (2) literele (b)-(e), sectorul și subsectorul menționate în anexa I sau II din care fac parte, tipul de servicii pe care le furnizează și dispoziția, dintre cele prevăzute la articolul 2 alineatul (2) literele (b)-(e), în temeiul căreia au fost identificate.

(6) Până la 17 aprilie 2025 și la cererea Comisiei, statele membre pot notifica Comisiei denumirile entităților esențiale și ale entităților importante menționate la alineatul (5) litera (b).

Articolul 4

Acte juridice sectoriale ale Uniunii

(1) În cazul în care actele juridice sectoriale ale Uniunii impun entităților esențiale sau entităților importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele semnificative, iar cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute în prezenta directivă, dispozițiile relevante ale prezentei directive, inclusiv dispozițiile privind supravegherea și asigurarea respectării legii prevăzute în capitolul VII, nu se aplică acestor entități. În cazul în care actele juridice sectoriale ale Uniunii nu acoperă toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive se aplică în continuare entităților care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii.

(2) Cerințele menționate la alineatul (1) din prezentul articol sunt considerate echivalente în privința efectului cu obligațiile prevăzute în prezenta directivă, în cazul în care:

(a) măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente în privința efectului cu cele prevăzute la articolul 21 alineatele (1) și (2); sau

(b) actul juridic sectorial al Uniunii prevede accesul imediat, după caz automat și direct, la notificările incidentelor pentru echipele CSIRT, autoritățile competente sau punctele unice de contact în temeiul prezentei directive și dacă cerințele de notificare a incidentelor semnificative au un efect cel puțin echivalent cu cele prevăzute la articolul 23 alineatele (1)-(6) din prezenta directivă.

(3) Comisia, până la 17 iulie 2023, oferă orientări care clarifică aplicarea alineatelor (1) și (2). Comisia revizuiește orientările respective în mod periodic. La elaborarea acestor orientări, Comisia ia în considerare observațiile Grupului de cooperare și ale ENISA.

Articolul 5

Armonizarea minimă

Prezenta directivă nu împiedică statele membre să adopte sau să mențină dispoziții care asigură un nivel mai ridicat de securitate cibernetică, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.

Articolul 6

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

1. „rețea și sistem informatic” înseamnă:

   (a) o rețea de comunicații electronice, astfel cum este definită la articolul 2 punctul 1 din Directiva (UE) 2018/1972;

(b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale; sau

(c) datele digitale stocate, prelucrate, recuperate sau transmise de elemente reglementate în temeiul literelor (a) și (b) în vederea funcționării, utilizării, protejării și întreținerii lor;

2. „securitatea rețelelor și a sistemelor informatice" înseamnă capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărui eveniment care poate compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

3. „securitate cibernetică" înseamnă securitate cibernetică astfel cum este definită la articolul 2 alineatul (1) din Regulamentul (UE) 2019/881;

4. „strategie națională de securitate cibernetică" înseamnă un cadru coerent al unui stat membru care prevede obiective și priorități strategice în domeniul securității cibernetice și guvernanța necesară pentru realizarea acestora în statul membru respectiv;

5. „incident evitat la limită" înseamnă un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;

6. „incident" înseamnă un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;

7. „incident de securitate cibernetică de mare amploare" înseamnă un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre;

8. „gestionarea incidentului" înseamnă toate acțiunile și procedurile care vizează prevenirea, detectarea, analizarea și limitarea unui incident, sau vizează răspunsul la acesta și redresarea în urma incidentului;

9. „risc" înseamnă potențialul de pierderi sau de perturbări cauzate de un incident și trebuie exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului;

10. „amenințare cibernetică" înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

11. „amenințare cibernetică semnificativă" înseamnă o amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețeaua și sistemele informatice ale unei entități sau utilizatorii serviciilor furnizate de entitate, cauzând prejudicii materiale sau morale considerabile;

12. „produs TIC" înseamnă un produs astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881;

13. „serviciu TIC" înseamnă un serviciu TIC astfel cum este definit la articolul 2 punctul 13 din Regulamentul (UE) 2019/881;

14. „proces TIC" înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881;

15. „vulnerabilitate" înseamnă un punct slab, o susceptibilitate sau o deficiență a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o amenințare cibernetică;

16. „standard" înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([29]);

17. „specificație tehnică" înseamnă o specificație tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

([29]) Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

18. „internet *exchange point*" înseamnă o facilitate a rețelei care permite interconectarea a mai mult de două rețele autonome independente (sisteme autonome), în special în scopul facilitării schimbului de trafic de internet, care furnizează interconectare doar pentru sisteme autonome și care nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau interacționează într-un alt mod cu acest trafic;

19. „sistem de nume de domenii DNS" sau „DNS" înseamnă un sistem ierarhic și distribuit de atribuire de nume care face posibilă identificarea serviciilor și a resurselor de pe internet, permițând dispozitivelor utilizatorilor finali să utilizeze serviciile de rutare și conectivitate pe internet pentru a accesa serviciile și resursele respective;

20. „furnizor de servicii DNS" înseamnă o entitate care furnizează:

    (a) servicii de rezoluție a numelor de domenii recursive accesibile publicului pentru utilizatorii finali de internet; sau

    (b) servicii de rezoluție a numelor de domenii cu autoritate pentru utilizarea de către terți, cu excepția serverelor pentru nume primare;

21. „registru de nume de domenii de prim nivel" sau „registru de nume TLD" (*top-level domain* – TLD) înseamnă o entitate căreia i s-a delegat un anumit TLD și care este responsabilă cu administrarea TLD-ului, inclusiv cu înregistrarea numelor de domenii în cadrul TLD-ului și cu exploatarea tehnică a TLD-ului, inclusiv exploatarea serverelor sale de nume, întreținerea bazelor sale de date și distribuirea fișierelor zonale TLD între serverele de nume, indiferent dacă oricare dintre aceste operațiuni este efectuată de entitatea însăși sau este externalizată, dar excluzând situațiile în care numele TLD sunt utilizate de un registru numai pentru uzul propriu;

22. „entitate care furnizează servicii de înregistrare a numelor de domenii" înseamnă un operator de registru sau un agent care acționează în numele operatorilor de registru, cum ar fi un furnizor sau un revânzător de servicii de protecție a confidențialității sau servicii de proxy;

23. „serviciu digital" înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului ([30]);

24. „serviciu de încredere" înseamnă un serviciu de încredere astfel cum este definit la articolul 3 punctul 16 din Regulamentul (UE) nr. 910/2014;

25. „prestator de servicii de încredere" înseamnă un prestator de servicii de încredere astfel cum este definit la articolul 3 punctul 19 din Regulamentul (UE) nr. 910/2014;

26. „serviciu de încredere calificat" înseamnă un serviciu de încredere calificat astfel cum este definit la articolul 3 punctul 17 din Regulamentul (UE) nr. 910/2014;

27. „prestator de servicii de încredere calificat" înseamnă un prestator de servicii de încredere calificat astfel cum este definit la articolul 3 punctul 20 din Regulamentul (UE) nr. 910/2014;

28. „piață online" înseamnă o piață online astfel cum este definită la articolul 2 litera (n) din Directiva 2005/29/CE a Parlamentului European și a Consiliului ([31]);

29. „motor de căutare online" înseamnă un motor de căutare online astfel cum este definit la articolul 2 punctul 5 din Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului ([32]);

30. „serviciu de *cloud computing*" înseamnă un serviciu digital care permite administrarea la cerere și accesul amplu la distanță la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun, inclusiv atunci când aceste resurse sunt distribuite în mai multe locații;

([30]) Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

([31]) Directiva 2005/29/CE a Parlamentului European și a Consiliului din 11 mai 2005 privind practicile comerciale neloiale ale întreprinderilor de pe piața internă față de consumatori și de modificare a Directivei 84/450/CEE a Consiliului, a Directivelor 97/7/CE, 98/27/CE și 2002/65/CE ale Parlamentului European și ale Consiliului și a Regulamentului (CE) nr. 2006/2004 al Parlamentului European și al Consiliului („Directiva privind practicile comerciale neloiale") (JO L 149, 11.6.2005, p. 22).

([32]) Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului din 20 iunie 2019 privind promovarea echității și a transparenței pentru întreprinderile utilizatoare de servicii de intermediere online (JO L 186, 11.7.2019, p. 57).

31. „serviciu de centre de date” înseamnă un serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a tehnologiei informației și a echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului;

32. „rețea de furnizare de conținut” înseamnă o rețea de servere distribuite geografic cu scopul de a asigura o disponibilitate ridicată, accesibilitate sau furnizare rapidă de conținut digital și servicii către utilizatorii de internet în numele furnizorilor de conținut și de servicii;

33. „platformă de servicii de socializare în rețea” înseamnă o platformă care le permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei prin intermediul mai multor dispozitive, în special prin chat, postări, materiale video și recomandări;

34. „reprezentant” înseamnă o persoană fizică sau juridică stabilită în Uniune care este desemnată în mod explicit să acționeze în numele unui furnizor de servicii DNS, al unui registru de nume TLD, al unei entități care furnizează servicii de înregistrare a numelor de domenii, al unui furnizor de servicii de *cloud computing*, al unui furnizor de servicii de centre de date, al unui furnizor de rețele de furnizare de conținut, al unui furnizor de servicii gestionate, al unui furnizor de servicii de securitate gestionate sau al unui furnizor al unei piețe online, al unui motor de căutare online sau al unei platforme de servicii de socializare în rețea, care nu este stabilit în Uniune, căreia o autoritate națională competentă sau o echipă CSIRT i se poate adresa în locul entității în cauză în ceea ce privește obligațiile entității respective în temeiul prezentei directive;

35. „entitate a administrației publice” înseamnă o entitate recunoscută ca atare într-un stat membru în conformitate cu dreptul intern, cu excepția sistemului judiciar, a parlamentelor și a băncilor centrale, care îndeplinește următoarele criterii:

    (a) a fost înființată în scopul de a răspunde unor necesități de interes general și nu are un caracter industrial sau comercial;

    (b) are personalitate juridică sau este abilitată prin lege să acționeze în numele unei alte entități cu personalitate juridică;

    (c) este finanțată, în cea mai mare parte, de stat, de autoritățile regionale sau de alte organisme de drept public, este supusă controlului de gestiune din partea autorităților sau a organismelor respective sau are un consiliu de administrație, de conducere sau de supraveghere ai cărui membri sunt desemnați în proporție de peste 50 % de stat, de autoritățile regionale sau de alte organisme de drept public;

    (d) are competența de a adresa persoanelor fizice sau juridice decizii administrative sau de reglementare care le afectează drepturile în ceea ce privește circulația transfrontalieră a persoanelor, mărfurilor, serviciilor sau capitalurilor;

36. „rețea publică de comunicații electronice” înseamnă o rețea publică de comunicații electronice astfel cum este definită la articolul 2 punctul 8 din Directiva (UE) 2018/1972;

37. „serviciu de comunicații electronice” înseamnă un serviciu de comunicații electronice astfel cum este definit la articolul 2 punctul 4 din Directiva (UE) 2018/1972;

38. „entitate” înseamnă o persoană fizică sau juridică constituită și recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații;

39. „furnizor de servicii gestionate” înseamnă o entitate care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță;

40. „furnizor de servicii de securitate gestionate” înseamnă un furnizor de servicii gestionate care efectuează sau furnizează asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică;

41. „organizație de cercetare” înseamnă o entitate care are ca obiectiv principal să desfășoare activități de cercetare aplicată sau de dezvoltare experimentală în vederea exploatării rezultatelor cercetării respective în scopuri comerciale, dar care nu include instituțiile de învățământ.

CAPITOLUL II

CADRE COORDONATE ÎN MATERIE DE SECURITATE CIBERNETICĂ

Articolul 7

Strategia națională de securitate cibernetică

(1) Fiecare stat membru adoptă o strategie națională de securitate cibernetică care prevede obiectivele strategice, resursele necesare pentru atingerea obiectivelor respective și măsurile de politică și de reglementare adecvate, în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică include următoarele elemente:

(a) obiectivele și prioritățile strategiei de securitate cibernetică a statului membru, care acoperă în special sectoarele menționate în anexele I și II;

(b) un cadru de guvernanță pentru realizarea obiectivelor și priorităților menționate la litera (a) de la prezentul alineat, inclusiv politicile menționate la alineatul (2);

(c) un cadru de guvernanță care clarifică rolurile și responsabilitățile părților interesate relevante la nivel național, care sprijină cooperarea și coordonarea la nivel național între autoritățile competente, punctele unice de contact și echipele CSIRT în temeiul prezentei directive, precum și coordonarea și cooperarea dintre aceste organisme și autoritățile competente în temeiul actelor juridice sectoriale ale Uniunii;

(d) un mecanism care să identifice activele și o evaluare a riscurilor din statul membru respectiv;

(e) o identificare a măsurilor de asigurare a pregătirii pentru incidente, a capacității de răspuns la acestea și a redresării în urma acestora, inclusiv cooperarea dintre sectorul public și cel privat;

(f) o listă a diferitelor autorități și părți interesate care participă la punerea în aplicare a strategiei naționale de securitate cibernetică;

(g) un cadru de politică menit să asigure o mai bună coordonare între autoritățile competente în temeiul prezentei directive și al Directivei (UE) 2022/2557 în scopul schimbului de informații privind riscurile, amenințările cibernetice și incidentele, precum și privind riscurile, amenințările și incidentele fără caracter cibernetic și al exercitării sarcinilor de supraveghere, după caz;

(h) un plan, inclusiv măsurile necesare pentru a spori nivelul general de sensibilizare a cetățenilor cu privire la securitatea cibernetică.

(2) În cadrul strategiei naționale de securitate cibernetică, statele membre adoptă politici:

(a) care abordează securitatea cibernetică în lanțul de aprovizionare pentru produsele TIC și serviciile TIC utilizate de entități pentru furnizarea serviciilor lor;

(b) privind includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele TIC și serviciile TIC în cadrul achizițiilor publice, inclusiv în legătură cu certificarea de securitate cibernetică, criptarea și utilizarea produselor de securitate cibernetică cu sursă deschisă;

(c) de gestionare a vulnerabilităților, inclusiv promovarea și facilitarea divulgării coordonate a vulnerabilităților în temeiul articolului 12 alineatul (1);

(d) legate de menținerea disponibilității, integrității și confidențialității generale a nucleului public al internetului deschis, inclusiv securitatea cibernetică a cablurilor de comunicații submarine, după caz;

(e) de promovare a dezvoltării și integrării tehnologiilor avansate relevante care vizează implementarea unor măsuri de ultimă generație de gestionare a riscurilor în materie de securitate cibernetică;

(f) de promovare și dezvoltare a educației și a formării privind securitatea cibernetică, competențele, sensibilizarea și inițiativele de cercetare și dezvoltare în materie de securitate cibernetică, precum și orientări privind bunele practici și controale în materie de igienă cibernetică, destinate cetățenilor, părților interesate și entităților;

(g) de sprijinire a instituțiilor academice și de cercetare în vederea dezvoltării, consolidării și promovării implementării unor instrumente de securitate cibernetică și a unei infrastructuri de rețele securizate;

(h) care să includă proceduri relevante și instrumente adecvate de schimb de informații care să sprijine schimbul voluntar de informații în materie de securitate cibernetică între entități, în conformitate cu dreptul Uniunii;

(i) de consolidare a rezilienței cibernetice și a nivelului de referință în materie de igienă cibernetică pentru întreprinderile mici și mijlocii, în special pentru cele excluse din domeniul de aplicare al prezentei directive, prin furnizarea de orientări și asistență ușor accesibile pentru nevoile lor specifice;

(j) de promovare a unei protecții cibernetice active.

(3) Statele membre notifică Comisiei strategiile lor naționale de securitate cibernetică în termen de trei luni de la adoptarea acestora. Statele membre pot exclude din astfel de notificări informații care se referă la securitatea lor națională.

(4) Statele membre își evaluează periodic, dar cel puțin o dată la cinci ani, strategiile naționale de securitate cibernetică pe baza indicatorilor-cheie de performanță și, dacă este necesar, le actualizează. ENISA sprijină statele membre, la cererea acestora, la elaborarea sau actualizarea unei strategii naționale de securitate cibernetică și a unor indicatori-cheie de performanță pentru evaluarea strategiei respective, în vederea alinierii acesteia la cerințele și obligațiile prevăzute în prezenta directivă.

Articolul 8

Autoritățile naționale competente și punctele unice de contact

(1) Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere menționate în capitolul VII (autorități competente).

(2) Autoritățile competente menționate la alineatul (1) monitorizează punerea în aplicare a prezentei directive la nivel național.

(3) Fiecare stat membru desemnează sau instituie un punct unic de contact. În cazul în care un stat membru desemnează sau instituie o singură autoritate competentă conform alineatului (1), autoritatea competentă respectivă servește, de asemenea, drept punct unic de contact pentru statul membru respectiv.

(4) Fiecare punct unic de contact exercită o funcție de legătură menită să asigure cooperarea transfrontalieră a autorităților din statul membru de care aparține cu autoritățile relevante din alte state membre, și, acolo unde este cazul, cu Comisia și cu ENISA, dar și să asigure cooperarea transsectorială cu alte autorități competente din statul membru de care aparține.

(5) Statele membre se asigură că autoritățile lor competente și punctele unice de contact dispun de resurse adecvate pentru a-și îndeplini în mod eficace și eficient atribuțiile și a realiza astfel obiectivele prezentei directive.

(6) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea autorității competente menționate la alineatul (1) și a punctului unic de contact menționat la alineatul (3), sarcinile respectivelor autorități și orice modificare ulterioară a acestora. Fiecare stat membru face publică identitatea autorității sale competente. Comisia face publică lista punctelor unice de contact.

Articolul 9

Cadrele naționale de gestionare a crizelor cibernetice

(1) Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor (denumite în continuare „autorități de gestionare a crizelor cibernetice”). Statele membre se asigură că respectivele autorități dispun de resurse adecvate pentru a îndeplini, în mod eficace și eficient, sarcinile care le-au fost încredințate. Statele membre asigură corelarea cu cadrele existente pentru gestionarea națională generală a crizelor.

(2) În cazul în care un stat membru desemnează sau instituie mai mult de o autoritate de gestionare a crizelor cibernetice în temeiul alineatului (1), acesta indică în mod clar care dintre autoritățile respective servește drept coordonator pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor.

(3) Fiecare stat membru identifică capacitățile, mijloacele și procedurile care pot fi utilizate în caz de criză în sensul prezentei directive.

(4) Fiecare stat membru adoptă un plan național de răspuns la incidente de securitate cibernetică de mare amploare și crize, în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor de securitate cibernetică de mare amploare și a crizelor. Planul respectiv stabilește, în special:

(a) obiectivele măsurilor și ale activităților naționale de pregătire;

(b) sarcinile și responsabilitățile autorităților de gestionare a crizelor cibernetice;

(c) procedurile de gestionare a crizelor cibernetice, inclusiv integrarea acestora în cadrul național general de gestionare a crizelor și canalele de schimb de informații;

(d) măsurile naționale de pregătire, inclusiv exerciții și activități de formare;

(e) părțile interesate relevante din sectorul public și privat și infrastructura implicată;

(f) procedurile naționale și acordurile dintre autoritățile și organismele naționale relevante menite să asigure participarea efectivă a statului membru la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor la nivelul Uniunii și sprijinul acordat de acesta.

(5) În termen de trei luni de la desemnarea sau instituirea autorității de gestionare a crizelor cibernetice menționate la alineatul (1), fiecare stat membru notifică Comisiei identitatea autorității sale și orice modificări ulterioare ale acesteia. Statele membre prezintă Comisiei și Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) informații relevante referitoare la cerințele de la alineatul (4) cu privire la planurile lor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize, în termen de trei luni de la adoptarea planurilor respective. Statele membre pot exclude informații în cazul și în măsura în care o asemenea excludere este necesară pentru securitatea lor națională.

Articolul 10

Echipele de intervenție în caz de incidente de securitate informatică (echipe CSIRT)

(1) Fiecare stat membru desemnează sau instituie una sau mai multe echipe CSIRT. Echipele CSIRT pot fi desemnate sau instituite din cadrul unei autorități competente. Echipele CSIRT respectă cerințele prevăzute la articolul 11 alineatul (1), acoperă cel puțin sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II și sunt responsabile de gestionarea incidentelor în conformitate cu o procedură bine definită.

(2) Statele membre se asigură că fiecare echipă CSIRT dispune de resurse adecvate pentru a-și îndeplini efectiv sarcinile stabilite la articolul 11 alineatul (3).

(3) Statele membre se asigură că fiecare echipă CSIRT dispune de o infrastructură de comunicare și de informații adecvată, sigură și reziliență prin care face schimb de informații cu entitățile esențiale și entitățile importante și cu alte părți interesate relevante. În acest scop, statele membre se asigură că fiecare echipă CSIRT contribuie la implementarea unor instrumente securizate de schimb de informații.

(4) Echipele CSIRT cooperează și, după caz, fac schimb de informații relevante în conformitate cu articolul 29 cu comunități sectoriale sau transsectoriale formate din entități esențiale și entități importante.

(5) Echipele CSIRT participă la evaluările *inter pares* organizate în conformitate cu articolul 19.

(6) Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT în cadrul rețelei CSIRT.

(7) Echipele CSIRT pot stabili relații de cooperare cu echipele naționale de intervenție în caz de incidente de securitate informatică din țări terțe. În cadrul acestor relații de cooperare, statele membre facilitează un schimb de informații eficace, eficient și securizat cu respectivele echipe naționale de intervenție în caz de incidente de securitate informatică din țări terțe, utilizând protocoalele relevante de schimb de informații, inclusiv „*Traffic Light Protocol*". Echipele CSIRT pot face schimb de informații relevante cu echipele naționale de intervenție în caz de incidente de securitate informatică din țări terțe, inclusiv de date cu caracter personal în conformitate cu dreptul Uniunii privind protecția datelor.

(8) Echipele CSIRT pot coopera cu echipele naționale de intervenție în caz de incidente de securitate informatică sau cu organisme echivalente din țări terțe, în special pentru a le oferi asistență în materie de securitate cibernetică.

(9) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea echipei CSIRT menționate la alineatul (1) de la prezentul articol și a echipei CSIRT desemnată drept coordonator în conformitate cu articolul 12 alineatul (1), sarcinile acestora în legătură cu entitățile esențiale și entitățile importante, precum și orice modificări ulterioare.

(10) Statele membre pot solicita asistența ENISA pentru instituirea echipelor lor CSIRT.

Articolul 11

Cerințele pe care trebuie să le respecte, capacitățile tehnice și sarcinile care le revin echipelor CSIRT

(1) Echipele CSIRT trebuie să respecte următoarele cerințe:

(a) echipele CSIRT asigură o disponibilitate ridicată a canalelor lor de comunicare evitând punctele unice de defecțiune și dispun de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment; acestea specifică în mod clar canalele de comunicare și le aduc la cunoștința bazei de utilizatori și a partenerilor de cooperare;

(b) localurile echipelor CSIRT și sistemele informatice de suport sunt situate în amplasamente securizate;

(c) echipele CSIRT dispun de un sistem adecvat de gestionare și rutare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor;

(d) echipele CSIRT asigură confidențialitatea și credibilitatea operațiunilor lor;

(e) echipele CSIRT dispun de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor și se asigură că personalul lor este format în mod corespunzător;

(f) echipele CSIRT sunt echipate cu sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor.

Echipele CSIRT pot participa la rețele internaționale de cooperare.

(2) Statele membre se asigură că echipele lor CSIRT dispun colectiv de capacitățile tehnice necesare pentru a-și îndeplini sarcinile menționate la alineatul (3). Statele membre se asigură că se alocă resurse suficiente echipelor lor CSIRT pentru a garanta un nivel adecvat de personal pentru ca acestea să își poată dezvolta capacitățile tehnice.

(3) Echipelor CSIRT le revin următoarele sarcini:

(a) monitorizarea și analizarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor la nivel național și, la cerere, acordarea de asistență entităților esențiale și entităților importante implicate cu privire la monitorizarea în timp real sau în timp aproape real a rețelei lor și a sistemelor lor informatice;

(b) asigurarea unor mecanisme de avertizare timpurii, alerte, anunțuri și diseminare de informații către entitățile esențiale și entitățile importante, precum și către autoritățile competente și alte părți interesate relevante cu privire la amenințările cibernetice, vulnerabilități și incidente, în timp aproape real, dacă este posibil;

(c) răspunsul la incidente și acordarea de asistență entităților esențiale și entitățile importante implicate, atunci când este cazul;

(d) colectarea și analizarea datelor criminalistice și furnizarea de analize dinamice de risc și de incident și conștientizarea situației în materie de securitate cibernetică;

(e) furnizarea, la cererea unei entități esențiale sau a unei entități importante, a unei scanări proactive a rețelelor și a sistemelor informatice ale entității implicate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ;

(f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă în funcție de capacitățile și competențele lor altor membri ai rețelei, la cererea acestora;

(g) după caz, acționarea în calitate de coordonator în scopul procesului de divulgare coordonată a vulnerabilităților menționat la articolul 12 alineatul (1);

(h) contribuirea la implementarea unor instrumente securizate de schimb de informații, în temeiul articolului 10 alineatul (3).

Echipele CSIRT pot efectua scanări proactive și neintruzive ale rețelelor și sistemelor informatice accesibile publicului ale entităților esențiale și ale entităților importante. Asemenea scanări se efectuează pentru a detecta rețelele și sistemele informatice vulnerabile sau configurate în mod nesigur și pentru a informa entitățile în cauză. Asemenea scanări nu au niciun impact negativ asupra funcționării serviciilor entităților.

Atunci când îndeplinesc sarcinile menționate la primul paragraf, echipele CSIRT pot acorda prioritate anumitor sarcini pe baza unei abordări bazate pe riscuri.

(4) Echipele CSIRT stabilesc relații de cooperare cu părțile interesate relevante din sectorul privat, în vederea îndeplinirii obiectivelor prezentei directive.

(5) Pentru a facilita cooperarea menționată la alineatul (4), echipele CSIRT promovează adoptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu:

(a) procedurile de gestionare a incidentelor;

(b) gestionarea crizelor; și

(c) divulgarea coordonată a vulnerabilităților în temeiul articolului 12 alineatul (1).

Articolul 12

Divulgarea coordonată a vulnerabilităților și baza de date europeană a vulnerabilităților

(1) Fiecare stat membru desemnează una dintre echipele sale CSIRT drept coordonator în scopul divulgării coordonate a vulnerabilităților. Echipa CSIRT desemnată drept coordonator acționează ca intermediar de încredere, facilitând, dacă este necesar, interacțiunea dintre persoana fizică sau juridică care raportează o vulnerabilitate și producătorul sau furnizorul de produse TIC sau servicii TIC potențial vulnerabile, la cererea oricărei părți. Sarcinile echipei CSIRT desemnate drept coordonator includ:

(a) identificarea și contactarea entităților implicate;

(b) asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate;

(c) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități.

Statele membre se asigură că persoanele fizice sau juridice pot raporta, în mod anonim atunci când solicită acest lucru, o vulnerabilitate echipei CSIRT desemnate drept coordonator. Echipa CSIRT desemnată drept coordonator se asigură că au loc acțiuni subsecvente susținute în ceea ce privește vulnerabilitatea raportată și asigură anonimatul persoanei fizice sau juridice care raportează vulnerabilitatea. În cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra entităților în mai multe state membre, echipa CSIRT desemnată drept coordonator din fiecare stat membru în cauză cooperează, dacă este cazul, cu alte echipe CSIRT desemnate drept coordonatori în cadrul rețelei CSIRT.

(2) ENISA creează și menține, după consultarea Grupului de cooperare, o bază de date europeană a vulnerabilităților. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate și adoptă măsurile tehnice și organizatorice necesare pentru a garanta securitatea și integritatea bazei de date europene a vulnerabilităților, în special pentru a permite entităților, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze, pe bază voluntară, vulnerabilitățile public cunoscute din produsele TIC sau serviciile TIC. Se oferă acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în baza de date europeană a vulnerabilităților. Baza de date include:

(a) informații care descriu vulnerabilitatea;

(b) produsele TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată;

(c) disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări oferite de autoritățile competente sau de echipele CSIRT adresate utilizatorilor de produse TIC și servicii TIC vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate.

Articolul 13

Cooperarea la nivel național

(1) Atunci când sunt separate, autoritățile competente, punctul unic de contact și echipele CSIRT ale aceluiași stat membru cooperează între ele pentru îndeplinirea obligațiilor ce le revin în temeiul prezentei directive.

(2) Statele membre se asigură că echipele lor CSIRT sau, atunci când este cazul, autoritățile lor competente primesc notificări privind incidentele semnificative în temeiul articolului 23, și incidentele, amenințările cibernetice și incidentele evitate la limită în temeiul articolului 30.

(3) Statele membre se asigură că echipele sale CSIRT sau, atunci când este cazul, autoritățile sale competente informează punctele lor unice de contact cu privire la notificările privind incidentele, amenințările cibernetice și incidentele evitate la limită comunicate în temeiul prezentei directive.

(4) Pentru a garanta că sarcinile și obligațiile autorităților competente, ale punctelor unice de contact și ale echipelor CSIRT sunt îndeplinite în mod eficient, statele membre asigură, în măsura posibilului, o cooperare adecvată între aceste organisme și autoritățile de aplicare a legii, autoritățile pentru protecția datelor, autoritățile naționale în temeiul Regulamentelor (CE) nr. 300/2008 și (UE) 2018/1139, organismele de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, autoritățile competente în temeiul Regulamentului (UE) 2022/2554, autoritățile naționale de reglementare în temeiul Directivei (UE) 2018/1972, autoritățile competente în temeiul Directivei (UE) 2022/2557, precum și autoritățile competente în temeiul altor acte juridice sectoriale ale Uniunii, din statul membru respectiv.

(5) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive și autoritățile lor competente în temeiul Directivei (UE) 2022/2557 cooperează și fac schimb periodic de informații pentru identificarea entităților critice, cu privire la riscurile, amenințările cibernetice și incidentele, precum și la riscurile, amenințările și incidentele de altă natură decât cibernetică care afectează entitățile esențiale identificate ca fiind critice în temeiul Directivei (UE) 2022/2557, precum și cu privire la măsurile luate ca răspuns la astfel de riscuri, amenințări și incidente. Statele membre se asigură, de asemenea, că autoritățile lor competente în temeiul prezentei directive și autoritățile lor competente în temeiul Regulamentului (UE) nr. 910/2014, al Regulamentului (UE) 2022/2554 și al Directivei (UE) 2018/1972 fac schimb de informații relevante în mod periodic, inclusiv în ceea ce privește incidentele și amenințările cibernetice relevante.

(6) Statele membre simplifică raportarea prin mijloace tehnice pentru notificările menționate la articolele 23 și 30.

CAPITOLUL III

COOPERARE LA NIVELUL UNIUNII ȘI LA NIVEL INTERNAȚIONAL

Articolul 14

Grupul de cooperare

(1) Pentru a sprijini și a facilita cooperarea strategică și schimbul de informații între statele membre, precum și pentru a consolida încrederea, se instituie un Grup de cooperare.

(2) Grupul de cooperare își îndeplinește sarcinile pe baza programelor bienale de lucru menționate la alineatul (7).

(3) Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă participă la activitățile Grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) și autoritățile competente în temeiul Regulamentului (UE) 2022/2554 pot participa la activitățile Grupului de cooperare în conformitate cu articolul 47 alineatul (1) din regulamentul respectiv.

După caz, Grupul de cooperare poate invita să participe la lucrările sale Parlamentul European și reprezentanți ai părților interesate relevante.

Comisia asigură secretariatul.

(4) Grupului de cooperare îi revin următoarele sarcini:

(a) furnizarea de orientări autorităților competente în legătură cu transpunerea și punerea în aplicare a prezentei directive;

(b) furnizarea de orientări autorităților competente în legătură cu elaborarea și punerea în aplicare a politicilor privind divulgarea coordonată a vulnerabilităților, astfel cum se menționează la articolul 7 alineatul (2) litera (c);

(c) schimbul de bune practici și de informații în legătură cu punerea în aplicare a prezentei directive, inclusiv în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, incidentele evitate la limită, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, standardele și specificațiile tehnice, precum și identificarea entităților esențiale și a entităților importante în temeiul articolului 2 alineatul (2) literele (b)-(e);

(d) schimbul de opinii și cooperarea cu Comisia cu privire la inițiativele emergente de politică în materie de securitate cibernetică, precum și coerența generală a cerințelor de securitate cibernetică specifice fiecărui sector;

(e) schimbul de opinii și cooperarea cu Comisia cu privire la proiectele de acte delegate sau de punere în aplicare adoptate în temeiul prezentei directive;

(f) schimbul de bune practici și de informații cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii;

(g) schimbul de opinii cu privire la punerea în aplicare a actelor juridice sectoriale ale Uniunii care conțin dispoziții privind securitatea cibernetică;

(h) atunci când este cazul, discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 19 alineatul (9) și stabilirea de concluzii și recomandări;

(i) efectuarea unor evaluări coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice, în conformitate cu articolul 22 alineatul (1);

(j) discutarea cazurilor de asistență reciprocă, inclusiv a experiențelor și rezultatelor acțiunilor comune de supraveghere transfrontaliere, astfel cum se menționează la articolul 37;

(k) la cererea unuia sau a mai multor state membre în cauză, discutarea cererilor specifice de asistență reciprocă astfel cum se menționează la articolul 37;

(l) furnizarea de orientări strategice rețelei CSIRT și EU-CyCLONe cu privire la aspecte emergente specifice;

(m) schimbul de opinii cu privire la politica privind acțiunile ulterioare incidentelor de securitate cibernetică de mare amploare și crizelor, pe baza lecțiilor învățate din rețeaua CSIRT și EU-CyCLONe;

(n) contribuția la capacitățile în materie de securitate cibernetică în întreaga Uniune prin facilitarea schimbului de funcționari naționali prin intermediul unui program de consolidare a capacităților care implică personal din cadrul autorităților competente sau al echipelor CSIRT;

(o) organizarea de reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară Grupul de cooperare și pentru a colecta informații cu privire la provocările emergente în materie de politici;

(p) discutarea activității desfășurate în legătură cu exercițiile de securitate cibernetică, inclusiv a activității desfășurate de ENISA;

(q) stabilirea metodologiei și a aspectelor organizatorice ale evaluărilor *inter pares* menționate la articolul 19 alineatul (1), precum și definirea metodologiei de autoevaluare pentru statele membre în conformitate cu articolul 19 alineatul (5), cu sprijinul Comisiei și al ENISA, și, în cooperare cu Comisia și cu ENISA, elaborarea codurilor de conduită care să stea la baza metodelor de lucru ale experților în materie de securitate cibernetică desemnați în conformitate cu articolul 19 alineatul (6);

(r) pregătirea de rapoarte în scopul revizuirii menționate la articolul 40 privind experiența obținută la nivel strategic și din evaluările *inter pares*;

(s) discutarea și efectuarea periodică a unei evaluări a situației amenințărilor sau incidentelor cibernetice, cum ar fi *ransomware*.

Grupul de cooperare prezintă rapoartele menționate la primul paragraf litera (r) Comisiei, Parlamentului European și Consiliului.

(5) Statele membre asigură cooperarea eficace, eficientă și sigură a reprezentanților lor în Grupul de cooperare.

(6) Grupul de cooperare poate solicita rețelei CSIRT un raport tehnic pe anumite teme.

(7) Până la 1 februarie 2024 și, ulterior, o dată la doi ani, Grupul de cooperare stabilește un program de lucru cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și a sarcinilor sale.

(8) Comisia poate adopta acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcționarea Grupului de cooperare.

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Comisia face schimb de opinii și cooperează cu Grupul de cooperare în ceea ce privește proiectele de acte de punere în aplicare menționate la primul paragraf de la prezentul alineat, în conformitate cu alineatul (4) litera (e).

(9) Grupul de cooperare se reunește periodic, și în toate cazurile cel puțin o dată pe an, cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) 2022/2557 pentru a promova și facilita cooperarea strategică și schimbul de informații.

Articolul 15

Rețeaua CSIRT

(1) Pentru a contribui la dezvoltarea încrederii și pentru a promova cooperarea operațională rapidă și eficace între statele membre, se stabilește o rețea a echipelor naționale CSIRT.

(2) Rețeaua echipelor CSIRT este formată din reprezentanți ai echipelor CSIRT desemnate sau instituite în temeiul articolului 10 și din Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE). Comisia participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și acordă asistență în mod activ pentru cooperarea între echipele CSIRT.

(3) Rețelei CSIRT îi revin următoarele sarcini:

(a) schimbul de informații privind capacitățile echipelor CSIRT;

(b) facilitarea partajării, transferului și schimbului de tehnologie și măsuri, politici, instrumente, procese, bune practici și cadre relevante între echipele CSIRT;

(c) schimbul de informații relevante privind incidentele, incidentele evitate la limită, amenințările cibernetice, riscurile și vulnerabilitățile;

(d) schimbul de informații în ceea ce privește publicațiile și recomandările în materie de securitate cibernetică;

(e) asigurarea interoperabilității în ceea ce privește specificațiile și protocoalele referitoare la schimbul de informații;

(f) la cererea unui membru al rețelei CSIRT care ar putea fi afectat de un incident, schimbul de informații și discutarea informațiilor cu privire la incidentul respectiv și la amenințările cibernetice, riscurile și vulnerabilitățile conexe;

(g) la cererea unui membru al rețelei CSIRT, discutarea și, după caz, punerea în aplicare a unui răspuns coordonat la un incident care a fost identificat în jurisdicția statului membru respectiv;

(h) furnizarea de asistență statelor membre în abordarea incidentelor transfrontaliere în temeiul prezentei directive;

(i) cooperarea, schimbul de bune practici și furnizarea de asistență echipelor CSIRT desemnate drept coordonatori în temeiul articolului 12 alineatul (1) în ceea ce privește gestionarea divulgării coordonate a vulnerabilităților care ar putea avea un impact semnificativ asupra entităților din mai multe state membre;

(j) discutarea și identificarea de noi forme de cooperare operațională, inclusiv în legătură cu:

(i) categoriile de amenințări cibernetice și incidente;

(ii) alertele timpurii;

(iii) asistența reciprocă;

(iv) principiile și modalitățile de coordonare, ca răspuns la riscuri și incidente transfrontaliere;

(v) contribuția la planul național de răspuns la incidente de securitate cibernetică de mare amploare și crize menționat la articolul 9 alineatul (4), la solicitarea unui stat membru;

(k) informarea Grupului de cooperare cu privire la activitățile sale și cu privire la noi forme de cooperare operațională discutate în temeiul literei (j) și, după caz, solicitarea de orientări în acest sens;

(l) bilanțul exercițiilor de securitate cibernetică, inclusiv al celor organizate de ENISA;

(m) la cererea unei anumite echipe CSIRT, discutarea capacităților și a nivelului de pregătire al echipei CSIRT respective;

(n) cooperarea și schimbul de informații cu centrele de operațiuni de securitate la nivel regional și la nivelul Uniunii pentru a îmbunătăți conștientizarea comună a situației cu privire la incidentele și amenințările cibernetice din întreaga Uniune;

(o) atunci când este cazul, discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 19 alineatul (9);

(p) oferirea de orientări pentru a facilita convergența practicilor operaționale în ceea ce privește aplicarea dispozițiilor prezentului articol referitoare la cooperarea operațională.

(4) Până la 17 ianuarie 2025 și, ulterior, o dată la doi ani, rețeaua CSIRT evaluează, în scopul revizuirii menționate la articolul 40, progresele înregistrate în ceea ce privește cooperarea operațională și adoptă un raport. Raportul formulează, în special, concluzii și recomandări pe baza rezultatelor evaluărilor *inter pares* menționate la articolul 19, care sunt efectuate în legătură cu echipele naționale CSIRT. Raportul respectiv se transmite Grupului de cooperare.

(5) Rețeaua CSIRT își adoptă regulamentul de procedură.

(6) Rețeaua CSIRT și EU-CyCLONe convin asupra modalităților procedurale și cooperează pe baza acestora.

Articolul 16

Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU - CyCLONe)

(1) EU-CyCLONe este instituită pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organele, oficiile și agențiile Uniunii.

(2) EU-CyCLONe este compusă din reprezentanți ai autorităților de gestionare a crizelor cibernetice din statele membre, precum și, în cazurile în care un incident de securitate cibernetică de mare amploare potențial sau în curs de desfășurare are sau este probabil să aibă un impact semnificativ asupra serviciilor și activităților care intră în domeniul de aplicare al prezentei directive, reprezentanți ai Comisiei. În celelalte cazuri, Comisia participă la activitățile EU-CyCLONe în calitate de observator.

ENISA asigură secretariatul EU-CyCLONe și sprijină schimbul securizat de informații și, de asemenea, furnizează instrumentele necesare pentru sprijinirea cooperării dintre statele membre, asigurând schimbul securizat de informații.

După caz, EU-CyCLONe poate invita să participe la lucrările sale, în calitate de observatori, reprezentanți ai părților interesate relevante.

(3) EU-CyCLONe are următoarele sarcini:

(a) consolidarea nivelului de pregătire pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor;

(b) dezvoltarea unei conștientizări comune a situației în cazul incidentelor de securitate cibernetică de mare amploare și al crizelor;

(c) evaluarea consecințelor și a impactului incidentelor de securitate cibernetică de mare amploare și crizelor relevante și propunerea unor posibile măsuri de atenuare;

(d) coordonarea gestionării incidentelor de securitate cibernetică de mare amploare și a crizelor și sprijinirea procesului decizional la nivel politic în legătură cu astfel de incidente și crize;

(e) discutarea, la solicitarea unui stat membru în cauză, a planurilor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize menționate la articolul 9 alineatul (4).

(4) EU-CyCLONe își adoptă regulamentul de procedură.

(5) EU-CyCLONe prezintă periodic rapoarte Grupului de cooperare cu privire la gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor, precum și la tendințe, concentrându-se în special pe impactul acestora asupra entităților esențiale și a entităților importante.

(6) EU-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite prevăzute la articolul 15 alineatul (6).

(7) Până la 17 iulie 2024 și, ulterior, la fiecare 18 luni, EU-CyCLONe prezintă un raport Parlamentului European și Consiliului în care își evaluează activitatea.

Articolul 17

Cooperarea internațională

După caz, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare, ale rețelei CSIRT, precum și ale EU-CyCLONe. Aceste acorduri respectă dreptul Uniunii în materie de protecție a datelor.

Articolul 18

Raportul privind situația în materie de securitate cibernetică în Uniune

(1) ENISA adoptă, în cooperare cu Comisia și Grupul de cooperare, un raport bienal privind situația în materie de securitate cibernetică în Uniune și înaintează și prezintă respectivul raport Parlamentului European. Raportul este, printre altele, pus la dispoziție într-un format citibil automat și include următoarele:

(a) o evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, ținând seama de situația amenințărilor cibernetice;

(b) o evaluare a dezvoltării capacităților în materie de securitate cibernetică în sectorul public și cel privat în întreaga Uniune;

(c) o evaluare a nivelului general de sensibilizare cu privire la securitatea cibernetică și igiena cibernetică în rândul cetățenilor și entităților, inclusiv al întreprinderilor mici și mijlocii;

(d) o evaluare globală a rezultatelor evaluărilor *inter pares* menționate la articolul 19;

(e) o evaluare globală a nivelului de maturitate a capacităților și a resurselor în materie de securitate cibernetică în întreaga Uniune, inclusiv a celor de la nivel sectorial, precum și a gradului de aliniere a strategiilor naționale de securitate cibernetică ale statelor membre.

(2) Raportul include recomandări de politică specifice pentru a aborda deficiențele și a îmbunătăți nivelul de securitate cibernetică în întreaga Uniune și un rezumat al constatărilor pentru perioada respectivă incluse în rapoartele UE privind situația tehnică în materie de securitate cibernetică cu privire la incidente și amenințări cibernetice, pregătite de ENISA în conformitate cu articolul 7 alineatul (6) din Regulamentul (UE) 2019/881.

(3) ENISA, în cooperare cu Comisia, Grupul de cooperare și rețeaua CSIRT, elaborează metodologia, inclusiv variabilele relevante, cum ar fi indicatori cantitativi și calitativi, pentru evaluarea globală menționată la alineatul (1) litera (e).

Articolul 19

Evaluări inter pares

(1) Grupul de cooperare stabilește, până la 17 ianuarie 2025, cu sprijinul Comisiei și al ENISA și, după caz, al rețelei CSIRT, metodologia și aspectele organizatorice ale evaluărilor *inter pares* pentru a învăța din experiențele comune, a consolida încrederea reciprocă, a atinge un nivel comun ridicat de securitate cibernetică, precum și a consolida capacitățile și politicile de securitate cibernetică ale statelor membre necesare pentru punerea în aplicare a prezentei directive. Participarea la evaluările *inter pares* se face pe bază voluntară. Evaluările *inter pares* sunt efectuate de experți în materie de securitate cibernetică. Experții în materie de securitate cibernetică sunt desemnați de cel puțin două state membre, diferite de statul membru care face obiectul evaluării.

Evaluările *inter pares* acoperă cel puțin unul din următoarele elemente:

(a) nivelul punerii în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare menționate la articolele 21 și 23;

(b) nivelul capacităților, inclusiv resursele financiare, tehnice și umane disponibile, precum și eficacitatea exercitării sarcinilor autorităților competente;

(c) capacitățile operaționale ale echipelor CSIRT;

(d) nivelul de punere în aplicare a asistenței reciproce menționate la articolul 37;

(e) nivelul de punere în aplicare a acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la articolul 29;

(f) aspecte specifice de natură transfrontalieră sau transsectorială.

(2) Metodologia menționată la alineatul (1) include criterii obiective, nediscriminatorii, echitabile și transparente pe baza cărora statele membre desemnează experți în domeniul securității cibernetice eligibili pentru efectuarea evaluărilor *inter pares*. ENISA și Comisia participă în calitate de observatori la evaluările *inter pares*.

(3) Statele membre pot identifica aspecte specifice, astfel cum sunt menționate la alineatul (1) litera (f), pentru o evaluare *inter pares*.

(4) Înainte de a începe o evaluare *inter pares*, astfel cum este menționată la alineatul (1), statele membre informează statele membre participante cu privire la domeniul de aplicare al acesteia, inclusiv aspectele specifice identificate în temeiul alineatului (3).

(5) Înainte de începerea evaluării *inter pares*, statele membre pot efectua o autoevaluare a aspectelor analizate și furniza autoevaluarea respectivă experților în materie de securitate cibernetică desemnați. Grupul de cooperare, cu sprijinul Comisiei și al ENISA, stabilește metodologia pentru autoevaluarea statelor membre.

(6) Evaluările *inter pares* implică vizite fizice sau virtuale și schimburi de informații *ex situ*. În conformitate cu principiul bunei cooperări, statul membru supus evaluării *inter pares* le furnizează experților în materie de securitate cibernetică desemnați informațiile necesare pentru evaluare, fără a aduce atingere dreptului Uniunii sau dreptului intern privind protecția informațiilor confidențiale sau clasificate și protejării funcțiilor esențiale ale statului, cum ar fi securitatea națională. Grupul de cooperare, în colaborare cu Comisia și ENISA, elaborează coduri de conduită adecvate care stau la baza metodelor de lucru ale experților în materie de securitate cibernetică desemnați. Orice informație obținută prin intermediul evaluării *inter pares* este utilizată exclusiv în acest scop. Experții în materie de securitate cibernetică care participă la evaluarea *inter pares* nu divulgă terților nicio informație sensibilă sau confidențială obținută în cursul evaluării *inter pares* respective.

(7) Odată ce au făcut obiectul unei evaluări *inter pares*, aceleași aspecte evaluate într-un stat membru nu fac obiectul unei noi evaluări *inter pares* în statul membru respectiv timp de doi ani de la încheierea evaluării *inter pares*, cu excepția cazului în care statul membru decide altfel sau se convine astfel la propunerea Grupului de cooperare.

(8) Statele membre se asigură că orice risc de conflict de interese în ceea ce privește experții în materie de securitate cibernetică desemnați este dezvăluit celorlalte state membre, Grupului de cooperare, Comisiei și ENISA, înainte de începerea evaluării *inter pares*. Statul membru supus evaluării *inter pares* se poate opune desemnării anumitor experți în materie de securitate cibernetică din motive justificate corespunzător, comunicate statului membru care i-a desemnat.

(9) Experții în materie de securitate cibernetică care participă la evaluări *inter pares* elaborează rapoarte cu privire la constatările și concluziile evaluărilor *inter pares*. Statele membre care fac obiectul unei evaluări *inter pares* pot prezenta observații cu privire la proiectele de rapoarte care le privesc, iar aceste observații se anexează la rapoarte. Rapoartele includ recomandări care să faciliteze îmbunătățirea aspectelor acoperite de evaluarea *inter pares*. Rapoartele sunt transmise Grupului de cooperare și rețelei CSIRT atunci când este cazul. Un stat membru care face obiectul unei evaluări *inter pares* poate decide să pună la dispoziția publicului raportul său sau o versiune ocultată a acestuia.

CAPITOLUL IV

MĂSURI DE GESTIONARE A RISCURILOR ÎN MATERIE DE SECURITATE CIBERNETICĂ ȘI OBLIGAȚII DE RAPORTARE

Articolul 20

Guvernanța

(1) Statele membre se asigură că organele de conducere ale entităților esențiale și ale entităților importante aprobă măsurile de gestionare a riscurilor în materie de securitate cibernetică luate de entitățile respective pentru a se conforma articolului 21, supraveghează punerea în aplicare a acestuia și pot fi trase la răspundere pentru încălcarea de către entități a respectivului articol.

Aplicarea prezentului alineat nu aduce atingere dreptului intern în ceea ce privește normele referitoare la răspundere aplicabile instituțiilor publice, precum și răspunderea funcționarilor publici și a funcționarilor aleși sau numiți.

(2) Statele membre se asigură că membrii organelor de conducere din cadrul entităților esențiale și al entităților importante au obligația de a urma o formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor în materie de securitate cibernetică și impactul acestora asupra serviciilor pe care le furnizează entitatea, și încurajează entitățile esențiale și entitățile importante să ofere o formare similară tuturor angajaților în mod regulat.

Articolul 21

Măsuri de gestionare a riscurilor în materie de securitate cibernetică

(1) Statele membre se asigură că entitățile esențiale și entitățile importante iau măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care entitățile respective le utilizează pentru operațiunile lor sau pentru a furniza servicii și pentru a preveni sau reduce la minimum impactul incidentelor asupra beneficiarilor serviciilor lor și asupra altor servicii.

Ținând seama de cele mai avansate standarde în domeniu și, atunci când este cazul, de standardele europene și internaționale relevante, precum și de costul punerii în aplicare, măsurile menționate la primul paragraf asigură un nivel de securitate a rețelelor și a sistemelor informatice corespunzător riscurilor prezentate. Atunci când se evaluează proporționalitatea acestor măsuri, se ține seama în mod corespunzător de gradul de expunere a entității la riscuri, de dimensiunea entității și de probabilitatea producerii incidentelor, precum și de gravitatea acestora, inclusiv de impactul lor societal și economic.

(2) Măsurile menționate la alineatul (1) se bazează pe o abordare multirisc care vizează protejarea rețelelor și a sistemelor informatice, precum și a mediului fizic al acestor sisteme împotriva incidentelor, și includ cel puțin următoarele:

(a) politici referitoare la analiza riscurilor și securitatea sistemelor informatice;

(b) gestionarea incidentelor;

(c) continuitatea activității, de exemplu gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor;

(d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate și prestatorii sau furnizorii săi direcți de servicii;

(e) securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora;

(f) politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică;

(g) practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice;

(h) politici și proceduri privind utilizarea criptografiei și, după caz, a criptării;

(i) securitatea resurselor umane, politicile de control al accesului și gestionarea activelor;

(j) utilizarea de soluții de autentificare multifactor sau de autentificare continuă, de comunicații securizate voce, video și text și de sisteme securizate de comunicații de urgență în cadrul entității, după caz.

(3) Statele membre se asigură că, atunci când analizează care măsuri menționate la alineatul (2) litera (d) de la prezentul articol sunt adecvate, entitățile iau în considerare vulnerabilitățile specifice fiecărui prestator și furnizor direct de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare. Statele membre se asigură, de asemenea, că, atunci când analizează care măsuri menționate la litera respectivă sunt adecvate, entitățile au obligația de a ține seama de rezultatele evaluărilor coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice efectuate în conformitate cu articolul 22 alineatul (1).

(4) Statele membre se asigură că o entitate care constată că nu respectă măsurile prevăzute la alineatul (2) ia, fără întârzieri nejustificate, toate măsurile corective necesare, adecvate și proporționale.

(5) Până la 17 octombrie 2024, Comisia adoptă acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice ale măsurilor menționate la alineatul (2) în ceea ce privește furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de *cloud computing*, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere.

Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice, precum și a cerințelor sectoriale, după caz, ale măsurilor menționate la alineatul (2) în ceea ce privește entitățile esențiale și entitățile importante, altele decât cele menționate la primul paragraf de la prezentul alineat.

Atunci când pregătește actele de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat, Comisia urmează, în cea mai mare măsură posibilă, standardele europene și internaționale, precum și specificațiile tehnice relevante. Comisia face schimb de opinii și cooperează cu Grupul de cooperare și ENISA privind proiectele de acte de punere în aplicare, în conformitate cu articolul 14 alineatul (4) litera (e).

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 22

Evaluări coordonate la nivelul Uniunii ale riscurilor de securitate legate de lanțurile de aprovizionare critice

(1) Grupul de cooperare, în cooperare cu Comisia și ENISA, poate efectua evaluări coordonate ale riscurilor în materie de securitate ale anumitor servicii TIC, sisteme TIC sau lanțuri de aprovizionare cu produse TIC critice, ținând seama de factorii de risc de natură tehnică și, după caz, care nu sunt de natură tehnică.

(2) Comisia, după consultarea Grupului de cooperare și a ENISA și, atunci când este necesar, a părților interesate relevante, identifică serviciile TIC, sistemele TIC sau produsele TIC critice specifice care pot face obiectul evaluării coordonate a riscurilor de securitate menționate la alineatul (1).

Articolul 23

Obligații de raportare

(1) Fiecare stat membru se asigură că entitățile esențiale și entitățile importante notifică, fără întârzieri nejustificate, echipei CSIRT sau, după caz, autorității sale competente, în conformitate cu alineatul (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor, astfel cum se menționează la alineatul (3) (incident semnificativ). Dacă este cazul, entitățile în cauză notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor incidentele semnificative care ar putea afecta în mod negativ prestarea serviciilor respective. Fiecare stat membru se asigură că entitățile respective raportează, inter alia, orice informație care îi permite echipei CSIRT sau, după caz, autorității competente să constate orice impact transfrontalier al incidentului. Simpla notificare nu expune entitatea notificatoare unei răspunderi sporite.

În cazul în care entitățile în cauză notifică autorității competente un incident semnificativ în temeiul primului paragraf, statul membru se asigură că autoritatea competentă înaintează notificarea echipei CSIRT la primirea acesteia.

În cazul unui incident semnificativ transfrontalier sau transsectorial, statele membre se asigură că punctele lor unice de contact primesc în timp util informațiile relevante notificate în conformitate cu alineatul (4).

(2) Dacă este cazul, statele membre se asigură că entitățile esențiale și entitățile importante comunică, fără întârzieri nejustificate, destinatarilor serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă orice măsuri sau măsuri corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. Dacă este cazul, entitățile informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă.

(3) Un incident este considerat semnificativ dacă:

(a) a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză;

(b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile.

(4) Statele membre se asigură că, în scopul notificării în temeiul alineatului (1), entitățile în cauză transmit echipei CSIRT sau, după caz, autorității competente:

(a) fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care au luat cunoștință de incidentul semnificativ, o avertizare timpurie care, după caz, indică dacă există suspiciuni că incidentul semnificativ este cauzat de acțiuni ilegale sau răuvoitoare sau ar putea avea un impact transfrontalier;

(b) fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, o notificare a incidentului, care, după caz, actualizează informațiile menționate la litera (a) și prezintă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili;

(c) la cererea unei echipe CSIRT sau, după caz, a autorității competente, un raport intermediar privind actualizarea relevantă a situației;

(d) un raport final, în termen de cel mult o lună de la transmiterea notificării incidentului în temeiul literei (b), care să includă următoarele elemente:

(i) o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia;

(ii) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;

(iii) măsurile de atenuare aplicate și în curs;

(iv) dacă este cazul, impactul transfrontalier al incidentului;

(e) în cazul unui incident în desfășurare la momentul prezentării raportului final menționat la litera (d), statele membre se asigură că entitățile în cauză prezintă la momentul respectiv un raport privind progresele înregistrate și un raport final în termen de o lună de la gestionarea incidentului.

Prin derogare de la primul paragraf litera (b), un prestator de servicii de încredere notifică, în ceea ce privește incidentele semnificative care afectează prestarea serviciilor sale de încredere, echipa CSIRT sau, după caz, autoritatea competentă, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de incidentul semnificativ.

(5) Echipa CSIRT sau autoritatea competentă furnizează, fără întârzieri nejustificate și, atunci când este posibil, în termen de 24 de ore de la primirea alertei timpurii menționate la alineatul (4) litera (a), un răspuns entității notificatoare, inclusiv un feedback inițial cu privire la incidentul semnificativ și, la cererea entității, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de atenuare. În cazul în care echipa CSIRT nu este destinatarul inițial al notificării menționate la alineatul (1), orientările sunt furnizate de autoritatea competentă în colaborare cu echipa CSIRT. Echipa CSIRT furnizează sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se suspectează că incidentul este de natură penală, echipa CSIRT sau autoritatea competentă furnizează, de asemenea, orientări privind raportarea incidentului către autoritățile de aplicare a legii.

(6) După caz, și în special dacă incidentul semnificativ implică două sau mai multe state membre, echipa CSIRT, autoritatea competentă sau punctul unic de contact informează, fără întârzieri nejustificate, celelalte state membre afectate și ENISA cu privire la incidentul semnificativ. Aceste informații includ tipul de informații primite în conformitate cu alineatul (4). Astfel, echipa CSIRT, autoritatea competentă sau punctul unic de contact, în conformitate cu dreptul Uniunii sau dreptul intern, protejează interesele de securitate și comerciale ale entității, precum și confidențialitatea informațiilor furnizate.

(7) În cazul în care sensibilizarea publicului este necesară pentru a preveni un incident semnificativ sau pentru a gestiona un incident semnificativ în curs sau în cazul în care divulgarea incidentului semnificativ este în alt mod în interesul public, echipa CSIRT a unui stat membru sau, după caz, autoritatea sa competentă, și, după caz, echipele CSIRT sau autoritățile competente din alte state membre în cauză pot, după consultarea entității în cauză, să informeze publicul cu privire la incidentul semnificativ sau să solicite entității să facă acest lucru.

(8) La cererea echipei CSIRT sau a autorității competente, punctul unic de contact înaintează notificările primite în temeiul alineatului (1) punctelor unice de contact din celelalte state membre afectate.

(9) Punctul unic de contact transmite ENISA o dată la trei luni un raport de sinteză care include date anonimizate și agregate privind incidentele semnificative, incidentele, amenințările cibernetice semnificative și incidentele evitate la limită notificate în conformitate cu alineatul (1) de la prezentul articol și cu articolul 30. Pentru a contribui la furnizarea de informații comparabile, ENISA poate adopta orientări tehnice cu privire la parametrii informațiilor care trebuie incluse în raportul de sinteză. ENISA informează Grupul de cooperare și rețeaua CSIRT cu privire la constatările sale referitoare la notificările primite o dată la șase luni.

(10) Echipele CSIRT sau, după caz, autoritățile competente furnizează autorităților competente în temeiul Directivei (UE) 2022/2557 informații cu privire la incidentele semnificative, incidentele, amenințările cibernetice și incidentele evitate la limită notificate în conformitate cu alineatul (1) de la prezentul articol și cu articolul 30 de către entitățile identificate ca fiind entități critice în temeiul Directivei (UE) 2022/2557.

(11) Comisia poate adopta acte de punere în aplicare pentru a preciza mai în detaliu tipul de informații, formatul și procedura referitoare la o notificare transmisă în temeiul alineatului (1) de la prezentul articol și al articolului 30 și la o comunicare transmisă în temeiul alineatului (2) de la prezentul articol.

Până la 17 octombrie 2024, Comisia adoptă, în ceea ce privește furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de *cloud computing*, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, acte de punere în aplicare pentru a preciza mai în detaliu cazurile în care un incident este considerat a fi semnificativ, astfel cum se menționează la alineatul (3). Comisia poate adopta astfel de acte de punere în aplicare și pentru alte entități esențiale și entități importante.

Comisia face schimb de opinii și cooperează cu Grupul de cooperare privind proiectele de acte de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat, în conformitate cu articolul 14 alineatul (4) litera (e).

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 24

Utilizarea sistemelor europene de certificare a securității cibernetice

(1) Pentru a demonstra conformitatea cu anumite cerințe de la articolul 21, statele membre le pot solicita entităților esențiale și entităților importante să utilizeze anumite produse TIC, servicii TIC și procese TIC, dezvoltate de entități esențiale sau de entități importante ori achiziționate de la părți terțe, care sunt certificate în cadrul sistemelor europene de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. De asemenea, statele membre încurajează entitățile esențiale și entitățile importante să utilizeze servicii de încredere calificate.

(2) Comisia este împuternicită să adopte acte delegate, în conformitate cu articolul 38, pentru a completa prezenta directivă prin specificarea categoriilor de entități esențiale și de entități importante care au obligația de a utiliza anumite produse TIC, servicii TIC și procese TIC certificate sau de a obține un certificat în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 din Regulamentul (UE) 2019/881. Respectivele acte delegate se adoptă atunci când se identifică niveluri insuficiente de securitate cibernetică și includ o perioadă de punere în aplicare.

Înainte de a adopta astfel de acte delegate, Comisia efectuează o evaluare a impactului și desfășoară consultări în conformitate cu articolul 56 din Regulamentul (UE) 2019/881.

(3) În cazurile în care nu este disponibil niciun sistem european adecvat de certificare a securității cibernetice în sensul alineatului (2) de la prezentul articol, Comisia poate solicita ENISA să pregătească o propunere de sistem în temeiul articolului 48 alineatul (2) din Regulamentul (UE) 2019/881, după consultarea Grupului de cooperare și a Grupului european pentru certificarea securității cibernetice.

Articolul 25

Standardizarea

(1) Pentru promovarea punerii în aplicare convergente a articolului 21 alineatele (1) și (2), statele membre, fără a impune un anumit tip de tehnologie sau a discrimina în favoarea utilizării acestuia, încurajează utilizarea standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice.

(2) ENISA, în cooperare cu statele membre și, după caz, după consultarea părților interesate relevante, elaborează avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale, care ar permite reglementarea respectivelor domenii.

CAPITOLUL V

JURISDICȚIE ȘI ÎNREGISTRARE

Articolul 26

Jurisdicție și teritorialitate

(1) Entitățile care intră în domeniul de aplicare al prezentei directive sunt considerate ca fiind sub jurisdicția statului membru în care sunt stabilite, cu următoarele excepții:

(a) furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului, care se consideră că intră sub jurisdicția statului membru în care își prestează serviciile;

(b) furnizorii de servicii DNS, registrele de nume TLD, entitățile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii de *cloud computing*, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, care se consideră că se află sub jurisdicția statului membru în care își au sediul principal în Uniune în temeiul alineatului (2);

(c) entitățile administrației publice, care se consideră că intră sub jurisdicția statului membru care le-a instituit.

(2) În sensul prezentei directive, se consideră că o entitate, astfel cum este menționată la alineatul (1) litera (b), își are sediul principal din Uniune în statul membru în care se iau în mod predominant deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică. Dacă un astfel de stat membru nu poate fi stabilit sau dacă astfel de decizii nu sunt luate în Uniune, sediul principal este considerat a fi în statul membru în care se desfășoară operațiunile de securitate cibernetică. Dacă un astfel de stat membru nu poate fi stabilit, sediul principal este considerat a fi în statul membru în care entitatea în cauză își are sediul cu cel mai mare număr de angajați din Uniune.

(3) În cazul în care o entitate, astfel cum este menționată la alineatul (1) litera (b), nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant în Uniune desemnat în temeiul prezentului alineat, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru încălcarea prezentei directive.

(4) Desemnarea unui reprezentant de către o entitate, astfel cum este menționată la alineatul (1) litera (b), nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva entității înseși.

(5) Statele membre care au primit o cerere de asistență reciprocă în legătură cu o entitate, astfel cum este menționată la alineatul (1) litera (b), pot, în limitele cererii respective, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în ceea ce privește entitatea în cauză care furnizează servicii sau care are o rețea și un sistem informatic pe teritoriul lor.

Articolul 27

Registrul entităților

(1) ENISA creează și păstrează un registru al furnizorilor de servicii DNS, registrelor de nume TLD, al entităților care prestează servicii de înregistrare a numelor de domenii, al furnizorilor de servicii de *cloud computing*, al furnizorilor de servicii de centre de date, al furnizorilor de rețele de furnizare de conținut, al furnizorilor de servicii gestionate, al furnizorilor de servicii de securitate gestionate, precum și al furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, pe baza informațiilor primite de la punctele unice de contact în conformitate cu alineatul (4). La cerere, ENISA permite accesul autorităților competente la registrul respectiv, asigurându-se în același timp că confidențialitatea informațiilor este protejată, după caz.

(2) Până la 17 ianuarie 2025, statele membre solicită entităților menționate la alineatul (1) să transmită autorităților competente următoarele informații:

(a) denumirea entității;

(b) sectorul, subsectorul relevant și tipul de entitate menționate în anexa I sau II, după caz;

(c) adresa sediului principal al entității și a celorlalte sedii legale ale sale din Uniune sau, dacă nu este stabilită în Uniune, adresa reprezentantului său desemnat în temeiul articolului 26 alineatul (3);

(d) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale entității și, după caz, ale reprezentantului său desemnat în temeiul articolului 26 alineatul (3);

(e) statele membre în care entitatea furnizează servicii; și

(f) gamele de adrese IP ale entității.

(3) Statele membre se asigură că entitățile menționate la alineatul (1) notifică autorității competente fără întârziere și, în orice caz, în termen de trei luni de la data modificării, orice modificare a informațiilor pe care le-au transmis în temeiul alineatului (2).

(4) După ce primește informațiile menționate la alineatele (2) și (3), cu excepția celor menționate la alineatul (2) litera (f), punctul unic de contact al statului membru în cauză le înaintează către ENISA, fără întârzieri nejustificate.

(5) După caz, informațiile menționate la alineatele (2) și (3) de la prezentul articol se transmit prin mecanismul național menționat la articolul 3 alineatul (4) al patrulea paragraf.

Articolul 28

Baza de date pentru datele de înregistrare a numelor de domenii

(1) Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să colecteze și să mențină date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, cu diligența necesară, în conformitate cu dreptul Uniunii în materie de protecție a datelor cu caracter personal.

(2) În sensul alineatului (1), statele membre solicită ca baza de date cu datele de înregistrare a numelor de domenii să conțină informațiile necesare pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor. Informațiile includ:

(a) numele de domeniu;

(b) data înregistrării;

(c) numele, adresa de e-mail și numărul de telefon de contact ale solicitantului înregistrării;

(d) adresa de e-mail și numărul de telefon de contact ale punctului de contact care administrează numele de domeniu în cazul în care acestea sunt diferite de cele ale solicitantului înregistrării.

(3) Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să dispună de politici și proceduri, inclusiv proceduri de verificare, care să asigure că bazele de date menționate la alineatul (1) conțin informații exacte și complete. Statele membre solicită ca aceste politici și proceduri să fie puse la dispoziția publicului.

(4) Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să pună la dispoziția publicului, fără întârzieri nejustificate după înregistrarea unui nume de domeniu, datele de înregistrare a numelui de domeniu care nu sunt date cu caracter personal.

(5) Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să ofere acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate în mod corespunzător ale solicitanților de acces legitimi, în conformitate cu dreptul Uniunii în materie de protecție a datelor. Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să răspundă fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la primirea cererilor de acces. Statele membre solicită ca politicile și procedurile de divulgare a unor astfel de date să fie puse la dispoziția publicului.

(6) Respectarea obligațiilor prevăzute la alineatele (1)-(5) nu trebuie să ducă la o suprapunere în colectarea datelor de înregistrare a numelor de domenii. În acest scop, statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să coopereze între ele.

CAPITOLUL VI

SCHIMBUL DE INFORMAȚII

Articolul 29

Acorduri privind schimbul de informații în materie de securitate cibernetică

(1) Statele membre se asigură că entitățile care intră în domeniul de aplicare al prezentei directive și, după caz, alte entități care nu intră în domeniul de aplicare al prezentei directive pot face schimb reciproc de informații relevante în materie de securitate cibernetică, pe bază voluntară, inclusiv de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice, în cazul în care un astfel de schimb de informații:

(a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;

(b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre entitățile publice și private în domeniul cercetării amenințărilor cibernetice.

(2) Statele membre se asigură că schimbul de informații are loc în cadrul unor comunități ale entităților esențiale și ale entităților importante și, după caz, ale prestatorilor sau furnizorilor lor de servicii. Un astfel de schimb este pus în aplicare prin acorduri privind schimbul de informații în materie de securitate cibernetică, în considerarea caracterului potențial sensibil al informațiilor partajate.

(3) Statele membre facilitează instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) de la prezentul articol. Astfel de acorduri pot specifica elemente operaționale, inclusiv utilizarea platformelor TIC dedicate și a instrumentelor de automatizare, conținutul și condițiile acordurilor privind schimbul de informații. Atunci când stabilesc detaliile implicării autorităților publice în astfel de acorduri, statele membre pot impune condiții cu privire la informațiile puse la dispoziție de autoritățile competente sau de echipele CSIRT. Statele membre oferă asistență pentru aplicarea unor astfel de acorduri în conformitate cu politicile lor menționate la articolul 7 alineatul (2) litera (h).

(4) Statele membre se asigură că entitățile esențiale și entitățile importante informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2), odată cu încheierea unor astfel de acorduri sau, după caz, cu retragerea din astfel de acorduri, după ce retragerea intră în vigoare.

(5) ENISA oferă asistență pentru instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) prin schimbul de bune practici și oferind orientări.

Articolul 30

Notificarea voluntară a informațiilor relevante

(1) Statele membre se asigură că, pe lângă obligația de notificare prevăzută la articolul 23, notificările pot fi transmise echipelor CSIRT sau, după caz, autorităților competente, în mod voluntar, de către:

(a) entitățile esențiale și entitățile importante, cu privire la incidente, amenințări cibernetice și incidente evitate la limită;

(b) alte entități decât cele menționate la litera (a), indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, cu privire la incidente semnificative, amenințări cibernetice și incidente evitate la limită.

(2) Statele membre prelucrează notificările menționate la alineatul (1) de la prezentul articol în conformitate cu procedura prevăzută la articolul 23. Statele membre pot trata notificările obligatorii cu prioritate față de notificările voluntare.

Dacă este necesar, echipele CSIRT și, după caz, autoritățile competente furnizează punctelor unice de contact informațiile despre notificările primite în temeiul prezentului articol, asigurând totodată confidențialitatea și protecția adecvată a informațiilor furnizate de entitatea notificatoare. Fără a aduce atingere prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, raportarea voluntară nu impune entității notificatoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.

CAPITOLUL VII

SUPRAVEGHEREA ȘI ASIGURAREA RESPECTĂRII LEGII

Articolul 31

Aspecte generale privind supravegherea și asigurarea respectării legii

(1) Statele membre se asigură că autoritățile lor competente supraveghează în mod eficace și iau măsurile necesare pentru a asigura respectarea prezentei directive.

(2) Statele membre pot permite autorităților lor competente să acorde prioritate sarcinilor de supraveghere. O asemenea prioritizare are la bază o abordare bazată pe riscuri. În acest scop, atunci când își exercită sarcinile de supraveghere prevăzute la articolele 32 și 33, autoritățile competente pot stabili metodologii de supraveghere care să permită tratarea cu prioritate a acestor sarcini, urmând o abordare bazată pe riscuri.

(3) Autoritățile competente lucrează în strânsă cooperare cu autoritățile de supraveghere în temeiul Regulamentului (UE) 2016/679 în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, fără a aduce atingere competențelor și sarcinilor autorităților de supraveghere în temeiul regulamentului respectiv.

(4) Fără a aduce atingere cadrelor legislative și instituționale naționale, statele membre se asigură că, în ceea ce privește supravegherea respectării prezentei directive de către entitățile administrației publice și aplicarea de măsuri de asigurare a respectării legii în cazul încălcării prezentei directive, autoritățile competente au competențele corespunzătoare pentru a îndeplini astfel de sarcini cu independență operațională în raport cu entitățile administrației publice care sunt supravegheate. Statele membre pot decide impunerea unor măsuri adecvate, proporționale și efective de supraveghere și de asigurare a respectării legii în ceea ce privește respectivele entități, în conformitate cu cadrele legislative și instituționale naționale.

Articolul 32

Măsurile de supraveghere și de asigurare a respectării legii în ceea ce privește entitățile esențiale

(1) Statele membre se asigură că măsurile de supraveghere sau de asigurare a respectării legii impuse entităților esențiale în ceea ce privește obligațiile prevăzute în prezenta directivă sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.

(2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, au competența de a supune entitățile respective cel puțin:

(a) unor inspecții la fața locului și unei supravegheri *ex situ*, inclusiv unor verificări aleatorii, realizate de profesioniști cu formare corespunzătoare;

(b) unor audituri de securitate periodice și specifice efectuate de un organism independent sau de o autoritate competentă;

(c) unor audituri ad-hoc, inclusiv în cazurile justificate de un incident semnificativ sau de o încălcare a prezentei directive de către entitatea esențială;

(d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, după caz cu cooperarea entității în cauză;

(e) unor cereri de informații necesare pentru a evalua măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate, precum și respectarea obligației de a trimite informații autorităților competente în temeiul articolului 27;

(f) unor cereri de acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor lor de supraveghere;

(g) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și mijloacele de probă care stau la baza acestora.

Auditurile de securitate specifice, menționate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.

Rezultatele oricărui audit de securitate specific se pun la dispoziția autorității competente. Costurile unui astfel de audit de securitate specific efectuat de un organism independent sunt plătite de entitatea auditată, în afara cazurilor justificate corespunzător, atunci când autoritatea competentă decide altfel.

(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (e), (f) sau (g), autoritățile competente precizează scopul solicitării și informațiile solicitate.

(4) Statele membre se asigură că, atunci când își exercită competențele de asigurare a respectării legii în ceea ce privește entitățile esențiale, autoritățile lor competente au competența cel puțin:

(a) de a emite avertismente cu privire la încălcări ale prezentei directive de către entitățile în cauză;

(b) de a adopta instrucțiuni obligatorii, inclusiv în ceea ce privește măsurile necesare pentru a preveni sau remedia un incident, precum și termene-limită pentru punerea în aplicare a acestor măsuri și pentru a raporta cu privire la punerea lor în aplicare, sau un ordin prin care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcările prezentei directive;

(c) de a dispune ca entitățile în cauză să înceteze conduita prin care încalcă prezenta directivă și să se abțină de la repetarea conduitei respective;

(d) de a dispune ca entitățile în cauză să asigure că măsurile lor de gestionare a riscurilor în materie de securitate cibernetică respectă dispozițiile de la articolul 21 sau să îndeplinească obligațiile de raportare prevăzute la articolul 23, într-un anumit mod și într-o anumită perioadă;

(e) de a dispune ca entitățile în cauză să informeze persoanele fizice sau juridice cu privire la care furnizează servicii sau desfășoară activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la caracterul amenințării, precum și cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la amenințarea respectivă;

(f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;

(g) de a desemna un ofițer de monitorizare cu sarcini bine definite pe o perioadă determinată de timp pentru a supraveghea respectarea de către entitățile în cauză a articolelor 21 și 23;

(h) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcări ale prezentei directive;

(i) de a aplica sau a solicita aplicarea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei amenzi administrative în temeiul articolului 34, în plus față de oricare dintre măsurile menționate la literele (a)-(h) de la prezentul alineat.

(5) În cazul în care măsurile de asigurare a respectării legii adoptate în temeiul alineatului (4) literele (a)-(d) și (f) sunt ineficiente, statele membre se asigură că autoritățile lor competente au competența de a stabili un termen în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor sau să respecte cerințele autorităților respective. În cazul în care acțiunea solicitată nu este întreprinsă în termenul stabilit, statele membre se asigură că autoritățile lor competente au competența:

(a) de a suspenda temporar sau de a solicita unui organism de certificare sau de autorizare sau unei instanțe, în conformitate cu dreptul intern, suspendarea temporară a unei certificări sau a unei autorizații privind o parte sau toate serviciile relevante furnizate sau activitățile relevante desfășurate de entitatea esențială;

(b) de a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei interdicții temporare de a exercita funcții de conducere în cadrul entității respective împotriva oricărei persoane fizice care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal în entitatea esențială.

Suspendările sau interdicțiile temporare impuse în temeiul prezentului alineat se aplică numai până în momentul în care entitatea în cauză ia măsurile necesare în vederea remedierii deficiențelor sau a respectării cerințelor impuse de autoritatea competentă pentru care au fost aplicate aceste măsuri de asigurare a respectării legii. Impunerea unor astfel de suspendări sau interdicții temporare face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv dreptul la o cale de atac eficace și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.

Măsurile de asigurare a respectării legii prevăzute la prezentul alineat nu se aplică entităților administrației publice care intră în domeniul de aplicare al prezentei directive.

(6) Statele membre se asigură că orice persoană fizică responsabilă de o entitate esențială sau care acționează în calitate de reprezentant legal al unei entități esențiale pe baza competenței de a o reprezenta, a autorității de a lua decizii în numele acesteia sau a autorității de a exercita controlul asupra acesteia are competența de a se asigura că aceasta respectă prezenta directivă. Statele membre se asigură că aceste persoane fizice pot fi trase la răspundere pentru încălcarea obligațiilor care le revin de a asigura respectarea prezentei directive.

În ceea ce privește entitățile administrației publice, prezentul alineat nu aduce atingere dreptului intern în ceea ce privește răspunderea funcționarilor publici și a funcționarilor aleși sau numiți.

(7) Atunci când iau oricare dintre măsurile de asigurare a respectării legii menționate la alineatul (4) sau (5), autoritățile competente respectă dreptul la apărare, iau în considerare circumstanțele fiecărui caz în parte și țin seama în mod corespunzător cel puțin de:

(a) gravitatea încălcării și importanța dispozițiilor încălcate, următoarele fiind considerate, printre altele, încălcări grave în orice situație:

(i) încălcări repetate;

(ii) o neîndeplinire a obligației de notificare sau de remediere a incidentelor semnificative;

(iii) o neremediere a deficiențelor în urma instrucțiunilor obligatorii din partea autorităților competente;

(iv) obstrucționarea auditurilor sau a activităților de monitorizare dispuse de autoritatea competentă în urma constatării unei încălcări;

(v) furnizarea de informații false sau vădit denaturate în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică sau obligațiile de raportare prevăzute la articolele 21 și 23;

(b) durata încălcării;

(c) orice încălcare anterioară relevantă comisă de entitatea în cauză;

(d) orice prejudicii materiale sau morale cauzate, inclusiv pierderile financiare sau economice, efectele asupra altor servicii și numărul de utilizatori afectați;

(e) orice intenție sau neglijență din partea autorului încălcării;

(f) orice măsuri luate de entitate pentru a preveni sau a atenua prejudiciile materiale sau morale;

(g) orice aderare la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

(h) măsura în care persoanele fizice sau juridice declarate responsabile cooperează cu autoritățile competente.

(8) Autoritățile competente prezintă o motivare detaliată a măsurilor lor de asigurare a respectării legii. Înainte de a adopta astfel de măsuri, autoritățile competente notifică entităților în cauză constatările lor preliminare. De asemenea, acestea acordă entităților respective un termen rezonabil să prezinte observații, cu excepția cazurilor justificate în mod corespunzător, când ar fi împiedicată o acțiune imediată pentru a preveni sau răspunde la incidente.

(9) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează autoritățile competente relevante din același stat membru în temeiul Directivei (UE) 2022/2557 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea de către o entitate identificată ca fiind entitate critică în temeiul Directivei (UE) 2022/2557 a prezentei directive. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 pot solicita autorităților competente în temeiul prezentei directive să își exercite competențele de supraveghere și de asigurare a respectării legii în legătură cu o entitate care este identificată ca fiind entitate critică în temeiul Directivei (UE) 2022/2557.

(10) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive cooperează cu autoritățile competente relevante din statul membru în cauză în temeiul Regulamentului (UE) 2022/2554. În special, statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) 2022/2554 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o entitate esențială, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/2554.

Articolul 33

Măsuri de supraveghere și de asigurare a respectării legii în ceea ce privește entitățile importante

(1) Atunci când li se furnizează dovezi, indicii sau informații că o entitate importantă nu ar respecta prezenta directivă, în special articolele 21 și 23, statele membre se asigură că autoritățile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere ex post. Statele membre se asigură că aceste măsuri sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.

(2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile importante, au competența de a supune entitățile respective cel puțin:

(a) unor inspecții la fața locului și unei supravegheri *ex situ ex post* realizate de profesioniști cu formare corespunzătoare;

(b) unor audituri de securitate specifice efectuate de un organism independent sau de o autoritate competentă;

(c) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, după caz cu cooperarea entității în cauză;

(d) unor cereri de informații necesare pentru a evalua, ex post, măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate, precum și respectarea obligației de a transmite informații autorităților competente în temeiul articolului 27;

(e) unor cereri de acces la date, la documente și la informații necesare pentru îndeplinirea sarcinilor lor de supraveghere;

(f) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și mijloacele de probă care stau la baza acestora.

Auditurile de securitate specifice, menționate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.

Rezultatele oricărui audit de securitate specific se pun la dispoziția autorității competente. Costurile unui astfel de audit de securitate specific efectuat de un organism independent sunt plătite de entitatea auditată, în afara cazurilor justificate corespunzător, atunci când autoritatea competentă decide altfel.

(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (d), (e) sau (f), autoritățile competente precizează scopul solicitării și informațiile solicitate.

(4) Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legii în ceea ce privește entitățile importante, autoritățile competente au competența cel puțin:

(a) de a emite avertismente cu privire la încălcări ale prezentei directive de către entitățile în cauză;

(b) de a adopta instrucțiuni obligatorii sau un ordin prin care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcarea prezentei directive;

(c) de a dispune ca entitățile în cauză să înceteze conduita prin care încalcă prezenta directivă și să se abțină de la repetarea conduitei respective;

(d) de a dispune ca entitățile în cauză să asigure că măsurile lor de gestionare a riscurilor în materie de securitate cibernetică respectă dispozițiile de la articolul 21 sau să îndeplinească obligațiile de raportare prevăzute la articolul 23, într-un anumit mod și într-o anumită perioadă;

(e) de a dispune ca entitățile în cauză să informeze persoanele fizice sau juridice cu privire la care furnizează servicii sau desfășoară activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la caracterul amenințării, precum și cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la amenințarea respectivă;

(f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;

(g) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcările prezentei directive;

(h) de a aplica sau a solicita aplicarea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei amenzi administrative în temeiul articolului 34, în plus față de oricare dintre măsurile menționate la literele (a)-(g) de la prezentul alineat.

(5) Articolul 32 alineatele (6), (7) și (8) se aplică, mutatis mutandis, măsurilor de supraveghere și de asigurare a respectării legii prevăzute în prezentul articol pentru entitățile importante.

(6) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive cooperează cu autoritățile competente relevante din statul membru în cauză în temeiul Regulamentului (UE) 2022/2554. În special, statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) 2022/2554 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o entitate importantă, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/2554.

Articolul 34

Condiții generale pentru aplicarea de amenzi administrative entităților esențiale și entităților importante

(1) Statele membre se asigură că amenzile administrative aplicate entităților esențiale și entităților importante în temeiul prezentului articol în ceea ce privește încălcările prezentei directive sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.

(2) Amenzile administrative sunt aplicate în plus față de oricare dintre măsurile menționate la articolul 32 alineatul (4) literele (a)-(h), la articolul 32 alineatul (5) și la articolul 33 alineatul (4) literele (a)-(g).

(3) Atunci când se ia decizia de a aplica o amendă administrativă și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită cel puțin elementelor prevăzute la articolul 32 alineatul (7).

(4) Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, entitățile esențiale sunt supuse, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puțin 10 000 000 EUR sau o limită superioară de cel puțin 2 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține entitatea esențială, luându-se în considerare valoarea cea mai mare dintre acestea.

(5) Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, entitățile importante sunt supuse, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puțin 7 000 000 EUR sau având o limită superioară de cel puțin 1,4 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține entitatea importantă, luându-se în considerare valoarea cea mai mare dintre acestea.

(6) Statele membre pot prevedea competența de a aplica penalități cu titlu cominatoriu pentru a obliga o entitate esențială sau o entitate importantă să înceteze o încălcare a prezentei directive în conformitate cu o decizie prealabilă a autorității competente.

(7) Fără a aduce atingere competențelor autorităților competente menționate la articolele 32 și 33, fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi aplicate amenzi administrative entităților administrației publice cărora le revin obligațiile prevăzute în prezenta directivă.

(8) În cazul în care sistemul juridic al unui stat membru nu prevede amenzi administrative, statul membru respectiv se asigură că prezentul articol este aplicat astfel încât amenda să fie inițiată de autoritatea competentă și aplicată de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficiente și că au un efect echivalent cu cel al amenzilor administrative aplicate de autoritățile competente. În orice caz, amenzile aplicate sunt efective, proporționale și cu efect de descurajare. Statele membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la 17 octombrie 2024, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.

Articolul 35

Încălcări care implică o încălcare a securității datelor cu caracter personal

(1) În cazul în care, în cursul supravegherii sau al asigurării respectării legii, autoritățile competente iau cunoștință de faptul că încălcarea de către o entitate esențială sau de către o entitate importantă a obligațiilor prevăzute la articolele 21 și 23 din prezenta directivă poate atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) 2016/679, care trebuie notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează fără întârzieri nejustificate autoritățile de supraveghere menționate la articolele 55 sau 56 din regulamentul respectiv.

(2) În cazul în care autoritățile de supraveghere menționate la articolele 55 sau 56 din Regulamentul (UE) 2016/679 aplică o amendă administrativă în temeiul articolului 58 alineatul (2) litera (i) din regulamentul respectiv, autoritățile competente nu aplică o amendă administrativă în conformitate cu articolul 34 din prezenta directivă pentru o încălcare menționată la alineatul (1) din prezentul articol rezultată în urma aceluiași comportament care a făcut obiectul amenzii administrative în temeiul articolului 58 alineatul (2) litera (i) din Regulamentul (UE) 2016/679. Cu toate acestea, autoritățile competente pot aplica măsurile de asigurare a respectării legii prevăzute la articolul 32 alineatul (4) literele (a)-(h), la articolul 32 alineatul (5) și la articolul 33 alineatul (4) literele (a)-(g) din prezenta directivă.

(3) În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este stabilită într-un alt stat membru decât autoritatea competentă, autoritatea competentă informează autoritatea de supraveghere stabilită în statul său membru cu privire la potențiala încălcare a securității datelor menționată la alineatul (1).

Articolul 36

Sancțiuni

Statele membre adoptă normele privind sancțiunile care se aplică în cazul nerespectării măsurilor naționale adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura aplicarea acestora. Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre notifică aceste norme și aceste măsuri Comisiei până la 17 ianuarie 2025 și notifică acesteia, fără întârziere, orice modificare ulterioară a acestora.

Articolul 37

Asistență reciprocă

(1) Dacă o entitate furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar rețeaua și sistemele sale informatice sunt situate în unul sau mai multe alte state membre, autoritățile competente ale statelor membre în cauză cooperează și își oferă asistență reciprocă, după caz. Această cooperare implică cel puțin următoarele:

(a) autoritățile competente care aplică măsuri de supraveghere sau de asigurare a respectării legii într-un stat membru informează și consultă, prin intermediul punctului unic de contact, autoritățile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere și de asigurare a respectării legii luate;

(b) o autoritate competentă poate solicita unei alte autorități competente să ia măsuri de supraveghere sau de asigurare a respectării legii;

(c) la primirea unei cereri motivate din partea altei autorități competente, o autoritate competentă acordă asistență reciprocă celeilalte autorități competente proporțional cu resursele sale, astfel încât măsurile de supraveghere sau de asigurare a respectării legii să poată fi puse în aplicare într-un mod eficace, eficient și consecvent.

Asistența reciprocă menționată la primul paragraf litera (c) poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața locului, a unei supravegheri *ex situ* sau a unor audituri de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu refuză cererea respectivă, cu excepția cazului în care se stabilește că nu are competența de a furniza asistența solicitată, asistența solicitată nu este proporțională cu sarcinile de supraveghere ale autorității competente sau cererea privește informații sau implică activități care, dacă ar fi divulgate sau desfășurate, ar fi contrare intereselor esențiale ale statului membru respectiv în materie de securitate națională, siguranță publică sau apărare. Înainte de a refuza o astfel de cerere, autoritatea competentă consultă celelalte autorități competente în cauză, precum și, la cererea unuia dintre statele membre în cauză, Comisia și ENISA.

(2) Dacă este cazul și de comun acord, autorități competente din diferite state membre pot desfășura acțiuni comune de supraveghere.

CAPITOLUL VIII

ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 38

Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Competența de a adopta acte delegate menționată la articolul 24 alineatul (2) se conferă Comisiei pe o perioadă de cinci ani de la 16 ianuarie 2023.

(3) Delegarea de competențe menționată la articolul 24 alineatul (2) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 24 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu, sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 39

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

(3) În cazul în care avizul comitetului urmează să fie obținut prin procedură scrisă, respectiva procedură se încheie fără rezultat atunci când, în termenul stabilit pentru emiterea avizului, președintele comitetului decide în acest sens sau un membru al comitetului solicită acest lucru.

CAPITOLUL IX

DISPOZIȚII FINALE

Articolul 40

Revizuirea

Până la 17 octombrie 2027 și, ulterior, la fiecare 36 de luni, Comisia revizuiește funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special relevanța dimensiunii entităților vizate și sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. În acest scop și în vederea intensificării cooperării strategice și operaționale, Comisia ține cont de rapoartele Grupului de cooperare și ale rețelei CSIRT privind experiența obținută la nivel strategic și operațional. Raportul este însoțit, după caz, de o propunere legislativă.

Articolul 41

Transpunerea

(1) Până la 17 octombrie 2024, statele membre adoptă și publică măsurile necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta.

Statele membre aplică măsurile respective de la 18 octombrie 2024.

(2) Atunci când statele membre adoptă măsurile menționate la alineatul (1), acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri.

Articolul 42

Modificarea Regulamentului (UE) nr. 910/2014

În Regulamentul (UE) nr. 910/2014, articolul 19 se elimină de la 18 octombrie 2024.

Articolul 43

Modificarea Directivei (UE) 2018/1972

În Directiva (UE) 2018/1972, articolele 40 și 41 se elimină de la 18 octombrie 2024.

Articolul 44

Abrogarea

Directiva (UE) 2016/1148 se abrogă de la 18 octombrie 2024.

Trimiterile la directiva abrogată se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexa III.

Articolul 45

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 46

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Strasbourg, 14 decembrie 2022.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	M. BEK

ANEXA I

SECTOARE CU O IMPORTANȚĂ CRITICĂ RIDICATĂ

Sectorul	Subsectorul	Tipul de entitate
1. Energie	(a) Electricitate	— Întreprinderile din domeniul energiei electrice, astfel cum sunt definite la articolul 2 punctul 57 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului ([1]), care îndeplinesc funcția de „furnizare", astfel cum este definită la articolul 2 punctul 12 din directiva respectivă
		— Operatorii de distribuție, astfel cum sunt definiți la articolul 2 punctul 29 din Directiva (UE) 2019/944
		— Operatorii de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 35 din Directiva (UE) 2019/944
		— Producătorii, astfel cum sunt definiți la articolul 2 punctul 38 din Directiva (UE) 2019/944
		— Operatorii pieței de energie electrică desemnați, astfel cum sunt definiți la articolul 2 punctul 8 din Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului ([2]) — Participanții la piață, astfel cum sunt definiți la articolul 2 punctul 25 din Regulamentul (UE) 2019/943, care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie, astfel cum sunt definite la articolul 2 punctele 18, 20 și 59 din Directiva (UE) 2019/944 — Operatorii unui punct de reîncărcare care sunt responsabili cu gestionarea și exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare utilizatorilor finali, inclusiv în numele și în contul unui furnizor de servicii de mobilitate
	(b) Încălzire centralizată și răcire centralizată	— Operatorii de încălzire centralizată sau răcire centralizată, astfel cum este definită la articolul 2 punctul 19 din Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului ([3])
	(c) Petrol	— Operatorii de conducte de transport al petrolului
		— Operatorii instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport
		— Entitățile centrale de stocare, astfel cum sunt definite la articolul 2 litera (f) din Directiva 2009/119/CE a Consiliului ([4])
	(d) Gaze	— Întreprinderile de furnizare, astfel cum sunt definite la articolul 2 punctul 8 din Directiva 2009/73/CE a Parlamentului European și a Consiliului ([5])
		— Operatorii de distribuție, astfel cum sunt definiți la articolul 2 punctul 6 din Directiva 2009/73/CE
		— Operatorii de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 4 din Directiva 2009/73/CE
		— Operatorii de înmagazinare, astfel cum sunt definiți la articolul 2 punctul 10 din Directiva 2009/73/CE
		— Operatorii de sistem GNL, astfel cum sunt definiți la articolul 2 punctul 12 din Directiva 2009/73/CE
		— Întreprinderile din sectorul gazelor naturale, astfel cum sunt definite la articolul 2 punctul 1 din Directiva 2009/73/CE
		— Operatorii de instalație de rafinare și de tratare a gazelor naturale
	(e) Hidrogen	— Operatorii de producție, stocare și transport de hidrogen

Sectorul	Subsectorul	Tipul de entitate
2. Transport	(a) Transport aerian	— Transportatorii aerieni, astfel cum sunt definiți la articolul 3 punctul 4 din Regulamentul (CE) nr. 300/2008, utilizați în scop comercial
		— Organele de administrare a aeroporturilor, astfel cum sunt definite la articolul 2 punctul 2 din Directiva 2009/12/CE a Parlamentului European și a Consiliului ([6]), aeroporturile, astfel cum sunt definite la articolul 2 punctul 1 din directiva respectivă, inclusiv aeroporturile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului ([7]), precum și entitățile care operează instalații auxiliare în cadrul aeroporturilor
		— Operatorii de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului ([8])
	(b) Transport feroviar	— Administratorii infrastructurii, astfel cum sunt definiți la articolul 3 punctul 2 din Directiva 2012/34/UE a Parlamentului European și a Consiliului ([9])
		— Întreprinderile feroviare, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2012/34/UE, inclusiv operatorii unei infrastructuri de servicii, astfel cum sunt definiți la articolul 3 punctul 12 din directiva respectivă
	(c) Transport pe apă	— Companiile de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului ([10]) fără a include navele individuale operate de companiile respective
		— Organele de gestionare a porturilor, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2005/65/CE a Parlamentului European și a Consiliului ([11]), inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, și entitățile care realizează lucrări și operează echipamente în cadrul porturilor
		— Operatorii de servicii de trafic maritim (STM), astfel cum sunt definiți la articolul 3 litera (o) din Directiva 2002/59/CE a Parlamentului European și a Consiliului ([12])
	(d) Transport rutier	— Autoritățile rutiere, astfel cum sunt definite la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei ([13]) responsabile cu controlul gestionării traficului, cu excepția entităților publice în cazul cărora gestionarea traficului sau exploatarea sistemelor de transport inteligente reprezintă doar o parte neesențială a activității lor generale
		— Operatorii de sisteme de transport inteligente, astfel cum sunt definite la articolul 4 punctul 1 din Directiva 2010/40/UE a Parlamentului European și a Consiliului ([14])
3. Sectorul bancar		Instituțiile de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului ([15])
4. Infrastructuri ale pieței financiare		— Operatorii de locuri de tranzacționare, astfel cum sunt definite la articolul 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European și a Consiliului ([16])
		— Contrapărțile centrale (CPC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului ([17])

Sectorul	Subsectorul	Tipul de entitate
5. Sectorul sănătății		— Furnizorii de servicii medicale, astfel cum sunt definiți la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului ([18])
		— Laboratoarele de referință ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului ([19])
		— Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor, astfel cum sunt definite la articolul 1 punctul 2 din Directiva 2001/83/CE a Parlamentului European și a Consiliului ([20]) — Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în secțiunea C diviziunea 21 din NACE Rev. 2 — Entitățile care fabrică dispozitive medicale considerate a fi esențiale în contextul unei urgențe de sănătate publică (lista dispozitivelor esențiale pentru urgența de sănătate publică) în sensul articolului 22 din Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului ([21])
6. Apă potabilă		Furnizorii și distribuitorii de apă destinată consumului uman, astfel cum este definită la articolul 2 punctul 1 litera (a) din Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului ([22]) excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă o parte neesențială din activitatea lor generală de distribuție a altor produse de bază și bunuri
7. Ape uzate		Întreprinderile care colectează, evacuează sau tratează ape urbane reziduale, ape menajere uzate sau ape industriale uzate, astfel cum sunt definite la articolul 2 punctele 1, 2 și 3 din Directiva 91/271/CEE a Consiliului ([23]) cu excepția întreprinderilor pentru care colectarea, evacuarea sau tratarea apelor urbane reziduale, a apelor menajere uzate sau a apelor industriale uzate reprezintă o parte neesențială a activității lor generale
8. Infrastructură digitală		— Furnizorii de IXP (internet *exchange point*)
		— Furnizorii de servicii DNS, cu excepția operatorilor de servere pentru nume primare
		— Registrele de nume TLD
		— Furnizorii de servicii de *cloud computing*
		— Furnizorii de servicii de centre de date
		— Furnizorii de rețele de furnizare de conținut
		— Furnizorii de servicii de încredere
		— Furnizorii de rețele publice de comunicații electronice –Furnizorii de servicii de comunicații electronice accesibile publicului
		— Furnizorii de IXP (internet *exchange point*)
9. Gestionarea serviciilor TIC (*business-to-business*)		— Furnizorii de servicii gestionate — Furnizorii de servicii de securitate gestionate

Sectorul	Subsectorul	Tipul de entitate
10. Administrație publică		— Entitățile de administrație publică din administrația centrală, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern
		— Entitățile de administrație publică la nivel regional, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern
11. Spațiu		Operatorii de infrastructură terestră deținută, gestionată și operată de statele membre sau de părți private, care sprijină furnizarea de servicii spațiale, cu excepția furnizorilor de rețele publice de comunicații electronice

([1]) Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).
([2]) Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului din 5 iunie 2019 privind piața internă de energie electrică (JO L 158, 14.6.2019, p. 54).
([3]) Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului din 11 decembrie 2018 privind promovarea utilizării energiei din surse regenerabile (JO L 328, 21.12.2018, p. 82).
([4]) Directiva 2009/119/CE a Consiliului din 14 septembrie 2009 privind obligația statelor membre de a menține un nivel minim de rezerve de țiței și/sau de produse petroliere (JO L 265, 9.10.2009, p. 9).
([5]) Directiva 2009/73/CE a Parlamentului European și a Consiliului din 13 iulie 2009 privind normele comune pentru piața internă în sectorul gazelor naturale și de abrogare a Directivei 2003/55/CE (JO L 211, 14.8.2009, p. 94).
([6]) Directiva 2009/12/CE a Parlamentului European și a Consiliului din 11 martie 2009 privind tarifele de aeroport (JO L 70, 14.3.2009, p. 11).
([7]) Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea rețelei transeuropene de transport și de abrogare a Deciziei nr. 661/2010/UE (JO L 348, 20.12.2013, p. 1).
([8]) Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea cerului unic european (regulament-cadru) (JO L 96, 31.3.2004, p. 1).
([9]) Directiva 2012/34/UE a Parlamentului European și a Consiliului din 21 noiembrie 2012 privind instituirea spațiului feroviar unic european (JO L 343, 14.12.2012, p. 32).
([10]) Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare (JO L 129, 29.4.2004, p. 6).
([11]) Directiva 2005/65/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind consolidarea securității portuare (JO L 310, 25.11.2005, p. 28).
([12]) Directiva 2002/59/CE a Parlamentului European și a Consiliului din 27 iunie 2002 de instituire a unui sistem comunitar de monitorizare și informare privind traficul navelor maritime și de abrogare a Directivei 93/75/CEE a Consiliului (JO L 208, 5.8.2002, p. 10).
([13]) Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic (JO L 157, 23.6.2015, p. 21).
([14]) Directiva 2010/40/UE a Parlamentului European și a Consiliului din 7 iulie 2010 privind cadrul pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport (JO L 207, 6.8.2010, p. 1).
([15]) Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).
([16]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).
([17]) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1).
([18]) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

([19]) Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului din 23 noiembrie 2022 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE (JO L 314, 6.12.2022, p. 26).

([20]) Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman (JO L 311, 28.11.2001, p. 67).

([21]) Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului din 25 ianuarie 2022 privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora (JO L 20, 31.1.2022, p. 1).

([22]) Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului din 16 decembrie 2020 privind calitatea apei destinate consumului uman (JO L 435, 23.12.2020, p. 1).

([23]) Directiva 91/271/CEE a Consiliului din 21 mai 1991 privind tratarea apelor urbane reziduale (JO L 135, 30.5.1991, p. 40).

ANEXA II

ALTE SECTOARE DE IMPORTANȚĂ CRITICĂ

Sectorul	Subsectorul	Tipul de entitate
1. Servicii poștale și de curierat		Furnizorii de servicii poștale, astfel cum sunt definiți la articolul 2 punctul 1a din Directiva 97/67/CE, inclusiv furnizori de servicii de curierat
2. Gestionarea deșeurilor		Întreprinderile care efectuează gestionarea deșeurilor, astfel cum este definită la articolul 3 punctul 9 din Directiva 2008/98/CE a Parlamentului European și a Consiliului ([1]), cu excepția întreprinderilor pentru care gestionarea deșeurilor nu reprezintă principala activitate economică
3. Fabricarea, producția și distribuția de substanțe chimice		Întreprinderile care produc substanțe și distribuie substanțe sau amestecuri, astfel cum se menționează la articolul 3 punctele 9 și 14 din Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului ([2]) și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din regulamentul respectiv, din substanțe sau amestecuri
4. Producția, prelucrarea și distribuția de alimente		Întreprinderile care produc substanțe și distribuie substanțe sau amestecuri, astfel cum se menționează la articolul 3 punctele 9 și 14 din Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului ([3]) și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din regulamentul respectiv, din substanțe sau amestecuri
5. Fabricare	(a) Fabricarea de dispozitive medicale și de dispozitive medicale pentru diagnostic in vitro	Entitățile care fabrică dispozitive medicale, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului ([4]), și entități care fabrică dispozitive medicale pentru diagnostic in vitro, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului ([5]), cu excepția entităților care fabrică dispozitive medicale menționate în anexa I punctul 5 a cincea liniuță din prezenta directivă
	(b) (b) Fabricarea computerelor și a produselor electronice și optice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 26 din NACE Rev. 2
	(c) Fabricarea echipamentelor electrice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 27 din NACE Rev. 2
	(d) Fabricarea altor mașini și echipamente n.c.a.	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 28 din NACE Rev. 2
	(e) Fabricarea autovehiculelor, remorcilor și semiremorcilor	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 29 din NACE Rev. 2
	(f) Fabricarea altor echipamente de transport	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 30 din NACE Rev. 2

Sectorul	Subsectorul	Tipul de entitate
6. Furnizori digitali		— Furnizorii de piețe online
		— Furnizorii de motoare de căutare online
		— Furnizorii de platforme de servicii de socializare în rețea
7. Cercetare		Organizațiile de cercetare

([1]) Directiva 2008/98/CE a Parlamentului European și a Consiliului din 19 noiembrie 2008 privind deșeurile și de abrogare a anumitor directive (JO L 312, 22.11.2008, p. 3).

([2]) Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

([3]) Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

([4]) Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1).

([5]) Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

ANEXA III

TABEL DE CORESPONDENȚĂ

Directiva (UE) 2016/1148	Prezenta directivă
Articolul 1 alineatul (1)	Articolul 1 alineatul (1)
Articolul 1 alineatul (2)	Articolul 1 alineatul (2)
Articolul 1 alineatul (3)	-
Articolul 1 alineatul (4)	Articolul 2 alineatul (12)
Articolul 1 alineatul (5)	Articolul 2 alineatul (13)
Articolul 1 alineatul (6)	Articolul 2 alineatele (6) și (11)
Articolul 1 alineatul (7)	Articolul 4
Articolul 2	Articolul 2 alineatul (14)
Articolul 3	Articolul 5
Articolul 4	Articolul 6
Articolul 5	–
Articolul 6	–
Articolul 7 alineatul (1)	Articolul 7 alineatele (1) și (2)
Articolul 7 alineatul (2)	Articolul 7 alineatul (4)
Articolul 7 alineatul (3)	Articolul 7 alineatul (3)
Articolul 8 alineatele (1)-(5)	Articolul 8 alineatele (1)-(5)
Articolul 8 alineatul (6)	Articolul 13 alineatul (4)
Articolul 8 alineatul (7)	Articolul 8 alineatul (6)
Articolul 9 alineatele (1), (2) și (3)	Articolul 10 alineatele (1), (2) și (3)
Articolul 9 alineatul (4)	Articolul 10 alineatul (9)
Articolul 9 alineatul (5)	Articolul 10 alineatul (10)
Articolul 10 alineatele (1), (2) și (3) primul paragraf	Articolul 13 alineatele (1), (2) și (3)
Articolul 10 alineatul (3) al doilea paragraf	Articolul 23 alineatul (9)
Articolul 11 alineatul (1)	Articolul 14 alineatele (1) și (2)
Articolul 11 alineatul (2)	Articolul 14 alineatul (3)
Articolul 11 alineatul (3)	Articolul 14 alineatul (4) primul paragraf literele (a)-(q) și (s), și alineatul (7)
Articolul 11 alineatul (4)	Articolul 14 alineatul (4) primul paragraf litera (r) și al doilea paragraf
Articolul 11 alineatul (5)	Articolul 14 alineatul (8)
Articolul 12 alineatele (1)-(5)	Articolul 15 alineatele (1)-(5)
Articolul 13	Articolul 17
Articolul 14 alineatele (1) și (2)	Articolul 21 alineatele (1)-(4)
Articolul 14 alineatul (3)	Articolul 23 alineatul (1)
Articolul 14 alineatul (4)	Articolul 23 alineatul (3)
Articolul 14 alineatul (5)	Articolul 23 alineatele (5), (6) și (8)

Directiva (UE) 2016/1148	Prezenta directivă
Articolul 14 alineatul (6)	Articolul 23 alineatul (7)
Articolul 14 alineatul (7)	Articolul 23 alineatul (11)
Articolul 15 alineatul (1)	Articolul 31 alineatul (1)
Articolul 15 alineatul (2) primul paragraf litera (a)	Articolul 32 alineatul (2) litera (e)
Articolul 15 alineatul (2) primul paragraf litera (b)	Articolul 32 alineatul (2) litera (g)
Articolul 15 alineatul (2) al doilea paragraf	Articolul 32 alineatul (3)
Articolul 15 alineatul (3)	Articolul 32 alineatul (4) litera (b)
Articolul 15 alineatul (4)	Articolul 31 alineatul (3)
Articolul 16 alineatele (1) și (2)	Articolul 21 alineatele (1)-(4)
Articolul 16 alineatul (3)	Articolul 23 alineatul (1)
Articolul 16 alineatul (4)	Articolul 23 alineatul (3)
Articolul 16 alineatul (5)	–
Articolul 16 alineatul (6)	Articolul 23 alineatul (6)
Articolul 16 alineatul (7)	Articolul 23 alineatul (7)
Articolul 16 alineatele (8) și (9)	Articolul 21 alineatul (5) și articolul 23 alineatul (11)
Articolul 16 alineatul (10)	–
Articolul 16 alineatul (11)	Articolul 2 alineatele (1), (2) și (3)
Articolul 17 alineatul (1)	Articolul 33 alineatul (1)
Articolul 17 alineatul (2) litera (a)	Articolul 32 alineatul (2) litera (e)
Articolul 17 alineatul (2) litera (b)	Articolul 32 alineatul (4) litera (b)
Articolul 17 alineatul (3)	Articolul 37 alineatul (1) literele (a) și (b)
Articolul 18 alineatul (1)	Articolul 26 alineatul (1) litera (b) și alineatul (2)
Articolul 18 alineatul (2)	Articolul 26 alineatul (3)
Articolul 18 alineatul (3)	Articolul 26 alineatul (4)
Articolul 19	Articolul 25
Articolul 20	Articolul 30
Articolul 21	Articolul 36
Articolul 22	Articolul 39
Articolul 23	Articolul 40
Articolul 24	–
Articolul 25	Articolul 41
Articolul 26	Articolul 45
Articolul 27	Articolul 46
Anexa I, punctul 1	Articolul 11 alineatul (1)
Anexa I, punctul 2 litera (a) punctele (i)-(iv)	Articolul 11 alineatul (2) literele (a)-(d)

Directiva (UE) 2016/1148	Prezenta directivă
Anexa I, punctul 2 litera (a) punctul (v)	Articolul 11 alineatul (2) litera (f)
Anexa I, punctul 2 litera (b)	Articolul 11 alineatul (4)
Anexa I, punctul 2 litera (c) punctele (i) și (ii)	Articolul 11 alineatul (5) litera (a)
Anexa II	Anexa I
Anexa III, punctele 1 și 2	Anexa II, punctul 6
Anexa III, punctul 3	Anexa I, punctul 8

DIRECTIVA (UE) 2022/2556 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 14 decembrie 2022

de modificare a Directivelor 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341 privind reziliența operațională digitală pentru sectorul financiar

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 53 alineatul (1) și articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Băncii Centrale Europene ([1]),

având în vedere avizul Comitetului Economic și Social European ([2]),

hotărând în conformitate cu procedura legislativă ordinară ([3]),

întrucât:

(1) Uniunea trebuie să abordeze în mod adecvat și cuprinzător riscurile digitale pentru toate entitățile financiare care rezultă dintr-o utilizare sporită a tehnologiei informației și comunicațiilor (TIC) în furnizarea și consumul de servicii financiare, contribuind astfel la realizarea potențialului finanțelor digitale în ceea ce privește stimularea inovării și promovarea concurenței într-un mediu digital sigur.

(2) Entitățile financiare depind în mare măsură de utilizarea tehnologiilor digitale în activitatea lor de zi cu zi. Prin urmare, este extrem de important să se asigure reziliența operațională a operațiunilor lor digitale împotriva riscurilor TIC. Această necesitate a devenit și mai stringentă ca urmare a creșterii tehnologiilor inovatoare de pe piață, în special a tehnologiilor care permit transferul și stocarea electronică a reprezentărilor digitale ale valorii sau ale drepturilor, utilizând un registru distribuit sau o tehnologie similară (criptoactive), și a serviciilor asociate acestor active.

([1]) JO C 343, 26.8.2021, p. 1.
([2]) JO C 155, 30.4.2021, p. 38.
([3]) Poziția Parlamentului European din 10 noiembrie 2022 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 28 noiembrie 2022.

(3) La nivelul Uniunii, cerințele privind gestionarea riscurilor TIC pentru sectorul financiar sunt prevăzute în prezent în Directivele 2009/65/CE ([4]), 2009/138/CE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) și (UE) 2016/2341 ([11]) ale Parlamentului European și ale Consiliului.

Respectivele cerințe sunt diverse și, uneori, incomplete. În unele cazuri, riscurile TIC au fost abordate doar în mod implicit ca parte a riscurilor operaționale, în timp ce în alte cazuri nu au fost abordate deloc. Aceste aspecte ar trebui să fie remediate prin adoptarea Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului ([12]). Prin urmare, respectivele directive ar trebui să fie modificate, pentru a se asigura consecvența cu respectivul regulament. Prezenta directivă conține un set de modificări care sunt necesare pentru a asigura claritatea și consecvența juridică în ceea ce privește diferitele cerințe în materie de reziliență operațională digitală pe care entitățile financiare autorizate și supravegheate le aplică în conformitate cu directivele respective și care sunt necesare pentru exercitarea activităților lor și în furnizarea de servicii, garantând astfel buna funcționare a pieței interne. Este necesar să se asigure caracterul adecvat al cerințelor respective în raport cu evoluțiile pieței, încurajând în același timp proporționalitatea, în special în ceea ce privește dimensiunea entităților financiare și regimurile specifice care se aplică acestora, cu scopul de a reduce costurile de conformitate.

(4) În domeniul serviciilor bancare, Directiva 2013/36/UE stabilește în prezent doar norme generale de guvernanță internă și dispoziții privind riscurile operaționale care conțin cerințe referitoare la planurile de intervenție și de continuitate a activității care servesc în mod implicit drept bază pentru abordarea riscurilor TIC. Cu toate acestea, pentru a aborda riscurile TIC în mod explicit și clar, cerințele privind planurile de intervenție și de continuitate a activității ar trebui să fie modificate pentru a include și planuri de continuitate a activității, precum și planuri de răspuns și de recuperare referitoare la riscurile TIC, în conformitate cu cerințele stabilite în Regulamentul (UE) 2022/2554. În plus, riscurile TIC sunt incluse doar implicit, ca parte a riscurilor operaționale, în procesul de supraveghere și evaluare (SREP), efectuat de autoritățile competente, iar criteriile de evaluare a acestora sunt definite în prezent în Ghidul privind evaluarea riscurilor asociate TIC în cadrul procesului de supraveghere și evaluare (SREP), publicat de Autoritatea europeană de supraveghere (Autoritatea Bancară Europeană,ABE), instituită prin Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([13]). Pentru a asigura claritate juridică

([4]) Directiva 2009/65/CE a Parlamentului European și a Consiliului din 13 iulie 2009 de coordonare a actelor cu putere de lege și a actelor administrative privind organismele de plasament colectiv în valori mobiliare (OPCVM) (JO L 302, 17.11.2009, p. 32).

([5]) Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 335, 17.12.2009, p. 1).

([6]) Directiva 2011/61/UE a Parlamentului European și a Consiliului din 8 iunie 2011 privind administratorii fondurilor de investiții alternative și de modificare a Directivelor 2003/41/CE și 2009/65/CE și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 1095/2010 (JO L 174, 1.7.2011, p. 1).

([7]) Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

([8]) Directiva 2014/59/UE a Parlamentului European și a Consiliului din 15 mai 2014 de instituire a unui cadru pentru redresarea și rezoluția instituțiilor de credit și a firmelor de investiții și de modificare a Directivei 82/891/CEE a Consiliului și a Directivelor 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE și 2013/36/UE ale Parlamentului European și ale Consiliului, precum și a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 648/2012 ale Parlamentului European și ale Consiliului (JO L 173, 12.6.2014, p. 190).

([9]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).

([10]) Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE (JO L 337, 23.12.2015, p. 35).

([11]) Directiva (UE) 2016/2341 a Parlamentului European și a Consiliului din 14 decembrie 2016 privind activitățile și supravegherea instituțiilor pentru furnizarea de pensii ocupaționale (IORP) (JO L 354, 23.12.2016, p. 37).

([12]) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (a se vedea pagina 1 din prezentul Jurnal Oficial).

([13]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Bancară Europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12).

și faptul că autoritățile de supraveghere bancară identifică în mod eficace riscurile TIC și monitorizează gestionarea acestora de către entitățile financiare în conformitate cu noul cadru privind reziliența operațională digitală, domeniul de aplicare al SREP ar trebui să fie de asemenea modificat pentru a trimite explicit la cerințele din Regulamentul (UE) 2022/2554 și pentru a acoperi în special riscurile evidențiate de rapoartele privind incidentele majore legate de TIC și de rezultatele testelor de reziliență operațională digitală efectuate de entități financiare în conformitate cu regulamentul menționat.

(5) Reziliența operațională digitală este esențială pentru menținerea funcțiilor critice și a liniilor de activitate esențiale ale unei entități financiare în caz de rezoluție, evitându-se astfel perturbarea economiei reale și a sistemului financiar. Incidentele operaționale majore pot afecta capacitatea unei entități financiare de a continua să funcționeze și pot pune în pericol obiectivele de rezoluție. Anumite acorduri contractuale privind utilizarea serviciilor TIC sunt esențiale pentru a asigura continuitatea operațională și pentru a furniza datele necesare în caz de rezoluție. Pentru a se alinia la obiectivele cadrului Uniunii pentru reziliența operațională, Directiva 2014/59/UE ar trebui modificată în consecință pentru a garanta că informațiile privind reziliența operațională sunt luate în considerare în contextul planificării rezoluției și al evaluării posibilității de rezoluție a entităților financiare.

(6) Directiva 2014/65/UE stabilește norme mai stricte în materie de riscuri TIC pentru firmele de investiții și locurile de tranzacționare care sunt implicate în tranzacționări algoritmice. În cazul serviciilor de raportare a datelor și al registrelor centrale de tranzacții se aplică cerințe mai puțin detaliate. De asemenea, Directiva 2014/65/UE conține doar trimiteri limitate la măsurile de control și de protecție pentru sistemele de prelucrare a informațiilor și la utilizarea unor sisteme, resurse și proceduri adecvate pentru a asigura continuitatea și regularitatea serviciilor destinate întreprinderilor. În plus, directiva respectivă ar trebui aliniată cu Regulamentul (UE) 2022/2554 în ceea ce privește continuitatea și regularitatea furnizării serviciilor de investiții și în desfășurarea activităților de investiții, reziliența operațională, capacitatea sistemelor de tranzacționare și eficacitatea mecanismelor de asigurare a continuității activității și a gestionării riscurilor.

(7) Directiva (UE) 2015/2366 stabilește norme specifice privind controalele de securitate și elementele de atenuare a riscurilor TIC în scopul obținerii unei autorizări pentru prestarea de servicii de plată. Respectivele norme de autorizare ar trebui să fie modificate în vederea alinierii lor la Regulamentul (UE) 2022/2554. În plus, pentru a reduce sarcina administrativă și pentru a evita complexitatea și suprapunerea cerințelor de raportare, normele privind raportarea incidentelor prevăzute în directiva respectivă ar trebui să înceteze să se aplice prestatorilor de servicii de plată care sunt reglementați în temeiul directivei respective și care fac simultan obiectul Regulamentului (UE) 2022/2554, pentru a permite respectivilor prestatori de servicii de plată să beneficieze de un mecanism unic, pe deplin armonizat de raportare a incidentelor în ceea ce privește toate incidentele operaționale sau de securitate legate de plăți, indiferent dacă astfel de incidente sunt legate de TIC sau nu.

(8) Directiva 2009/138/CE și Directiva (UE) 2016/2341 acoperă parțial riscurile TIC în cadrul dispozițiilor lor generale privind guvernanța și gestionarea riscurilor, urmând ca anumite cerințe să fie precizate prin acte delegate, cu sau fără trimiteri specifice la riscurile TIC. În mod similar, administratorilor de fonduri de investiții alternative care fac obiectul Directivei 2011/61/UE și societăților de administrare care fac obiectul Directivei 2009/65/CE li se aplică doar norme foarte generale. Prin urmare, directivele menționate ar trebui să fie aliniate cu cerințele prevăzute în Regulamentul (UE) 2022/2554 în ceea ce privește gestionarea sistemelor și a instrumentelor TIC.

(9) În multe cazuri, cerințe suplimentare privind riscurile TIC au fost deja stabilite în acte delegate și de punere în aplicare, adoptate pe baza proiectelor de standarde tehnice de reglementare și pe baza proiectelor de standarde tehnice de punere în aplicare elaborate de către autoritatea europeană de supraveghere competentă. Întrucât dispozițiile Regulamentului (UE) 2022/2554 constituie, de acum înainte, cadrul juridic privind riscurile TIC în sectorul financiar, anumite delegări de competențe pentru adoptarea actelor delegate și a actelor de punere în aplicare prevăzute în Directivele 2009/65/CE, 2009/138/CE, 2011/61/UE și 2014/65/UE ar trebui să fie modificate pentru a elimina dispozițiile privind riscurile TIC din domeniul de aplicare al respectivelor delegări de competențe.

(10) Pentru a se asigura o punere în aplicare coerentă a noului cadru privind reziliența operațională digitală pentru sectorul financiar, statele membre ar trebui să aplice dispozițiile de drept intern care transpun prezenta directivă de la data aplicării Regulamentului (UE) 2022/2554.

(11) Directivele 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341 au fost adoptate în temeiul articolului 53 alineatul (1) sau al articolului 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), sau al ambelor articole. Modificările din prezenta directivă au fost incluse într-un act legislativ unic, având în vedere interconectarea dintre obiectul și obiectivele modificărilor. Prin urmare, prezenta directivă ar trebui să fie adoptată atât în temeiul articolului 53 alineatul (1), cât și al articolului 114 din TFUE.

(12) Întrucât obiectivele prezentei directive nu pot fi realizate în mod satisfăcător de către statele membre, deoarece presupun armonizarea cerințelor deja cuprinse în directive, dar, având în vedere amploarea și efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea obiectivelor respective.

(13) În conformitate cu Declarația politică comună din 28 septembrie 2011 a statelor membre și a Comisiei privind documentele explicative ([14]), statele membre s-au angajat ca, în cazuri justificate, să transmită alături de notificarea măsurilor lor de transpunere și unul sau mai multe documente care să explice relația dintre componentele unei directive și părțile corespunzătoare din instrumentele naționale de transpunere. În ceea ce privește prezenta directivă, legiuitorul consideră că este justificată transmiterea unor astfel de documente,

ADOPTĂ PREZENTA DIRECTIVĂ:

Articolul 1

Modificări ale Directivei 2009/65/CE

Articolul 12 din Directiva 2009/65/CE se modifică după cum urmează:

1. La alineatul (1) al doilea paragraf, litera (a) se înlocuiește cu următorul text:

„(a) să aibă o bună organizare administrativă și contabilă, dispozitive de control și de securitate în domeniul prelucrării electronice a datelor, inclusiv cu privire la rețele și sisteme informatice instituite și gestionate în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*), precum și mecanisme adecvate de control intern, incluzând, în special, norme privind tranzacțiile personale ale angajaților săi sau privind deținerea ori administrarea investițiilor în instrumente financiare cu scopul de a investi pe cont propriu și garantând, cel puțin, că fiecare tranzacție în care este implicat OPCVM-ul poate fi reconstituită în ceea ce privește originea sa, părțile la ea, natura sa, precum și momentul și locul în care a fost efectuată și că activele OPCVM-ului administrate de societatea de administrare sunt investite în conformitate cu regulile fondului sau în conformitate cu actele constitutive și dispozițiile legale în vigoare;

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

2. Alineatul (3) se înlocuiește cu următorul text:

„(3) Fără a aduce atingere articolului 116, Comisia adoptă, prin intermediul actelor delegate în conformitate cu articolul 112a, măsuri în care precizează:

(a) procedurile și mecanismele menționate la alineatul (1) al doilea paragraf litera (a), altele decât procedurile și dispozitivele pentru rețelele și sistemele informatice;

(b) structurile și cerințele organizatorice pentru reducerea la minimum a conflictelor de interese menționate la alineatul (1) al doilea paragraf litera (b).”

([14]) JO C 369, 17.12.2011, p. 14.

Articolul 2

Modificări ale Directivei 2009/138/CE

Directiva 2009/138/CE se modifică după cum urmează:

1. La articolul 41, alineatul (4) se înlocuiește cu următorul text:

„(4) Întreprinderile de asigurare și de reasigurare adoptă măsuri rezonabile pentru a asigura continuitatea și regularitatea în desfășurarea activităților lor, inclusiv prin elaborarea unor planuri pentru situații neprevăzute. În acest scop, întreprinderile utilizează sisteme, resurse și proceduri adecvate și proporționale și, în special, instituie și gestionează rețele și sisteme informatice în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

2. La articolul 50 alineatul (1), literele (a) și (b) se înlocuiesc cu următorul text:

„(a) elementele sistemelor prevăzute la articolul 41, articolul 44, în special domeniile enumerate la articolul 44 alineatul (2), precum și articolele 46 și 47, altele decât elementele privind gestionarea riscurilor asociate tehnologiei informației și comunicațiilor;

(b) funcțiile prevăzute la articolele 44, 46, 47 și 48, altele decât funcțiile legate de gestionarea riscurilor asociate tehnologiei informației și comunicațiilor.”

Articolul 3

Modificarea Directivei 2011/61/UE

Articolul 18 din Directiva 2011/61/UE se înlocuiește cu următorul text:

„*Articolul 18*

Principii generale

(1) Statele membre solicită ca AFIA să utilizeze în orice moment resursele umane și tehnice adecvate și corespunzătoare necesare pentru buna administrare a FIA.

Autoritățile competente din statul membru de origine al AFIA, ținând seama, de asemenea, de natura FIA administrat de AFIA, solicită în special ca AFIA să aibă proceduri administrative și contabile solide și dispozitive de control și de protecție pentru prelucrarea electronică a datelor, inclusiv cu privire la rețele și sisteme informatice instituite și gestionate în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*), precum și mecanisme adecvate de control intern, incluzând, în special, norme privind tranzacțiile personale ale angajaților săi sau privind deținerea ori administrarea investițiilor cu scopul de a investi pe cont propriu și garantând, cel puțin, că fiecare tranzacție în care sunt implicate FIA poate fi reconstituită în ceea ce privește originea sa, părțile la aceasta, natura sa, precum și momentul și locul în care a fost efectuată și că activele FIA administrate de AFIA sunt investite în conformitate cu regulile sau actul constitutiv ale FIA și dispozițiile legale în vigoare.

(2) Comisia adoptă prin intermediul unor acte delegate, în conformitate cu articolul 56 și în condițiile prevăzute la articolele 57 și 58, măsuri care stabilesc procedurile și dispozitivele menționate la alineatul (1) de la prezentul articol, altele decât procedurile și dispozitivele pentru rețelele și sistemele informatice.

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

Articolul 4

Modificări ale Directivei 2013/36/UE

Directiva 2013/36/UE se modifică după cum urmează:

1. La articolul 65 alineatul (3) litera (a), punctul (vi) se înlocuiește cu următorul text:

„(vi) părți terțe către care entitățile menționate la punctele (i)-(iv) au externalizat anumite funcții sau activități, inclusiv furnizorii terți de servicii TIC menționați la capitolul V din Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*);

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1)."

2. La articolul 74 alineatul (1), primul paragraf se înlocuiește cu următorul text:

„Instituțiile dispun de un cadru solid de administrare a activității, care include o structură organizatorică clară cu linii de responsabilitate bine definite, transparente și coerente, procese eficace de identificare, administrare, monitorizare și raportare a riscurilor la care sunt sau pot fi expuse, mecanisme adecvate de control intern, inclusiv proceduri administrative și contabile riguroase, rețele și sisteme informatice instituite și gestionate în conformitate cu Regulamentul (UE) 2022/2554, precum și politici și practici de remunerare care să promoveze și să fie în concordanță cu o administrare sănătoasă și eficace a riscurilor."

3. La articolul 85, alineatul (2) se înlocuiește cu următorul text:

„(2) Autoritățile competente se asigură că instituțiile dispun de politici și planuri adecvate de intervenție și de continuitate a activității, inclusiv de politici și planuri de continuitate a activității TIC și de planuri de răspuns și de recuperare în domeniul TIC pentru tehnologia pe care o utilizează pentru comunicarea informațiilor și că aceste planuri sunt elaborate, gestionate și testate în conformitate cu articolul 11 din Regulamentul (UE) 2022/2554, pentru a le permite instituțiilor să își continue activitatea în caz de întrerupere gravă a activității și să limiteze pierderile suportate ca urmare a unei astfel de întreruperi."

4. La articolul 97 alineatul (1), se adaugă următoarea literă:

„(d) riscurile evidențiate de testarea rezilienței operaționale digitale în conformitate cu capitolul IV din Regulamentul (UE) 2022/2554."

Articolul 5

Modificări ale Directivei 2014/59/UE

Directiva 2014/59/UE se modifică după cum urmează:

1. Articolul 10 se modifică după cum urmează:

(a) la alineatul (7), litera (c) se înlocuiește cu următorul text:

„(c) o demonstrație a modului în care funcțiile critice și liniile de activitate esențiale ar putea fi separate din punct de vedere juridic și economic, în măsura necesară, de alte funcții în vederea asigurării continuității și a rezilienței operaționale digitale în cazul intrării în dificultate a instituției;";

(b) la alineatul (7), litera (q) se înlocuiește cu următorul text:

„(q) o descriere a operațiunilor și a sistemelor esențiale pentru a menține funcționarea continuă a proceselor operaționale ale instituției, inclusiv a rețelelor și sistemelor informatice menționate în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*);

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).";

(c) la alineatul (9), se adaugă următorul paragraf:

„În conformitate cu articolul 10 din Regulamentul (UE) nr. 1093/2010, ABE examinează și, după caz, actualizează standardele tehnice de reglementare în scopul, printre altele, de a ține seama de dispozițiile capitolului II din Regulamentul (UE) 2022/2554."

2. Anexa se modifică după cum urmează:

(a) în secțiunea A, punctul 16 se înlocuiește cu următorul text:

„16. aranjamentele și măsurile necesare pentru a menține funcționarea continuă a proceselor operaționale ale instituției, inclusiv rețelele și sistemele informatice instituite și gestionate în conformitate cu Regulamentul (UE) 2022/2554;";

(b) secțiunea B se modifică după cum urmează:

(i) punctul 14 se înlocuiește cu următorul text:

„14. identificarea proprietarilor sistemelor identificate la punctul 13, a acordurilor privind furnizarea serviciilor legate de acestea, precum și a oricăror programe informatice și sisteme sau licențe, inclusiv stabilirea de corespondențe cu persoanele juridice, operațiunile critice și liniile de activitate esențiale ale instituției, precum și o identificare a furnizorilor terți esențiali de servicii TIC, astfel cum sunt definiți la articolul 3 punctul (23) din Regulamentul (UE) 2022/2554;";

(ii) se introduce următorul punct:

„14a. rezultatele testării rezilienței operaționale digitale a instituțiilor în temeiul Regulamentului (UE) 2022/2554;";

(c) secțiunea C se modifică după cum urmează:

(i) punctul 4 se înlocuiește cu următorul text:

„4. măsura în care acordurile de servicii ale instituției, inclusiv acorduri contractuale privind utilizarea serviciilor TIC, sunt robuste și integral executabile în eventualitatea unei rezoluții a instituției;";

(ii) se introduce următorul punct:

„4a. reziliența operațională digitală a rețelelor și sistemelor informatice care sprijină funcțiile critice și liniile de activitate esențiale ale instituției, ținând seama de rapoartele privind incidentele majore legate de TIC și de rezultatele testării rezilienței operaționale digitale în temeiul Regulamentului (UE) 2022/2554;".

Articolul 6

Modificări ale Directivei 2014/65/UE

Directiva 2014/65/UE se modifică după cum urmează:

1. Articolul 16 se modifică după cum urmează:

(a) alineatul (4) se înlocuiește cu următorul text:

„(4) O firmă de investiții adoptă măsuri rezonabile pentru a garanta continuitatea și regularitatea în furnizarea serviciilor de investiții și în exercitarea activităților de investiții. În acest scop, ea utilizează sisteme adecvate și proporționate, inclusiv sisteme de tehnologie a informației și comunicațiilor (TIC) care sunt instituite și gestionate în conformitate cu articolul 7 din Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*), precum și resurse și proceduri adecvate și proporționate.

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).";

(b) la alineatul (5), al doilea și al treilea paragraf se înlocuiesc cu următorul text:

„O firmă de investiții dispune de proceduri contabile și administrative sigure, de mecanisme de control intern și de proceduri eficace de evaluare a riscurilor.

Fără a aduce atingere capacității autorităților competente de a cere accesul la comunicările realizate conform prezentei directive și Regulamentului (UE) nr. 600/2014, o firmă de investiții instituie mecanisme de securitate solide destinate să asigure, în conformitate cu cerințele prevăzute în Regulamentul (UE) 2022/2554, securitatea și autentificarea mijloacelor de transmitere a informațiilor, să reducă la minimum riscul de corupere a datelor și de acces neautorizat și să prevină scurgerile de informații, menținând astfel în permanență confidențialitatea datelor."

2. Articolul 17 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) O firmă de investiții care utilizează tranzacționarea algoritmică dispune de sisteme eficace și de mecanisme de control al riscului adecvate activităților pe care le desfășoară pentru a avea garanția că sistemele sale de tranzacționare sunt reziliente, au capacitate suficientă, în conformitate cu cerințele prevăzute în capitolul II din Regulamentul (UE) 2022/2554, și funcționează pe baza unor praguri și limite adecvate pentru a preveni transmiterea unor ordine eronate sau o funcționare necorespunzătoare a sistemelor care poate genera perturbații ale pieței sau poate contribui la apariția acestora.

O astfel de societate trebuie, de asemenea, să dispună de sisteme eficace și de mecanisme de control al riscului pentru a garanta că sistemele de tranzacționare nu pot fi utilizate în scopuri care contravin Regulamentului (UE) nr. 596/2014 sau regulilor locului de tranzacționare la care este conectată firma respectivă.

Firma de investiții dispune de mecanisme eficace de asigurare a continuității activităților pentru a putea face față oricărei disfuncții a sistemului său de tranzacționare, inclusiv de o politică și planuri de continuitate a activității TIC și de planuri de răspuns și de recuperare în domeniul TIC pentru tehnologia informației și comunicațiilor elaborate în conformitate cu articolul 11 din Regulamentul (UE) 2022/2554, și se asigură că sistemele sale sunt suficient testate și monitorizate corespunzător pentru a răspunde cerințelor generale prevăzute la prezentul alineat și oricăror cerințe specifice prevăzute în capitolele II și IV din Regulamentul (UE) 2022/2554.";

(b) la alineatul (7), litera (a) se înlocuiește cu următorul text:

„(a) detaliile privind cerințele organizatorice detaliate prevăzute la alineatele (1)-(6), altele decât cele legate de gestionarea riscurilor TIC, care trebuie impuse firmelor de investiții ce oferă diferite servicii de investiții, activități de investiții, servicii auxiliare sau o combinație a acestora, atunci când specificațiile referitoare la cerințele organizaționale menționate la alineatul (5) stabilesc cerințele specifice privind accesul direct la piață și privind accesul sponsorizat într-un mod care să garanteze că controalele aplicate accesului sponsorizat sunt cel puțin echivalente cu cele aplicate accesului direct la piață;".

3. La articolul 47, alineatul (1) se modifică după cum urmează:

(a) litera (b) se înlocuiește cu următorul text:

„(b) să fie dotată în mod corespunzător pentru gestionarea riscurilor la care este expusă, inclusiv pentru gestionarea riscurilor TIC în conformitate cu capitolul II din Regulamentul (UE) 2022/2554, să instituie măsuri și sisteme adecvate pentru identificarea riscurilor semnificative care îi pot compromite funcționarea și să aplice măsuri eficace de diminuare a riscurilor respective;";

(b) litera (c) se elimină.

4. Articolul 48 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Statele membre impun ca o piață reglementată să își construiască și să mențină reziliența operațională în conformitate cu cerințele stabilite în Capitolul II din Regulamentul (UE) 2022/2554 pentru ca sistemele sale de tranzacționare să fie reziliente, să aibă capacitate suficientă pentru a face față volumului maxim de ordine și de mesaje, să poată asigura o tranzacționare ordonată în condiții de tensiuni majore pe piață, să fie pe deplin testate pentru a asigura întrunirea acestor condiții și să facă obiectul unor măsuri eficace de asigurare a continuității activității, care să cuprindă o politică și planuri de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu articolul 11 din Regulamentul (UE) 2022/2554, pentru a asigura continuitatea serviciilor în cazul în care survine o defecțiune a sistemelor sale de tranzacționare.";

(b) alineatul (6) se înlocuiește cu următorul text:

„(6) Statele membre impun ca o piață reglementată să aibă instituite sisteme, proceduri și mecanisme eficace, inclusiv o cerință pentru membri sau participanți de a realiza teste adecvate ale algoritmilor și asigurarea cadrului pentru facilitarea acestor teste, în conformitate cu cerințele stabilite în capitolele II și IV din Regulamentul (UE) 2022/2554, pentru a se asigura că sistemele de tranzacționare algoritmică nu pot crea sau contribui la condiții de tranzacționare de natură să perturbe stabilitatea pieței și pentru a gestiona orice condiții de tranzacționare de natură să perturbe stabilitatea pieței care sunt generate de astfel de sisteme de tranzacționare algoritmică, inclusiv sisteme de limitare a raportului ordinelor neexecutate față de tranzacțiile care pot fi introduse în sistem de un membru sau de un participant, pentru a putea încetini fluxul ordinelor dacă există riscul de atingere a capacității maxime a sistemului său și pentru a limita și a impune pasul de cotare minim care poate fi executat pe piață.”;

(c) alineatul (12) se modifică după cum urmează:

(i) litera (a) se înlocuiește cu următorul text:

„(a) cerințele pentru a asigura faptul că sistemele de tranzacționare ale piețelor reglementate sunt reziliente și au o capacitate adecvată, cu excepția cerințelor legate de reziliența operațională digitală;”;

(ii) litera (g) se înlocuiește cu următorul text:

„(g) cerințele pentru a asigura testarea adecvată a algoritmilor, exceptând testarea rezilienței operaționale digitale, cu scopul de a garanta că sistemele de tranzacționare algoritmică sau de tranzacționare algoritmică de mare frecvență nu pot crea sau nu pot contribui la crearea unor condiții de tranzacționare de natură să perturbe stabilitatea pieței.”

Articolul 7

Modificări ale Directivei (UE) 2015/2366

Directiva (UE) 2015/2366 se modifică după cum urmează:

1. La articolul 3, litera (j) se înlocuiește cu următorul text:

„(j) serviciilor prestate de prestatorii de servicii tehnice, care contribuie la prestarea de servicii de plată, fără ca aceștia să intre în vreun moment în posesia fondurilor de transferat, inclusiv în domeniul procesării și stocării datelor, al serviciilor de încredere și de protecție a vieții private, al autentificării datelor și a entităților, al tehnologiei informației și comunicațiilor (TIC) și al furnizării de rețele de comunicații, al furnizării și întreținerii terminalelor și dispozitivelor folosite pentru serviciile de plată, cu excepția serviciilor de inițiere a plății și a serviciilor de informare cu privire la conturi;”.

2. Articolul 5 alineatul (1) se modifică după cum urmează:

(a) primul paragraf se modifică după cum urmează:

(i) litera (e) se înlocuiește cu următorul text:

„(e) o descriere a sistemului de conducere a solicitantului și a mecanismelor de control intern, inclusiv a procedurilor administrative, de gestionare a riscurilor și a procedurilor contabile, precum și a modalităților de utilizare a serviciilor TIC în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*), care să demonstreze că sistemele de conducere și mecanismele de control intern respective sunt proporționale, justificate, valide și adecvate;

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”;

(ii) litera (f) se înlocuiește cu următorul text:

„(f) o descriere a procedurilor existente pentru monitorizarea, tratarea și urmărirea unui incident de securitate și a plângerilor legate de securitate formulate de clienți, incluzând un mecanism de raportare a incidentelor care ține cont de obligațiile de notificare ale instituției de plată prevăzute la capitolul III din Regulamentul (UE) 2022/2554;”;

(iii) litera (h) se înlocuiește cu următorul text:

„(h) o descriere a măsurilor de asigurare a continuității activității, care să cuprindă o identificare clară a operațiunilor critice, o politică și planuri eficace de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC, precum și o procedură pentru testarea și reexaminarea periodică a caracterului adecvat și a eficienței acestor planuri în conformitate cu Regulamentul (UE) 2022/2554;";

(b) al treilea paragraf se înlocuiește cu următorul text:

„Măsurile de control al securității și de atenuare a riscurilor menționate la litera (j) de la primul paragraf trebuie să precizeze modul în care asigură un nivel ridicat de reziliență operațională digitală în conformitate cu capitolul II din Regulamentul (UE) 2022/2554, în special cu privire la securitatea tehnică și protecția datelor, inclusiv în ceea ce privește software-ul și sistemele TIC utilizate de solicitant sau de întreprinderile cărora le externalizează toate operațiunile sale sau o parte din acestea. Printre măsurile respective se numără, de asemenea, măsurile de securitate prevăzute la articolul 95 alineatul (1) din prezenta directivă. Măsurile respective țin seama de orientările ABE privind măsurile de securitate menționate la articolul 95 alineatul (3) din prezenta directivă odată ce acestea sunt adoptate."

3. La articolul 19 alineatul (6), al doilea paragraf se înlocuiește cu următorul text:

„Externalizarea funcțiilor operaționale importante, inclusiv sistemele TIC, nu poate fi realizată într-un mod care să dăuneze semnificativ calității controlului intern al instituției de plată și capacității autorităților competente de a controla și de a urmări respectarea de către instituția de plată a tuturor obligațiilor stabilite în prezenta directivă."

4. La articolul 95 alineatul (1), se adaugă următorul paragraf:

„Primul paragraf nu aduce atingere aplicării capitolului II din Regulamentul (UE) 2022/2554:

(a) prestatorilor de servicii de plată menționați la articolul 1 alineatul (1) literele (a), (b) și (d) din prezenta directivă;

(b) prestatorilor de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din prezenta directivă;

(c) instituțiilor de plată exceptate în temeiul articolului 32 alineatul (1) din prezenta directivă; și

(d) instituțiilor emitente de monedă electronică care fac obiectul unei derogări astfel cum se menționează la articolul 9 alineatul (1) din Directiva 2009/110/CE."

5. La articolul 96, se adaugă următorul alineat:

„(7) Statele membre se asigură că alineatele (1)-(5) de la prezentul articol nu se aplică:

(a) prestatorilor de servicii de plată menționați la articolul 1 alineatul (1) literele (a), (b) și (d) din prezenta directivă;

(b) prestatorilor de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din prezenta directivă;

(c) instituțiilor de plată exceptate în temeiul articolul 32 alineatul (1) din prezenta directivă; și

(d) instituțiilor emitente de monedă electronică care fac obiectul unei derogări astfel cum se menționează la articolul 9 alineatul (1) din Directiva 2009/110/CE."

6. La articolul 98, alineatul (5) se înlocuiește cu următorul text:

„(5) În conformitate cu articolul 10 din Regulamentul (UE) nr. 1093/2010, ABE examinează și, după caz, actualizează în mod periodic standardele tehnice de reglementare în scopul, printre altele, de a ține seama de inovare și de evoluțiile tehnologice, precum și de dispozițiile capitolului II din Regulamentul (UE) 2022/2554."

Articolul 8

Modificarea Directivei (UE) 2016/2341

Articolul 21 alineatul (5) din Directiva (UE) 2016/2341 se înlocuiește cu următorul text:

„(5) Statele membre se asigură că IORP adoptă măsuri rezonabile pentru a asigura continuitatea și desfășurarea normală a activităților lor, inclusiv prin elaborarea unor planuri de contingență. În acest scop, IORP utilizează sisteme,

resurse și proceduri adecvate și proporționale și, în special, instituie și gestionează rețele și sisteme informatice în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*), după caz.

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

Articolul 9

Transpunerea

(1) Statele membre adoptă și publică până la 17 ianuarie 2025 dispozițiile necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta.

Statele membre aplică dispozițiile respective de la 17 ianuarie 2025.

Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o astfel de trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

(2) Comisiei îi sunt comunicate de către statele membre textele principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 10

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 11

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Strasbourg, 14 decembrie 2022.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	M. BEK

DIRECTIVA (UE) 2022/2557 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 14 decembrie 2022

privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ parlamentelor naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

având în vedere avizul Comitetului Regiunilor ([2]),

hotărând în conformitate cu procedura legislativă ordinară ([3]),

întrucât:

(1) În calitatea lor de furnizoare de servicii esențiale, entitățile critice joacă un rol indispensabil în menținerea funcțiilor societale sau a activităților economice vitale pe piața internă, într-o economie a Uniunii din ce în ce mai interdependentă. Prin urmare, este esențial să se stabilească un cadru la nivelul Uniunii, care să urmărească atât consolidarea rezilienței entităților critice de pe piața internă prin stabilirea unor norme minime armonizate, cât și sprijinirea acestora prin intermediul unor măsuri coerente și specifice de sprijin și supraveghere.

(2) Directiva 2008/114/CE a Consiliului ([4]) prevede o procedură de desemnare a infrastructurilor critice europene din sectoarele energiei și transporturilor a căror perturbare sau distrugere ar avea efecte transfrontaliere semnificative asupra a cel puțin două state membre. Directiva menționată se axează exclusiv pe protecția unor astfel de infrastructuri. Cu toate acestea, în cadrul evaluării Directivei 2008/114/CE efectuate în 2019 s-a constatat că, dat fiind faptul că operațiunile care utilizează infrastructura critică sunt tot mai interconectate și au din ce în ce mai mult un caracter transfrontalier, măsurile de protecție care se referă numai la elemente individuale sunt insuficiente pentru a preveni producerea tuturor perturbărilor. Prin urmare, este necesar ca abordarea să fie reorientată către asigurarea faptului că riscurile sunt mai bine luate în considerare, că rolul și sarcinile entităților critice în calitate de

([1]) JO C 286, 16.7.2021, p. 170.
([2]) JO C 440, 29.10.2021, p. 99.
([3]) Poziția Parlamentului European din 22 noiembrie 2022 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 8 decembrie 2022.
([4]) Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

furnizori de servicii esențiale pentru funcționarea pieței interne sunt mai bine definite și sunt coerente, precum și că se adoptă norme ale Uniunii pentru a consolida reziliența entităților critice. Entitățile critice ar trebui să fie în măsură să își consolideze capacitatea de a preveni incidente care pot să perturbe furnizarea de servicii esențiale, de a oferi protecție și de a rezista în cazul producerii incidentelor respective, de a răspunde la acestea, de a le atenua și a le absorbi, de a se adapta la ele și de a se redresa în urma lor.

(3) Deși o serie de măsuri la nivelul Uniunii, precum programul european privind protecția infrastructurilor critice, și la nivel național urmăresc să sprijine protecția infrastructurilor critice din Uniune, ar trebui depuse mai multe eforturi pentru a pregăti mai bine entitățile care operează astfel de infrastructuri pentru a aborda riscurile la adresa operațiunilor lor care ar putea conduce la perturbarea furnizării de servicii esențiale. Ar trebui depuse mai multe eforturi pentru a pregăti mai bine entitățile menționate dată fiind dinamica amenințărilor, care include amenințări hibride și teroriste aflate în evoluție, precum și interdependențele tot mai accentuate între infrastructură și sectoare. În plus, există un risc fizic sporit din cauza dezastrelor naturale și a schimbărilor climatice, care intensifică frecvența și amploarea fenomenelor meteorologice extreme și aduce schimbări pe termen lung în privința condițiilor climatice medii care pot reduce capacitatea,, eficiența și durata de viață a anumitor tipuri de infrastructură dacă nu se instituie măsuri de adaptare la schimbările climatice. În plus, piața internă este caracterizată de fragmentare în ceea ce privește identificarea entităților critice, întrucât sectoarele și categoriile de entități relevante nu sunt recunoscute în mod consecvent ca fiind critice în toate statele membre. Prin urmare, prezenta directivă ar trebui să ofere un nivel solid de armonizare în ceea ce privește sectoarele și categoriile de entități care intră sub incidența sa.

(4) Deși anumite sectoare ale economiei, cum ar fi sectoarele energiei și transporturilor, sunt deja reglementate prin acte sectoriale din dreptul Uniunii, actele respective conțin norme care se referă numai la anumite aspecte ale rezilienței entităților care își desfășoară activitatea în sectoarele respective. Pentru a aborda în mod cuprinzător reziliența entităților care sunt critice pentru buna funcționare a pieței interne, prezenta directivă creează un cadru global care abordează reziliența entităților critice în ceea ce privește toate pericolele, indiferent dacă sunt naturale sau provocate de om, accidentale sau intenționate.

(5) Interdependențele tot mai accentuate între infrastructură și sectoare sunt rezultatul unei rețele de furnizare de servicii al cărei caracter transfrontalier și interdependent devine tot mai pregnant, care utilizează infrastructuri-cheie în întreaga Uniune în sectorul energiei, al transporturilor, bancar, al apei potabile, al apelor uzate, al producției, prelucrării și distribuției de produse alimentare, al sănătății, în sectorul spațial, al infrastructurii pieței financiare, al infrastructurii digitale, precum și în anumite aspecte ale administrației publice. Sectorul spațial intră sub incidența prezentei directive în ceea ce privește furnizarea anumitor servicii care depind de infrastructura terestră deținută, gestionată și operată fie de statele membre, fie de părți private; prin urmare, infrastructura deținută, gestionată sau operată de Uniune sau în numele acesteia în cadrul programului său spațial nu intră sub incidența prezentei directive.

În ceea ce privește sectorul energetic și, în special, metodele de producere și transport a energiei electrice (din punctul de vedere al furnizării acesteia), se înțelege că, atunci când se consideră adecvat, producerea de energie electrică poate include părți ale transportului de energie electrică din centralele nucleare, cu excepția însă a elementelor strict nucleare care intră sub incidența tratatelor și a dreptului Uniunii, inclusiv a actelor din dreptul Uniunii relevante în domeniul nuclear. Procesul de identificare a entităților critice din sectorul alimentar ar trebui să reflecte în mod adecvat natura pieței interne din sectorul respectiv, precum și normele cuprinzătoare ale Uniunii referitoare la principiile și cerințele generale ale legislației alimentare și ale siguranței alimentare. Prin urmare, pentru a asigura existența unei abordări proporționale și pentru a reflecta în mod adecvat rolul și importanța acestor entități la nivel național, ar trebui să fie identificate entități critice numai în rândul acelor întreprinderi din sectorul alimentar, indiferent dacă au sau nu un scop lucrativ sau dacă sunt publice sau private, care își desfășoară activitatea exclusiv în domeniul logisticii, al distribuției angro și al producției și prelucrării industriale la scară largă, cu o cotă de piață semnificativă observată la nivel național. Aceste interdependențe înseamnă că orice perturbare a serviciilor esențiale, chiar și cele care inițial sunt limitate la o singură entitate sau la un singur sector, poate avea efecte în cascadă mai ample, ceea ce ar putea avea efecte negative considerabile și pe termen lung asupra furnizării de servicii pe piața internă. Crizele majore, precum pandemia de COVID-19, au demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere dar cu efect major.

(6) Entitățile implicate în furnizarea serviciilor esențiale fac din ce în ce mai mult obiectul unor cerințe divergente impuse de dreptul intern. Faptul că unele state membre impun entităților respective cerințe de securitate mai puțin stricte nu numai că creează niveluri de reziliență diferite, ci riscă de asemenea să aibă un efect negativ asupra funcțiilor societale sau a activităților economice vitale în întreaga Uniune și creează obstacole în calea bunei funcționări a pieței interne. Investitorii și întreprinderile se pot baza pe entitățile critice care sunt reziliente și pot avea încredere în ele, iar fiabilitatea și încrederea constituie fundamentele unei piețe interne funcționale. Tipuri similare de entități sunt considerate critice în unele state membre, dar nu și în altele, iar cele care sunt identificate ca fiind critice fac obiectul unor cerințe divergente în diferite state membre. Acest lucru duce la o sarcină administrativă suplimentară și inutilă pentru întreprinderile care își desfășoară activitatea la nivel transfrontalier, în special pentru întreprinderile care își desfășoară activitatea în statele membre cu cerințe mai stricte. Un cadru la nivelul Uniunii ar avea, prin urmare, și efectul de a crea condiții de concurență echitabile pentru entitățile critice din întreaga Uniune.

(7) Este necesar să se stabilească norme minime armonizate pentru a se asigura furnizarea serviciilor esențiale pe piața internă, pentru a consolida reziliența entităților critice și pentru a îmbunătăți cooperarea transfrontalieră între autoritățile competente. Este important ca normele respective să fie adaptate exigențelor viitorului în ceea ce privește conceperea și punerea lor în aplicare, permițând totodată flexibilitatea necesară. De asemenea, este esențial să se îmbunătățească capacitatea entităților critice de a furniza servicii esențiale atunci când sunt confruntate cu diverse riscuri.

(8) Pentru a obține un nivel înalt de reziliență, statele membre ar trebui să identifice entitățile critice care vor face obiectul unor cerințe și al unei supravegheri specifice, dar cărora li se va acorda un sprijin special și orientări speciale în fața tuturor riscurilor relevante.

(9) Având în vedere importanța securității cibernetice pentru reziliența entităților critice și din motive de consecvență, ar trebui să se asigure, ori de câte ori este posibil, o abordare coerentă între prezenta directivă și Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([5]). Având în vedere frecvența sporită și caracteristicile specifice ale riscurilor cibernetice, Directiva (UE) 2022/2555 impune cerințe cuprinzătoare unei game ample de entități pentru a garanta securitatea lor cibernetică. Dat fiind că securitatea cibernetică este abordată suficient de Directiva (UE) 2022/2555, aspectele reglementate de directiva respectivă ar trebui să fie excluse din domeniul de aplicare al prezentei directive, fără a aduce atingere regimului special al entităților din sectorul infrastructurii digitale.

(10) În cazul în care dispozițiile actelor sectoriale din dreptul Uniunii impun entităților critice să ia măsuri menite pentru a-și spori reziliența, iar cerințele respective sunt recunoscute de statele membre ca fiind cel puțin echivalente cu obligațiile corespunzătoare prevăzute în prezenta directivă, dispozițiile relevante ale prezentei directive nu ar trebui să se aplice, pentru a se evita suprapunerile și sarcinile inutile. În acest caz, ar trebui să se aplice dispozițiile relevante ale unor astfel de acte din dreptul Uniunii. În cazul în care nu se aplică dispozițiile relevante ale prezentei directive, nu ar trebui să se aplice nici dispozițiile privind supravegherea și asigurarea respectării legislației stabilite prin prezenta directivă.

(11) Prezenta directivă nu afectează competențele statelor membre și ale autorităților lor în materie de autonomie administrativă, sau responsabilitatea de a proteja securitatea și apărarea națională sau competența lor de a proteja alte funcții esențiale ale statului, în special în materie de siguranță publică, integritate teritorială și menținerea ordinii publice. Excluderea entităților administrației publice din domeniul de aplicare al prezentei directive ar trebui să se aplice entităților care desfășoară activități în principal în domeniul securității naționale, al siguranței publice, al apărării sau al asigurării respectării legii, inclusiv în ceea ce privește cercetarea, depistarea și pedepsirea infracțiunilor. Cu toate acestea, entitățile administrației publice ale căror activități sunt legate doar într-o mică măsură de domeniile menționate ar trebui să intre sub incidența prezentei directive. În sensul prezentei directive, entitățile cu competențe de reglementare nu sunt considerate ca desfășurând activități în domeniul asigurării respectării legii și, prin urmare, nu sunt excluse din aceste motive din domeniul de aplicare al prezentei directive. Entitățile administrației publice care sunt înființate în comun cu o țară terță în conformitate cu un acord internațional sunt excluse din domeniul de aplicare al prezentei directive. Prezenta directivă nu se aplică misiunilor diplomatice și consulare ale statelor membre în țări terțe.

([5]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (a se vedea pagina 80 din prezentul Jurnal Oficial).

Anumite entități critice desfășoară activități în domeniul securității naționale, al siguranței publice, al apărării sau al asigurării respectării legii, inclusiv în ceea ce privește cercetarea, depistarea și pedepsirea infracțiunilor sau furnizează servicii exclusiv pentru entități ale administrației publice care desfășoară activități în principal în domeniile menționate. Având în vedere responsabilitatea statelor membre de a proteja securitatea și apărarea națională, statele membre ar trebui să poată decide că obligațiile stabilite prin prezenta directivă entităților critice nu se aplică, integral sau parțial, respectivelor entități critice în cazul în care serviciile pe care acestea le furnizează sau activitățile pe care le desfășoară sunt legate în principal de domeniul securității naționale, al siguranței publice, al apărării sau al asigurării respectării legii, inclusiv în ceea ce privește cercetarea, depistarea și pedepsirea infracțiunilor. Entitățile critice ale căror servicii sau activități sunt legate doar într-o mică măsură de domeniile menționate ar trebui să intre sub incidența prezentei directive. Niciun stat membru nu ar trebui să aibă obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale siguranței sale naționale. Sunt relevante normele din dreptul Uniunii sau cele de drept intern privind protecția informațiilor clasificate și acordurile de nedivulgare.

(12) Pentru a nu pune în pericol securitatea națională sau securitatea și interesele comerciale ale entităților critice, accesul la informații sensibile, schimbul de astfel de informații și prelucrarea acestora ar trebui realizate cu grijă, acordând o atenție deosebită canalelor de transmitere și capacităților de stocare utilizate.

(13) În vederea asigurării unei abordări cuprinzătoare în ce privește reziliența entităților critice, fiecare stat membru ar trebui să dispună de o strategie pentru sporirea rezilienței entităților critice (denumită în continuare „strategia"). Strategia respectivă ar trebui să stabilească obiective strategice și măsuri de politică care să fie puse în aplicare. Din motive de coerență și eficiență, strategia ar trebui să fie concepută pentru a integra fără probleme politicile existente, bazându-se, ori de câte ori este posibil, pe strategii, planuri ori documente similare existente relevante la nivel național sau sectorial. Pentru a realiza o abordare cuprinzătoare, statele membre ar trebui să se asigure că strategiile lor oferă un cadru de politică pentru o coordonare consolidată între autoritățile competente în temeiul prezentei directive și autoritățile competente în temeiul Directivei (UE) 2022/2555 în contextul schimbului de informații privind riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice și riscurile, amenințările și incidentele non-cibernetice, precum și în contextul exercitării sarcinilor de supraveghere. Atunci când își pun în aplicare strategiile, statele membre ar trebui să țină seama în mod corespunzător de natura hibridă a amenințărilor la adresa entităților critice.

(14) Statele membre ar trebui să comunice Comisiei strategiile lor și toate actualizările substanțiale ale acestora, în special pentru a permite Comisiei să evalueze aplicarea corectă a prezentei directive în materie de abordări de politică privind reziliența entităților critice la nivel național. Strategiile ar putea fi comunicate sub formă de informații clasificate, dacă este necesar. Comisia ar trebui să elaboreze un raport de sinteză privind strategiile comunicate de statele membre pentru a servi drept bază pentru schimburi în vederea identificării bunelor practici și a aspectelor de interes comun în cadrul Grupului privind reziliența entităților critice. Având în vedere caracterul sensibil al informațiilor agregate incluse în raportul de sinteză – indiferent dacă sunt sau nu clasificate – Comisia ar trebui să gestioneze acest raport de sinteză cu un nivel de sensibilizare adecvat în ceea ce privește securitatea entităților critice, a statelor membre și a Uniunii. Raportul de sinteză și strategiile ar trebui să fie protejate împotriva acțiunilor ilegale sau răuvoitoare și ar trebui să fie accesibile numai persoanelor autorizate pentru a îndeplini obiectivele prezentei directive. Comunicarea strategiilor și a actualizărilor substanțiale ale acestora ar trebui, de asemenea, să contribuie la înțelegerea de către Comisie a evoluțiilor privind abordările în materie de reziliență a entităților critice și să contribuie la monitorizarea impactului și a valorii adăugate a prezentei directive, pe care Comisia urmează să o revizuiască periodic.

(15) Acțiunile întreprinse de statele membre pentru a identifica și a contribui la asigurarea rezilienței entităților critice ar trebui să urmeze o abordare bazată pe riscuri, care se concentrează pe entitățile cele mai relevante pentru îndeplinirea funcțiilor societale sau a activităților economice vitale. Pentru a se asigura o astfel de abordare direcționată, fiecare stat membru ar trebui să efectueze, într-un cadru armonizat, o evaluare a riscurilor naturale și provocate de om relevante, inclusiv a celor intersectoriale și transfrontaliere, care ar putea să afecteze furnizarea serviciilor esențiale, inclusiv a accidentelor, a dezastrelor naturale, a situațiilor de urgență din domeniul sănătății publice, cum ar fi pandemiile și amenințările hibride sau alte amenințări antagoniste, printre care infracțiunile de terorism, infiltrarea unor elemente infracționale și sabotajul (denumită în continuare „evaluarea riscurilor de către statul membru"). Atunci când efectuează evaluări ale riscurilor de către statul membru, statele membre ar trebui să țină seama de alte evaluări generale sau sectoriale ale riscurilor efectuate în temeiul altor acte din dreptul Uniunii și ar trebui să ia în considerare gradul de dependență între sectoare, inclusiv între sectoarele din alte state membre și țări terțe. Rezultatele evaluării riscurilor de către statul membru ar trebui utilizate în scopul de identificare a

entităților critice și de a sprijini aceste entități în îndeplinirea cerințelor care le revin în materie de reziliență. Prezenta directivă se aplică numai statelor membre și entităților critice care își desfășoară activitatea în Uniune. Cu toate acestea, expertiza și cunoștințele generate de autoritățile competente, în special prin evaluări ale riscurilor, precum și de Comisie, în special prin diverse forme de sprijin și cooperare, ar putea fi utilizate, după caz și în conformitate cu instrumentele juridice aplicabile, în beneficiul țărilor terțe, în special al celor din vecinătatea directă a Uniunii, alimentând cooperarea existentă în materie de reziliență.

(16) Pentru a se asigura faptul că toate entitățile relevante fac obiectul cerințelor în materie de reziliență ale prezentei directive și pentru a se reduce divergențele în această privință, este important să se stabilească norme armonizate care să permită identificarea consecventă a entităților critice în întreaga Uniune, permițând totodată statelor membre să reflecte în mod adecvat rolul și importanța acestor entități la nivel național. Atunci când aplică criteriile prevăzute în prezenta directivă, fiecare stat membru ar trebui să identifice entitățile care furnizează unul sau mai multe servicii esențiale și care operează și dețin infrastructuri critice situate pe teritoriul său. Ar trebui să se considere că o entitate operează pe teritoriul unui stat membru atunci când în acel stat membru își desfășoară activitățile necesare pentru serviciul sau serviciile esențiale în cauză și infrastructura sa critică, care este utilizată pentru a furniza serviciul sau serviciile respective, se găsește în acel stat membru. În cazul în care nu există nicio entitate care să îndeplinească criteriile respective într-un stat membru, statul membru respectiv nu ar trebui să aibă obligația de a identifica o entitate critică în sectorul sau subsectorul corespunzător. Din motive de eficacitate, eficiență, consecvență și securitate juridică, ar trebui să se stabilească, de asemenea, norme corespunzătoare privind notificarea entităților care au fost identificate drept entități critice.

(17) Statele membre ar trebui să transmită Comisiei, într-un mod care îndeplinește obiectivele prezentei directive, o listă privind serviciile esențiale, numărul de entități critice identificate pentru fiecare sector și subsector prevăzut în anexă, precum și, în cazul serviciului sau serviciilor esențiale furnizate de fiecare entitate, dacă acest lucru se aplică, pragurile. Pragurile ar trebui să poată fi prezentate ca atare sau în formă agregată, adică informațiile pot fi prezentate ca valori medii pe zonă geografică, pe an, pe sector, pe subsector sau prin alte mijloace și pot include informații privind gama de indicatori furnizați.

(18) Ar trebui să se stabilească criterii pentru determinarea importanței unui efect perturbator produs de un incident. Respectivele criterii ar trebui să se bazeze pe criteriile prevăzute în Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([6]) pentru a valorifica eforturile depuse de statele membre în vederea identificării operatorilor de servicii esențiale definite în directiva menționată, precum și experiența dobândită în această privință. Crizele majore, cum ar fi pandemia de COVID-19, au demonstrat importanța asigurării securității lanțului de aprovizionare și au demonstrat modul în care perturbarea acestuia poate avea efecte economice și societale negative asupra unui număr mare de sectoare, precum și la nivel transfrontalier. Prin urmare, statele membre ar trebui, de asemenea, să ia în considerare efectele asupra lanțului de aprovizionare, în măsura posibilului, atunci când determină gradul de dependență al altor sectoare și subsectoare față de serviciul esențial furnizat de o entitate critică.

(19) În conformitate cu dreptul Uniunii și cu dreptul intern aplicabile, inclusiv cu Regulamentul (UE) 2019/452 al Parlamentului European și al Consiliului ([7]) care stabilește un cadru pentru examinarea investițiilor străine directe în Uniune, trebuie recunoscută amenințarea potențială reprezentată de controlul străin asupra infrastructurilor critice din Uniune, deoarece serviciile, economia, libera circulație și siguranța cetățenilor Uniunii depind de buna funcționare a infrastructurii critice.

(20) Directiva (UE) 2022/2555 impune entităților din sectorul infrastructurii digitale, care ar putea fi identificate ca fiind entități critice în temeiul prezentei directive, să ia măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice, precum și pentru a notifica incidentele și amenințările cibernetice semnificative. Întrucât amenințările la adresa securității rețelelor și a sistemelor informatice pot avea origini diferite, Directiva (UE) 2022/2555 aplică o abordare care ține seama de toate riscurile, care include reziliența rețelelor și a sistemelor informatice, precum și a componentelor lor fizice și a mediului sistemelor respective.

([6]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

([7]) Regulamentul (UE) 2019/452 al Parlamentului European și al Consiliului din 19 martie 2019 de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniune (JO L 79 I, 21.3.2019, p. 1).

Având în vedere că cerințele stabilite prin Directiva (UE) 2022/2555 în acest sens sunt cel puțin echivalente cu obligațiile corespunzătoare stabilite prin prezenta directivă, obligațiile stabilite la articolul 11 și în capitolele III, IV și VI din prezenta directivă nu ar trebui să se aplice entităților din sectorul infrastructurii digitale, pentru a se evita suprapunerile și sarcinile administrative inutile. Cu toate acestea, având în vedere importanța serviciilor furnizate de entitățile din sectorul infrastructurii digitale unor entități critice care aparțin tuturor celorlalte sectoare, statele membre ar trebui să identifice, pe baza criteriilor și utilizând procedura prevăzută în prezenta directivă, entitățile din sectorul infrastructurii digitale ca fiind entități critice. În consecință, ar trebui să se aplice strategiile, evaluările riscurilor de către statele membre și măsurile de sprijin prevăzute în capitolul II din prezenta directivă. Statele membre ar trebui să poată adopta sau menține dispoziții de drept intern pentru a atinge un nivel mai ridicat de reziliență pentru entitățile critice respective, cu condiția ca respectivele dispoziții să fie coerente cu dreptul aplicabil al Uniunii.

(21) Dreptul Uniunii în domeniul serviciilor financiare instituie cerințe cuprinzătoare pentru entitățile financiare de a gestiona toate riscurile cu care se confruntă acestea, inclusiv riscurile operaționale, și de a asigura continuitatea activității. Dreptul respectiv include Regulamentele (UE) nr. 648/2012 ([8]), (UE) nr. 575/2013 ([9]) și (UE) nr. 600/2014 ([10]) ale Parlamentului European și ale Consiliului și Directivele 2013/36/UE ([11]) și 2014/65/UE ([12]) ale Parlamentului European și ale Consiliului. Cadrul juridic menționat este completat de Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului ([13]), care stabilește cerințele aplicabile entităților financiare în ceea ce privește gestionarea riscurilor TIC, inclusiv protecția infrastructurilor TIC fizice. Întrucât reziliența entităților respective este, prin urmare, reglementată în mod cuprinzător, articolul 11 și capitolele III, IV și VI din prezenta directivă nu ar trebui să se aplice entităților respective, pentru a evita suprapunerile și sarcinile administrative inutile.

Cu toate acestea, având în vedere importanța serviciilor furnizate de entitățile din sectorul financiar unor entități critice care aparțin tuturor celorlalte sectoare, statele membre ar trebui să identifice, pe baza criteriilor și utilizând procedura prevăzută în prezenta directivă, entitățile din sectorul financiar ca fiind entități critice. În consecință, ar trebui să se aplice strategiile, evaluările riscurilor de către statele membre și măsurile de sprijin prevăzute în capitolul II din prezenta directivă. Statele membre ar trebui să poată adopta sau menține dispoziții de drept intern pentru a atinge un nivel mai ridicat de reziliență pentru entitățile critice respective, cu condiția ca respectivele dispoziții să fie coerente cu dreptul aplicabil al Uniunii.

(22) Statele membre ar trebui să desemneze sau să înființeze autorități competente care să supravegheze aplicarea și, dacă este necesar, să asigure respectarea normelor prezentei directive și să garanteze faptul că aceste autorități dispun de competențele și de resursele adecvate. Având în vedere diferențele dintre structurile naționale de guvernanță, pentru a salvgarda dispozițiile sectoriale existente sau organismele de supraveghere și de reglementare ale Uniunii, precum și pentru a evita suprapunerile, statele membre ar trebui să poată desemna sau înființa una sau mai multe autorități competente. Atunci când desemnează sau înființează mai multe autorități competente, statele membre ar trebui să delimiteze în mod clar sarcinile care le revin autorităților în cauză și să se asigure că acestea cooperează în mod armonios și eficace. Toate autoritățile competente ar trebui, de asemenea, să coopereze pe un plan mai general cu alte autorități relevante, la nivelul Uniunii și la nivel național.

([8]) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1).

([9]) Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

([10]) Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 173, 12.6.2014, p. 84).

([11]) Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

([12]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).

([13]) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/2011 (a se vedea pagina 1 din prezentul Jurnal Oficial).

(23) Pentru a facilita cooperarea și comunicarea la nivel transfrontalier și pentru a permite punerea în aplicare eficace a prezentei directive, fiecare stat membru ar trebui, fără a aduce atingere actelor sectoriale din dreptul Uniunii, să desemneze un punct unic de contact responsabil cu coordonarea aspectelor legate de reziliența entităților critice și de cooperarea transfrontalieră la nivelul Uniunii (denumit în continuare „punct unic de contact"), după caz în cadrul unei autorități competente. Fiecare punct unic de contact ar trebui să asigure legăturile și să coordoneze comunicarea, atunci când acest lucru este relevant, cu autoritățile competente din statul său membru, cu punctele unice de contact din alte state membre și cu Grupul privind reziliența entităților critice.

(24) Autoritățile competente în temeiul prezentei directive și autoritățile competente în temeiul Directivei (UE) 2022/2555 ar trebui să coopereze și să facă schimb de informații în ceea ce privește riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice și riscurile, amenințările și incidentele non-cibernetice care afectează entitățile critice, precum și în ceea ce privește măsurile relevante luate de autoritățile competente în temeiul prezentei directive și de autoritățile competente în temeiul Directivei (UE) 2022/2555. Este important ca statele membre să se asigure că cerințele prevăzute în prezenta directivă și în Directiva (UE) 2022/2555 sunt puse în aplicare în mod complementar și că entitățile critice nu sunt supuse unei sarcini administrative mai mari decât cea necesară pentru a atinge obiectivele prezentei directive și pe cele ale directivei menționate.

(25) Statele membre ar trebui să sprijine entitățile critice, inclusiv pe cele care pot fi considerate întreprinderi mici sau mijlocii, să își consolideze reziliența, în conformitate cu obligațiile care le revin statelor membre în temeiul prezentei directive, fără a aduce atingere responsabilității juridice a entităților critice de a asigura această conformitate, iar în cadrul demersurilor lor, ar trebui să evite sarcinile administrative excesive. Statele membre ar putea, în special, să elaboreze materiale de orientare și metodologii, să sprijine organizarea de exerciții pentru a testa reziliența entităților critice și să asigure furnizarea de consiliere și formarea personalului acestora. Atunci când acest lucru este necesar și justificat de obiective de interes public, statele membre ar putea furniza resurse financiare și ar trebui să faciliteze schimbul voluntar de informații și de bune practici între entitățile critice, fără a aduce atingere aplicării normelor în materie de concurență prevăzute în Tratatul privind funcționarea Uniunii Europene (TFUE).

(26) Pentru a consolida reziliența entităților critice identificate de statele membre și pentru a reduce sarcinile administrative ale acestor entități critice, autoritățile competente ar trebui să se consulte reciproc ori de câte ori acest lucru este oportun pentru a asigura aplicarea în mod coerent a prezentei directive. Consultările respective ar trebui să fie inițiate la cererea oricărei autorități competente interesate și ar trebui să se axeze pe asigurarea unei abordări convergente în ceea ce privește entitățile critice interconectate care utilizează infrastructuri critice conectate fizic între două sau mai multe state membre, care aparțin acelorași grupuri sau structuri corporative sau care au fost identificate într-un stat membru și furnizează servicii esențiale pentru alte state membre sau pe teritoriul acestora.

(27) În cazul în care dispoziții din dreptul Uniunii sau dreptul intern impun entităților critice să evalueze riscuri relevante în sensul prezentei directive și să ia măsuri pentru a asigura propria lor reziliență, cerințele respective ar trebui să fie luate în considerare în mod adecvat în scopul supravegherii respectării de către entitățile critice a prezentei directive.

(28) Entitățile critice ar trebui să aibă o înțelegere cuprinzătoare a riscurilor relevante la care sunt expuse, precum și sarcina de a le analiza. În acest scop, entitățile critice ar trebui să efectueze evaluări ale riscurilor, ori de câte ori este necesar, având în vedere situația lor specifică și evoluția respectivelor riscuri, și, în orice caz, o dată la patru ani, în vederea evaluării tuturor riscurilor relevante care ar putea întrerupe furnizarea serviciilor lor esențiale (denumită în continuare „evaluarea riscurilor de către entitatea critică"). Atunci când au efectuat alte evaluări ale riscurilor sau au întocmit documente în temeiul obligațiilor prevăzute în alte acte de drept care sunt relevante pentru evaluarea riscurilor de către entitatea critică, entitățile critice ar trebui să poată utiliza evaluările și documentele respective pentru a îndeplini cerințele prevăzute în prezenta directivă referitoare la evaluarea riscurilor de către entitatea critică. O autoritate competentă ar trebui să poată declara o evaluare existentă a riscurilor efectuată de o entitate critică, care abordează riscurile relevante și gradul de dependență existent, ca fiind conformă, integral sau parțial, cu obligațiile stabilite prin prezenta directivă.

(29) Entitățile critice ar trebui să ia măsuri tehnice, de securitate și organizatorice corespunzătoare și proporționale cu riscurile cu care se confruntă, astfel încât să prevină incidentele, să ofere protecție și să reziste în cazul producerii acestora, să răspundă și să reziste la ele, să le atenueze, să le absoarbă, să se adapteze la ele și să se redreseze în urma lor. În măsura în care entitățile critice ar trebui să ia măsurile menționate în conformitate cu prezenta directivă, detaliile și amploarea măsurilor respective ar trebui să reflecte, într-un mod adecvat și proporțional, diferitele riscuri pe care fiecare entitate critică le-a identificat în cadrul evaluării riscurilor de către entitatea critică, precum și specificitățile respectivei entități. Pentru a promova o abordare coerentă la nivelul Uniunii, Comisia ar trebui, după consultarea Grupului privind reziliența entităților critice, să adopte orientări fără caracter obligatoriu pentru a detalia măsurile tehnice, de securitate și organizatorice respective. Statele membre ar trebui să se asigure că fiecare entitate critică desemnează un ofițer de legătură sau un echivalent al acestuia ca punct de contact în relația cu autoritățile competente.

(30) Din motive de eficacitate și de asigurare a asumării răspunderii, entitățile critice ar trebui să descrie măsurile pe care le adoptă, cu un nivel de detaliere care permite realizarea într-o măsură suficientă a obiectivelor de eficacitate și de asigurare a asumării răspunderii, ținând seama de riscurile identificate, într-un plan de reziliență sau într-un document echivalent sau în documente echivalente cu un plan de reziliență, și să aplice în practică respectivul plan. În scopul de a evita suprapunerile, atunci când o entitate critică a adoptat deja măsuri tehnice, de securitate și organizatorice și a întocmit documente în temeiul altor acte de drept care sunt relevante pentru măsurile de consolidare a rezilienței în temeiul prezentei directive, entitatea critică în cauză ar trebui să poată utiliza măsurile și documentele respective pentru a-și îndeplini obligațiile în ceea ce privește măsurile de reziliență în temeiul prezentei directive. În scopul de a evita suprapunerile, o autoritate competentă ar trebui să poată declara măsurile de reziliență existente adoptate de o entitate critică pentru a-și îndeplini obligația de a adopta măsuri tehnice, de securitate și organizatorice în temeiul prezentei directive, ca fiind integral sau parțial conforme cu cerințele prezentei directive.

(31) Regulamentele (CE) nr. 725/2004 ([14]) și (CE) nr. 300/2008 ([15]) ale Parlamentului European și ale Consiliului și Directiva 2005/65/CE a Parlamentului European și a Consiliului ([16]) stabilesc cerințe aplicabile entităților din sectoarele aviației și transportului maritim pentru a preveni incidentele cauzate de acte ilegale, a rezista în cazul producerii unor astfel de incidente și a le atenua consecințele. Cu toate că măsurile necesare în temeiul prezentei directive sunt mai ample în ceea ce privește riscurile abordate și tipurile de măsuri care urmează să fie adoptate, entitățile critice din aceste sectoare ar trebui să reflecte în planul lor de reziliență sau în documente echivalente măsurile luate în temeiul altor acte de drept al Uniunii. Entitățile critice trebuie să ia în considerare și Directiva 2008/96/CE a Parlamentului European și a Consiliului ([17]), care introduce o evaluare la nivelul întregii rețele rutiere pentru a inventaria riscurile de accidente și o inspecție specifică în materie de siguranță rutieră pentru a identifica condițiile periculoase, defectele și problemele care sporesc riscul de accidente și de vătămare corporală, prin vizitarea la fața locului a drumurilor existente sau a tronsoanelor de drum. Asigurarea protecției și rezilienței entităților critice este extrem de importantă pentru sectorul feroviar și, atunci când pun în aplicare măsuri de reziliență în temeiul prezentei directive, entitățile critice sunt încurajate să ia în considerare orientările fără caracter obligatoriu și documentele de bune practici elaborate în cadrul unor fluxuri de lucru sectoriale, cum ar fi Platforma UE pentru securitatea călătorilor din transportul feroviar instituită prin Decizia 2018/C 232/03 a Comisiei ([18]).

(32) Riscul ca angajații sau contractanții entităților critice să abuzeze, de exemplu, de drepturile lor de acces în cadrul organizației entității critice pentru a provoca daune și a aduce prejudicii este din ce în ce mai îngrijorător. Prin urmare, statele membre ar trebui să precizeze condițiile în care entităților critice li se permite, în cazuri justificate în mod corespunzător și ținând seama de evaluarea riscurilor de către statul membru, să depună cereri de verificare a antecedentelor persoanelor aparținând unor categorii de personal propriu. Ar trebui să se asigure faptul că autoritățile relevante analizează astfel de cereri într-un termen rezonabil și le prelucrează în conformitate cu dreptul intern și procedurile naționale, precum și cu dreptul relevant și aplicabil al Uniunii, inclusiv în ceea ce privește protecția datelor cu caracter personal. Pentru a confirma identitatea unei persoane care face obiectul unei verificări a antecedentelor, statele membre pot solicita o dovadă a identității, precum un pașaport, o carte națională de identitate sau o formă digitală de identificare, în conformitate cu dreptul aplicabil.

([14]) Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare (JO L 129, 29.4.2004, p. 6).

([15]) Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72).

([16]) Directiva 2005/65/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind consolidarea securității portuare (JO L 310, 25.11.2005, p. 28).

([17]) Directiva 2008/96/CE a Parlamentului European și a Consiliului din 19 noiembrie 2008 privind gestionarea siguranței infrastructurii rutiere (JO L 319, 29.11.2008, p. 59).

([18]) Decizia Comisiei din 29 iunie 2018 de înființare a Platformei UE pentru securitatea călătorilor din transportul feroviar, 2018/C 232/03 (JO C 232, 3.7.2018, p. 10).

Verificarea antecedentelor ar trebui să includă verificarea cazierului judiciar al persoanei vizate. Statele membre ar trebui să folosească Sistemul european de informații cu privire la cazierele judiciare, în conformitate cu procedurile prevăzute în Decizia-cadru 2009/315/JAI a Consiliului ([19]) și, dacă este relevant și aplicabil, în Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului ([20]), pentru a obține informații din cazierele judiciare păstrate în alte state membre. Statele membre ar putea, de asemenea, dacă este relevant și aplicabil, să utilizeze Sistemul de informații Schengen de a doua generație (SIS II) instituit prin Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului ([21]), informații operative și orice alte informații obiective disponibile care ar putea fi necesare pentru a stabili dacă persoana în cauză este adecvată pentru a ocupa postul în legătură cu care entitatea critică a solicitat o verificare a antecedentelor.

(33) Ar trebui să se stabilească un mecanism de notificare a anumitor incidente care să permită autorităților competente să reacționeze rapid și în mod adecvat la incidente și să aibă o imagine de ansamblu cuprinzătoare asupra efectelor, naturii, cauzei și posibilelor consecințe ale incidentelor cu care se confruntă entitățile critice. Entitățile critice ar trebui să notifice autorităților competente, fără întârzieri nejustificate, incidentele care perturbă în mod semnificativ sau care au potențialul de a perturba în mod semnificativ furnizarea serviciilor esențiale. Cu excepția cazului în care nu pot face acest lucru din motive operaționale, entitățile critice ar trebui să transmită o notificare inițială în termen de cel mult 24 de ore de la data la care au luat cunoștință de un incident. Notificarea inițială ar trebui să includă numai informațiile absolut necesare pentru a informa autoritatea competentă cu privire la incident și pentru a permite entității critice să solicite asistență, dacă este necesar. O astfel de notificare ar trebui să indice, dacă este posibil, cauza presupusă a incidentului. Statele membre ar trebui să se asigure că cerința de transmitere a acestei notificări inițiale nu deviază resursele entității critice raportoare de la activitățile legate de gestionarea incidentelor, care ar trebui să aibă prioritate. Notificarea inițială ar trebui să fie urmată, după caz, de un raport detaliat în termen de cel mult o lună de la incident. Raportul detaliat ar trebui să completeze notificarea inițială și să ofere o imagine de ansamblu mai completă a incidentului.

(34) Standardizarea ar trebui să rămână, în principal, un proces bazat pe piață. Cu toate acestea, ar mai putea exista situații în care este oportun să se impună respectarea unor standarde specificate. Atunci când acest lucru este util, statele membre ar trebui să încurajeze utilizarea standardelor și specificațiilor tehnice europene și a celor internaționale care sunt pertinente pentru măsurile de securitate și de reziliență aplicabile entităților critice.

(35) Cu toate că entitățile critice își desfășoară în general activitatea în cadrul unei rețele tot mai interconectate de furnizare de servicii și de infrastructură și furnizează adesea servicii esențiale în mai multe state membre, unele dintre aceste entități critice au o importanță deosebită pentru Uniune și pentru piața internă a acesteia, deoarece furnizează servicii esențiale pentru șase sau mai multe state membre sau pe teritoriul acestora și, prin urmare, ar putea să beneficieze de sprijin specific la nivelul Uniunii. Prin urmare, ar trebui să se instituie norme privind misiuni de consiliere în ceea ce privește astfel de entități critice de importanță europeană deosebită. Normele respective nu aduc atingere normelor privind supravegherea și asigurarea respectării legislației, prevăzute în prezenta directivă.

(36) La cererea motivată din partea Comisiei sau din partea unuia sau a mai multor state membre cărora sau pe teritoriul cărora se furnizează serviciul esențial, în cazul în care sunt necesare informații suplimentare pentru a putea consilia o entitate critică în îndeplinirea obligațiilor care îi revin în temeiul prezentei directive sau pentru a evalua respectarea acestor obligații de către o entitate critică de importanță europeană deosebită, statul membru care a identificat o entitate critică de importanță europeană deosebită ca fiind o entitate critică ar trebui să pună la dispoziția Comisiei anumite informații astfel cum se prevede în prezenta directivă. De comun acord cu statul membru care a identificat entitatea critică de importanță europeană deosebită ca fiind o entitate critică, Comisia ar trebui să aibă posibilitatea de a organiza o misiune de consiliere pentru a evalua măsurile instituite de entitatea în cauză. Pentru a se asigura buna desfășurare a acestor misiuni de consiliere, ar trebui să se instituie norme complementare, în special în ceea ce privește organizarea și desfășurarea misiunilor de consiliere, acțiunile subsecvente desfășurate și obligațiile care le

([19]) Decizia-cadru 2009/315/JAI a Consiliului din 26 februarie 2009 privind organizarea și conținutul schimbului de informații extrase din cazierele judiciare între statele membre (JO L 93, 7.4. 2009, p. 23).

([20]) Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului din 17 aprilie 2019 de stabilire a unui sistem centralizat pentru determinarea statelor membre care dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierele judiciare, și de modificare a Regulamentului (UE) 2018/1726 (JO L 135, 22.5.2019, p. 1).

([21]) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56).

revin entităților critice de importanță europeană deosebită vizate. Fără a aduce atingere necesității ca statul membru în care se efectuează misiunea de consiliere și entitatea critică în cauză să respecte normele stabilite prin prezenta directivă, misiunea de consiliere ar trebui să se desfășoare cu respectarea normelor de drept detaliate ale respectivului stat membru, de exemplu cele privind condițiile exacte care trebuie să fie îndeplinite pentru a avea acces la sediile sau la documentele relevante și cele privind căile de atac. Expertiza specifică necesară pentru aceste misiuni de consiliere ar putea fi solicitată, după caz, prin intermediul Centrului de coordonare a răspunsului la situații de urgență instituit prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului ([22]).

(37) Pentru a sprijini Comisia și pentru a facilita cooperarea între statele membre și schimbul de informații, inclusiv de bune practici, cu privire la aspectele referitoare la prezenta directivă, ar trebui să se constituie Grupul privind reziliența entităților critice, ca grup de experți al Comisiei. Statele membre ar trebui să depună eforturi pentru a asigura o cooperare eficace și eficientă a reprezentanților desemnați ai autorităților lor competente în cadrul Grupului privind reziliența entităților critice, inclusiv prin desemnarea unor reprezentanți care să dețină autorizarea de securitate adecvată, atunci când este cazul. Grupul privind reziliența entităților critice ar trebui să înceapă să își îndeplinească sarcinile cât mai curând posibil, astfel încât să pună la dispoziție mijloace suplimentare pentru o cooperare corespunzătoare pe parcursul perioadei de transpunere a prezentei directive. Grupul privind reziliența entităților critice ar trebui să interacționeze cu alte grupuri de lucru relevante la nivel de experți, specifice sectorului.

(38) Grupul privind reziliența entităților critice ar trebui să coopereze cu Grupul de cooperare constituit în temeiul Directivei (UE) 2022/2555 în vederea sprijinirii unui cadru cuprinzător pentru reziliența cibernetică și non-cibernetică a entităților critice. Grupul privind reziliența entităților critice și Grupul de cooperare constituit în temeiul Directivei (UE) 2022/2555 ar trebui să se angajeze într-un dialog periodic pentru a promova cooperarea dintre autoritățile competente în temeiul prezentei directive și autoritățile competente în temeiul Directivei (UE) 2022/2555 și pentru a facilita schimbul de informații, în special cu privire la subiecte relevante pentru ambele grupuri.

(39) Pentru a realiza obiectivele prezentei directive și fără a aduce atingere responsabilității juridice a statelor membre și a entităților critice de a asigura respectarea obligațiilor care le revin în temeiul prezentei directive, Comisia ar trebui, atunci când consideră oportun, să sprijine autoritățile competente și entitățile critice în vederea facilitării respectării de către acestea a obligațiilor care le revin. Atunci când acordă sprijin statelor membre și entităților critice în punerea în aplicare a obligațiilor care le revin în temeiul prezentei directive, Comisia ar trebui să se bazeze pe structurile și instrumentele existente, cum ar fi cele din cadrul mecanismului de protecție civilă al Uniunii, instituit prin Decizia nr. 1313/2013/UE și al Rețelei europene de referință pentru protecția infrastructurii critice. În plus, Comisia ar trebui să informeze statele membre cu privire la resursele disponibile la nivelul Uniunii, cum ar fi cele din cadrul Fondului pentru securitate internă instituit prin Regulamentul (UE) 2021/1149 al Parlamentului European și al Consiliului ([23]), al programului Orizont Europa instituit prin Regulamentul (UE) 2021/695 al Parlamentului European și al Consiliului ([24]), sau al altor instrumente relevante pentru reziliența entităților critice.

(40) Statele membre ar trebui să asigure faptul că autoritățile lor competente dispun de anumite competențe specifice pentru aplicarea și asigurarea respectării în mod corespunzător a prezentei directive în ceea ce privește entitățile critice, în cazul în care aceste entități țin de jurisdicția lor, astfel cum se specifică în prezenta directivă. Printre aceste competențe ar trebui să se numere, în special, competența de a efectua inspecții și audituri, competența de a supraveghea, competența de a solicita entităților critice să furnizeze informații și dovezi cu privire la măsurile pe care le-au luat pentru a-și îndeplini obligațiile și, dacă este necesar, competența de a emite ordine pentru a remedia încălcările identificate. Atunci când emit astfel de ordine, statele membre nu ar trebui să impună măsuri care să depășească ceea ce este necesar și proporțional pentru a asigura respectarea normelor de către entitatea critică în cauză, ținând seama în special de gravitatea încălcării și de capacitatea economică a entității critice în cauză. La un nivel mai general, aceste competențe ar trebui să fie însoțite de garanții corespunzătoare și eficace care să fie

([22]) Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).

([23]) Regulamentul (UE) 2021/1149 al Parlamentului European și al Consiliului din 7 iulie 2021 de instituire a Fondului pentru securitate internă (JO L 251, 15.7.2021, p. 94).

([24]) Regulamentul (UE) 2021/695 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a programului-cadru pentru cercetare și inovare Orizont Europa, de stabilire a normelor sale de participare și de diseminare și de abrogare a Regulamentelor (UE) nr. 1290/2013 și (UE) nr. 1291/2013 (JO L 170, 12.5.2021, p. 1).

specificate în dreptul intern în conformitate cu Carta drepturilor fundamentale a Uniunii Europene. Atunci când analizează respectarea de către o entitate critică a obligațiilor care îi revin în temeiul prezentei directive, autoritățile competente în temeiul prezentei directive ar trebui să poată solicita autorităților competente în temeiul Directivei (UE) 2022/2555 să își exercite competențele de supraveghere și de asigurare a respectării legislației în legătură cu o entitate care intră sub incidența respectivei directive și care a fost identificată drept o entitate critică în temeiul prezentei directive. Autoritățile competente în temeiul prezentei directive și autoritățile competente în temeiul Directivei (UE) 2022/2555 ar trebui să coopereze și să facă schimb de informații în acest scop.

(41) Pentru a aplica prezenta directivă într-un mod eficace și consecvent, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei pentru a completa prezenta directivă prin elaborarea unei liste de servicii esențiale. Lista respectivă ar trebui să fie utilizată de autoritățile competente în scopul efectuării evaluării riscurilor de către statul membru și al identificării entităților critice în temeiul prezentei directive. În conformitate cu abordarea armonizării minime din prezenta directivă, lista menționată nu este exhaustivă, iar statele membre ar putea să o completeze cu servicii esențiale suplimentare la nivel național pentru a ține seama de particularitățile naționale în furnizarea serviciilor esențiale. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([25]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(42) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentei directive, Comisiei ar trebui să i se confere competențe de executare. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([26]).

(43) Întrucât obiectivele prezentei directive, și anume de a asigura că serviciile esențiale pentru menținerea funcțiilor societale sau a activităților economice vitale sunt furnizate pe piața internă fără a fi obstrucționate și de a consolida reziliența entităților critice care furnizează astfel de servicii, nu pot fi realizate în mod satisfăcător de către statele membre și, având în vedere efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul 5 menționat, prezenta directivă nu depășește ceea ce este necesar pentru realizarea acestor obiective.

(44) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([27]) și a emis un aviz la 11 august 2021.

(45) Prin urmare, Directiva 2008/114/CE ar trebui să fie abrogată,

([25]) JO L 123, 12.5.2016, p. 1.

([26]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([27]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

(1) Prezenta directivă:

(a) stabilește pentru statele membre obligații de a lua măsuri specifice menite să asigure furnizarea neîngrădită pe piața internă a serviciilor esențiale pentru menținerea funcțiilor societale sau a activităților economice vitale, în limitele domeniului de aplicare al articolului 114 din TFUE, în special obligații de a identifica entitățile critice și de a sprijini entitățile critice pentru a-și îndeplini obligațiile care le revin;

(b) stabilește pentru entitățile critice obligații menite să le sporească reziliența și capacitatea de a furniza pe piața internă serviciile menționate la litera (a);

(c) stabilește norme privind:

(i) supravegherea entităților critice;

(ii) asigurarea respectării legii;

(iii) identificarea entităților critice de importanță europeană deosebită și privind evaluarea de către misiunile de consiliere a măsurilor pe care entitățile menționate le-au pus în aplicare pentru a-și îndeplini obligațiile care le revin în temeiul capitolului III;

(d) stabilește proceduri comune de cooperare și raportare în ceea ce privește aplicarea prezentei directive;

(e) stabilește măsuri menite să asigure un nivel ridicat al rezilienței entităților critice pentru a asigura furnizarea serviciilor esențiale în Uniune și pentru a îmbunătăți funcționarea pieței interne.

(2) Prezenta directivă nu se aplică aspectelor reglementate de Directiva (UE) 2022/2555, fără a aduce atingere articolului 8 din prezenta directivă. Având în vedere relația dintre securitatea fizică și securitatea cibernetică a entităților critice, statele membre asigură punerea în aplicare coordonată a prezentei directive și a Directivei (UE) 2022/2555.

(3) Dispozițiile relevante ale prezentei directive, inclusiv dispozițiile privind supravegherea și asigurarea respectării legislației prevăzute în capitolul VI, nu se aplică în cazul în care dispozițiile actelor sectoriale din dreptul Uniunii impun entităților critice să ia măsuri de consolidare a rezilienței, iar cerințele respective sunt recunoscute de statele membre ca fiind cel puțin echivalente cu obligațiile corespunzătoare prevăzute în prezenta directivă.

(4) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în temeiul normelor Uniunii sau al normelor naționale, cum ar fi cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante în conformitate cu prezenta directivă numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații relevante și proporționale cu scopul respectivului schimb. Acest schimb de informații păstrează confidențialitatea informațiilor respective și securitatea și interesele comerciale ale entităților critice, respectând totodată securitatea statelor membre.

(5) Prezenta directivă nu aduce atingere responsabilității statelor membre de a proteja securitatea și apărarea națională sau competenței acestora de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale a statului și menținerea ordinii publice.

(6) Prezenta directivă nu se aplică entităților administrației publice care își desfășoară activitățile în domeniul securității naționale, al siguranței publice, al apărării sau al asigurării respectării legii, inclusiv în ceea ce privește cercetarea, depistarea și urmărirea penală a infracțiunilor.

(7) Statele membre pot decide că articolul 11 și capitolele III, IV și VI nu se aplică, integral sau parțial, anumitor entități critice care își desfășoară activitățile în domeniul securității naționale, al siguranței publice, al apărării sau al asigurării respectării legii, inclusiv în ceea ce privește cercetarea, depistarea și urmărirea penală a infracțiunilor, sau care prestează servicii exclusiv entităților administrației publice menționate la alineatul (6) de la prezentul articol.

(8) Obligațiile prevăzute în prezenta directivă nu implică furnizarea de informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

(9) Prezenta directivă nu aduce atingere dreptului Uniunii privind protecția datelor cu caracter personal, în special Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([28]) și Directivei 2002/58/CE a Parlamentului European și a Consiliului ([29]).

Articolul 2

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

1. „entitate critică” înseamnă o entitate publică sau privată care a fost identificată de un stat membru în conformitate cu articolul 6 ca aparținând uneia dintre categoriile menționate în a treia coloană a tabelului din anexă;

2. „reziliență” înseamnă capacitatea unei entități critice de a preveni un incident, de a oferi protecție și de a rezista în cazul producerii unui incident, de a răspunde la un incident, de a atenua un incident, de a absorbi un incident, de a se adapta unui incident și de a se redresa în urma unui incident;

3. „incident” înseamnă orice eveniment care are potențialul de a perturba în mod semnificativ sau care perturbă furnizarea unui serviciu esențial, inclusiv atunci când afectează sistemele naționale care protejează statul de drept;

4. „infrastructură critică” înseamnă un activ, o instalație, un echipament, o rețea ori un sistem, sau o componentă a unui activ, instalații, echipament, rețea ori sistem, care este necesar(ă) pentru furnizarea unui serviciu esențial;

5. „serviciu esențial” înseamnă un serviciu care este indispensabil pentru menținerea funcțiilor societale vitale, a activităților economice vitale, a sănătății și siguranței publice, sau a mediului;

6. „risc” înseamnă potențialele pierderi sau perturbări cauzate de un incident și se exprimă ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului respectiv;

7. „evaluarea riscurilor” înseamnă procesul global prin care se determină natura și amploarea unui risc prin identificarea și analiza potențialelor amenințări, vulnerabilități și pericole relevante care ar putea conduce la un incident și prin evaluarea potențialelor pierderi sau perturbări ale furnizării unui serviciu esențial provocate de incidentul respectiv;

8. „standard” înseamnă un standard în înțelesul definiției de la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([30]);

([28]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([29]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([30]) Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

9. „specificație tehnică” înseamnă o specificație tehnică în înțelesul definiției de la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

10. „entitate a administrației publice” înseamnă o entitate, recunoscută ca atare într-un stat membru în conformitate cu dreptul intern, cu excepția autorităților judecătorești, parlamentare sau a băncilor centrale, care îndeplinește următoarele criterii:

(a) a fost înființată în scopul satisfacerii unor nevoi de interes general și nu are caracter industrial sau comercial;

(b) are personalitate juridică sau este abilitată prin lege să acționeze în numele unei alte entități cu personalitate juridică;

(c) este finanțată, în cea mai mare parte, de autoritățile statului sau de alte organisme centrale de drept public, face obiectul unui control de gestiune din partea autorităților sau a organismelor respective, sau are un consiliu de administrație, de conducere sau de supraveghere ai cărui membri sunt desemnați în proporție de peste 50 % de autoritățile statului sau de alte organisme centrale de drept public;

(d) are competența de a adresa persoanelor fizice sau juridice decizii administrative sau de reglementare care le afectează drepturile în ceea ce privește circulația transfrontalieră a persoanelor, mărfurilor, serviciilor sau capitalurilor.

Articolul 3

Armonizarea minimă

Prezenta directivă nu împiedică adoptarea sau menținerea de către statele membre a unor dispoziții de drept intern în vederea obținerii unui nivel mai ridicat de reziliență a entităților critice, cu condiția care dispozițiile respective să fie conforme cu obligațiilor care revin statelor membre în temeiul dreptului Uniunii.

CAPITOLUL II

CADRELE NAȚIONALE PRIVIND REZILIENȚA ENTITĂȚILOR CRITICE

Articolul 4

Strategia privind reziliența entităților critice

(1) În urma unei consultări care este, în măsura în care este posibil din punct de vedere practic, deschisă părților interesate relevante, fiecare stat membru adoptă o strategie de consolidare a rezilienței entităților critice (denumită în continuare „strategia”) până la 17 ianuarie 2026. Strategia stabilește obiective strategice și măsuri de politică, pe baza strategiilor naționale și sectoriale existente relevante, a planurilor sau a unor documente similare, în vederea atingerii și menținerii unui nivel ridicat de reziliență a entităților critice și care acoperă cel puțin sectoarele prevăzute în anexă.

(2) Fiecare strategie include cel puțin următoarele elemente:

(a) obiectivele strategice și prioritățile în scopul consolidării rezilienței generale a entităților critice, ținând seama de dependențele și interdependențele transfrontaliere și intersectoriale;

(b) un cadru de guvernanță pentru realizarea obiectivelor strategice și a priorităților, inclusiv o descriere a rolurilor și responsabilităților diferitelor autorități, ale entităților critice și ale altor părți implicate în punerea în aplicare a strategiei;

(c) o descriere a măsurilor necesare pentru a consolida reziliența generală a entităților critice, inclusiv o descriere a evaluării riscurilor, astfel cum se menționează la articolul 5;

(d) o descriere a procesului prin care sunt identificate entitățile critice;

(e) o descriere a procesului de sprijinire a entităților critice în conformitate cu prezentul capitol, inclusiv a măsurilor de consolidare a cooperării dintre sectorul public, pe de o parte, și sectorul privat și entitățile publice și private, pe de altă parte;

(f) o listă a principalelor autorități și a părților interesate relevante, altele decât entitățile critice, implicate în punerea în aplicare a strategiei;

(g) un cadru de politică pentru coordonarea dintre autoritățile competente în temeiul prezentei directive (denumite în continuare „autoritățile competente") și autoritățile competente în temeiul Directivei (UE) 2022/2555 în scopul schimbului de informații privind riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice și riscurile, amenințările și incidentele non-cibernetice și al exercitării sarcinilor de supraveghere;

(h) o descriere a măsurilor deja în vigoare menite să faciliteze punerea în aplicare a obligațiilor care le revin în temeiul capitolului III din prezenta directivă de către întreprinderile mici și mijlocii în înțelesul anexei la Recomandarea 2003/361/CE a Comisiei ([31]) pe care statul membru în cauză le-a identificat drept entități critice.

În urma unei consultări care, în măsura în care este posibil din punct de vedere practic, este deschisă părților interesate relevante, statele membre își actualizează strategia cel puțin o dată la fiecare patru ani.

(3) Statele membre transmit Comisiei strategiile și orice actualizări substanțiale ale acestora în termen de trei luni de la adoptarea lor.

Articolul 5

Evaluarea riscurilor efectuată de statul membru

(1) Până la 17 noiembrie 2023, Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 23 pentru a completa prezenta directivă prin stabilirea unei liste neexhaustive a serviciilor esențiale din sectoarele și subsectoarele prevăzute în anexă. Autoritățile competente utilizează respectiva listă de servicii esențiale în scopul efectuării unei evaluări a riscurilor (denumită în continuare „evaluarea riscurilor efectuată de statul membru") până la 17 ianuarie 2026 și, ulterior, ori de câte ori este necesar, dar cel puțin o dată la fiecare patru ani. Autoritățile competente utilizează evaluarea riscurilor efectuată de statul membru pentru a identifica entitățile critice în conformitate cu articolul 6 și pentru a le sprijini în ceea ce privește luarea măsurilor prevăzute la articolul 13.

Evaluarea riscurilor efectuată de statul membru ia în considerare riscurile naturale și cele provocate de om relevante, inclusiv cele de ordin intersectorial sau transfrontalier, accidentele, dezastrele naturale, situațiile de urgență din domeniul sănătății publice și amenințările hibride, sau alte amenințări antagoniste, inclusiv infracțiunile de terorism prevăzute de Directiva (UE) 2017/541 a Parlamentului European și a Consiliului ([32]).

(2) La evaluarea riscurilor efectuată de statul membru, statele membre iau în considerare cel puțin următoarele:

(a) evaluarea generală a riscurilor efectuată în temeiul articolului 6 alineatul (1) din Decizia nr. 1313/2013/UE;

(b) alte evaluări relevante ale riscurilor, efectuate în conformitate cu cerințele actelor sectoriale relevante din dreptul Uniunii, inclusiv Regulamentele (UE) 2017/1938 ([33]) și (UE) 2019/941 ([34]) ale Parlamentului European și ale Consiliului și Directivele 2007/60/CE ([35]) și 2012/18/UE ([36]) ale Parlamentului European și ale Consiliului;

([31]) Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definiția microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

([32]) Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

([33]) Regulamentul (UE) 2017/1938 al Parlamentului European și al Consiliului din 25 octombrie 2017 privind măsurile de garantare a siguranței furnizării de gaze și de abrogare a Regulamentului (UE) nr. 994/2010 (JO L 280, 28.10.2017, p. 1).

([34]) Regulamentul (UE) 2019/941 al Parlamentului European și al Consiliului din 5 iunie 2019 privind pregătirea pentru riscuri în sectorul energiei electrice și de abrogare a Directivei 2005/89/CE (JO L 158, 14.6.2019, p. 1).

([35]) Directiva 2007/60/CE a Parlamentului European și a Consiliului din 23 octombrie 2007 privind evaluarea și gestionarea riscurilor de inundații (JO L 288, 6.11.2007, p. 27).

([36]) Directiva 2012/18/UE a Parlamentului European și a Consiliului din 4 iulie 2012 privind controlul pericolelor de accidente majore care implică substanțe periculoase, de modificare și ulterior de abrogare a Directivei 96/82/CE a Consiliului (JO L 197, 24.7.2012, p. 1).

(c) riscurile relevante care decurg din gradul de dependență existentă între sectoarele prevăzute în anexă, inclusiv din gradul de dependență a acestora de entități situate în alte state membre și în țări terțe, și impactul pe care o perturbare semnificativă într-un sector îl poate avea asupra altor sectoare, inclusiv orice risc semnificativ la adresa cetățenilor sau a pieței interne;

(d) orice informații privind incidentele notificate în conformitate cu articolul 15.

În sensul primului paragraf litera (c), statele membre cooperează cu autoritățile competente din alte state membre și, după caz, cu autoritățile competente din țări terțe.

(3) Statele membre pun la dispoziția entităților critice pe care le-au identificat în conformitate cu articolul 6 elementele relevante ale evaluării riscurilor efectuată de statul membru, după caz, prin intermediul punctelor unice de contact. Statele membre se asigură că informațiile furnizate entităților critice vin în sprijinul acestora în evaluarea riscurilor efectuată de acestea în temeiul articolului 12 și în luarea unor măsuri care să le asigure reziliența în temeiul articolului 13.

(4) În termen de trei luni de la evaluarea riscurilor efectuată de statul membru, un stat membru furnizează Comisiei informațiile relevante privind tipurile de riscuri identificate și rezultatele respectivei evaluări a riscurilor efectuată de statul membru, pentru fiecare sector și subsector prevăzut în anexă.

(5) Comisia, în cooperare cu statele membre, elaborează un model comun de raportare voluntar care să poată fi utilizat pentru asigurarea conformității cu alineatul (4).

Articolul 6

Identificarea entităților critice

(1) Până la 17 iulie 2026, fiecare stat membru identifică entitățile critice pentru sectoarele și subsectoarele prevăzute în anexă.

(2) Atunci când identifică entitățile critice în temeiul alineatului (1), un stat membru ia în considerare rezultatele propriei evaluări a riscurilor efectuată de statul membru și strategia sa și aplică cumulativ următoarele criterii:

(a) entitatea furnizează unul sau mai multe servicii esențiale;

(b) entitatea operează, și infrastructura sa critică este situată, pe teritoriul statului membru respectiv; și

(c) un incident ar avea efecte perturbatoare semnificative, determinate în conformitate cu articolul 7 alineatul (1), asupra furnizării de către o entitate a unuia sau mai multor servicii esențiale ori asupra furnizării altor servicii esențiale în sectoarele prevăzute în anexă care depind de acel serviciu esențial sau de acele servicii esențiale.

(3) Fiecare stat membru stabilește o listă a entităților critice identificate în temeiul alineatului (2) și se asigură că respectivele entități critice sunt notificate cu privire la identificarea lor ca entități critice în termen de o lună de la identificarea respectivă. Statele membre informează entitățile critice respective cu privire la obligațiile care le revin în temeiul capitolelor III și IV și cu privire la data de la care obligațiile respective le revin, fără a aduce atingere articolului 8. Statele membre informează entitățile critice din sectoarele prevăzute la punctele 3, 4 și 8 din tabelul din anexă cu privire la faptul că nu le revin obligații în temeiul capitolelor III și IV, cu excepția cazului în care norme naționale prevăd altfel.

Capitolul III se aplică entităților critice vizate după 10 luni de la data notificării menționate la primul paragraf de la prezentul alineat.

(4) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive notifică autorităților competente în temeiul Directivei (UE) 2022/2555 identitatea entităților critice pe care le-au identificat în temeiul prezentului articol, în termen de o lună de la identificarea respectivă. Notificarea respectivă specifică, dacă este cazul, că entitățile critice vizate sunt entități din sectoarele prevăzute la punctele 3, 4 și 8 din tabelul din anexa la prezenta directivă și că acestora nu le revin obligații în temeiul capitolelor III și IV din prezenta directivă.

(5) Atunci când este necesar și, în orice caz, cel puțin o dată la fiecare patru ani, statele membre revizuiesc și, după caz, actualizează lista entităților critice identificate menționate la alineatul (3). În cazul în care actualizările respective conduc la identificarea unor entități critice suplimentare, acelor entități critice suplimentare li se aplică alineatele (3) și (4). În plus, statele membre se asigură că entitățile care nu mai sunt identificate ca entități critice în urma unei astfel de actualizări sunt notificate în timp util cu privire la aceasta și cu privire la faptul că, de la primirea notificării respective, nu le mai revin obligațiile prevăzute în capitolul III.

(6) Comisia, în cooperare cu statele membre, elaborează recomandări și orientări fără caracter obligatoriu pentru a sprijini statele membre în identificarea entităților critice.

Articolul 7

Efect perturbator semnificativ

(1) La determinarea importanței unui efect perturbator astfel cum se menționează la articolul 6 alineatul (2) litera (c), statele membre țin cont de următoarele criterii:

(a) numărul de utilizatori care se bazează pe serviciul esențial furnizat de entitatea în cauză;

(b) gradul de dependență al altor sectoare și subsectoare prevăzute în anexă de serviciul esențial respectiv;

(c) efectele pe care l-ar putea avea incidentele, ca intensitate și durată, asupra activităților economice și societale, a mediului, a siguranței și securității publice, sau a sănătății populației;

(d) cota de piață a entității pe piața serviciului esențial sau a serviciilor esențiale respective;

(e) zona geografică ce ar putea fi afectată de un incident, inclusiv eventualele efecte transfrontaliere, ținând seama de vulnerabilitatea asociată cu gradul de izolare al anumitor tipuri de zone geografice, cum ar fi regiunile insulare, regiunile îndepărtate sau zonele montane;

(f) importanța entității pentru menținerea unui nivel suficient al serviciului esențial, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului esențial respectiv.

(2) După identificarea entităților critice în temeiul articolului 6 alineatul (1), fiecare stat membru transmite fără întârziere Comisiei următoarele informații:

(a) o listă a serviciilor esențiale în respectivul stat membru atunci când există servicii esențiale suplimentare față de cele care figurează în lista serviciilor esențiale menționată la articolul 5 alineatul (1);

(b) numărul de entități critice identificate pentru fiecare sector și subsector prevăzut în anexă și pentru fiecare serviciu esențial;

(c) orice praguri aplicate pentru a specifica unul sau mai multe dintre criteriile de la alineatul (1).

Pragurile menționate la primul paragraf litera (c) pot fi prezentate ca atare sau sub formă agregată.

Ulterior, statele membre transmit informațiile menționate la primul paragraf ori de câte ori este necesar și cel puțin o dată la fiecare patru ani.

(3) După consultarea Grupului privind reziliența entităților critice menționat la articolul 19, Comisia adoptă orientări fără caracter obligatoriu pentru a facilita aplicarea criteriilor menționate la alineatul (1) de la prezentul articol, ținând seama de informațiile menționate la alineatul (2) de la prezentul articol.

Articolul 8

Entități critice din sectorul bancar, sectorul infrastructurii pieței financiare și sectorul infrastructurii digitale

Statele membre se asigură că articolul 11 și capitolele III, IV și VI nu se aplică entităților critice pe care le-au identificat din sectoarele prevăzute la punctele 3, 4 și 8 din tabelul din anexă. Statele membre pot adopta sau menține dispoziții de drept intern pentru a atinge un nivel mai ridicat de reziliență pentru entitățile critice respective, cu condiția ca respectivele dispoziții să fie coerente cu dreptul aplicabil al Uniunii.

Articolul 9

Autoritățile competente și punctul unic de contact

(1) Fiecare stat membru desemnează sau înființează una sau mai multe autorități competente responsabile cu aplicarea corectă și, după caz, cu asigurarea respectării dispozițiilor prezentei directive la nivel național.

În ceea ce privește entitățile critice din sectoarele prevăzute la punctele 3 și 4 din tabelul din anexa la prezenta directivă, autoritățile competente sunt, în principiu, autoritățile competente menționate la articolul 46 din Regulamentul (UE) 2022/2554. În ceea ce privește entitățile critice din sectorul prevăzut la punctul 8 din tabelul din anexa la prezenta directivă, autoritățile competente sunt, în principiu, autoritățile competente în temeiul Directivei (UE) 2022/2555. Statele membre pot desemna o altă autoritate competentă pentru sectoarele prevăzute la punctele 3 și 4 din tabelul din anexa la prezenta directivă, în conformitate cu cadrele naționale existente.

În cazul în care desemnează sau înființează mai multe autorități competente, statele membre stabilesc în mod clar sarcinile care revin fiecăreia dintre autoritățile în cauză și se asigură că acestea cooperează în mod eficace în vederea îndeplinirii sarcinilor care le revin în temeiul prezentei directive, inclusiv în ceea ce privește desemnarea și activitățile punctului unic de contact menționat la alineatul (2).

(2) Fiecare stat membru desemnează sau înființează un punct unic de contact care să exercite o funcție de legătură pentru a asigura cooperarea transfrontalieră cu punctele unice de contact ale altor state membre și cu Grupul privind reziliența entităților critice menționat la articolul 19 (denumit în continuare „punctul unic de contact"). După caz, un stat membru desemnează punctul său unic de contact în cadrul unei autorități competente. După caz, un stat membru poate dispune ca punctul său unic de contact să exercite și o funcție de legătură cu Comisia și să asigure cooperarea cu țările terțe.

(3) Până la 17 iulie 2028 și, ulterior, la fiecare doi ani, punctele unice de contact prezintă Comisiei și Grupului privind reziliența entităților critice menționat la articolul 19 un raport de sinteză privind notificările pe care le-au primit, inclusiv cu privire la numărul de notificări, natura incidentelor notificate și măsurile luate în conformitate cu articolul 15 alineatul (3).

Comisia, în cooperare cu Grupul privind reziliența entităților critice, elaborează un model comun de raportare. Autoritățile competente pot utiliza în mod voluntar modelul comun de raportare în scopul transmiterii rapoartelor de sinteză menționate la primul paragraf.

(4) Fiecare stat membru se asigură că autoritatea sa competentă și punctul unic de contact dețin competențele și resursele financiare, umane și tehnice adecvate pentru a îndeplini, în mod eficace și eficient, sarcinile care le sunt încredințate.

(5) Fiecare stat membru se asigură că autoritatea sa competentă se consultă și cooperează, după caz și în conformitate cu dreptul Uniunii și cu dreptul intern, cu alte autorități naționale relevante, inclusiv cu cele responsabile de protecția civilă, de asigurarea respectării legii și de protecția datelor cu caracter personal, precum și cu entitățile critice și cu părțile interesate relevante.

(6) Fiecare stat membru se asigură că autoritatea sa competentă în temeiul prezentei directive cooperează și face schimb de informații cu autoritățile competente în temeiul Directivei (UE) 2022/2555 în ceea ce privește riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice, precum și riscurile, amenințările și incidentele non-cibernetice care afectează entitățile critice, precum și în ceea ce privește măsurile relevante luate de autoritatea competentă și de autoritățile competente în temeiul Directivei (UE) 2022/2555.

(7) Fiecare stat membru notifică Comisiei desemnarea sau înființarea autorității competente și a punctului unic de contact în termen de trei luni de la desemnarea sau înființarea acestora, inclusiv sarcinile și responsabilitățile care le revin în temeiul prezentei directive, datele lor de contact și orice modificare ulterioară a acestora. Statele membre informează Comisia cu privire la decizia de a desemna o altă autoritate decât autoritățile competente menționate la alineatul (1) al doilea paragraf drept autoritate competentă în ceea ce privește entitățile critice din sectoarele prevăzute la punctele 3, 4 și 8 din tabelul din anexă. Fiecare stat membru face publică identitatea autorității sale competente și a punctului său unic de contact.

(8) Comisia întocmește și publică o listă a punctelor unice de contact.

Articolul 10

Sprijinul acordat de statele membre entităților critice

(1) Statele membre acordă sprijin entităților critice în vederea consolidării rezilienței acestora. Sprijinul respectiv poate include elaborarea de materiale de orientare și metodologii, sprijinul pentru organizarea de exerciții pentru a testa reziliența acestor entități și furnizarea de consiliere și formare personalului entităților critice. Fără a aduce atingere normelor aplicabile privind ajutoarele de stat, statele membre pot furniza resurse financiare entităților critice, atunci când acest lucru este necesar și justificat de obiective de interes public.

(2) Fiecare stat membru se asigură că autoritatea sa competentă cooperează și face schimb de informații și de bune practici cu entitățile critice din sectoarele prevăzute în anexă.

(3) Statele membre facilitează schimbul voluntar de informații între entitățile critice în ceea ce privește aspectele reglementate de prezenta directivă, în conformitate cu dreptul Uniunii și cu dreptul intern privind, în special, informațiile clasificate și sensibile, concurența și protecția datelor cu caracter personal.

Articolul 11

Cooperarea dintre statele membre

(1) Statele membre se consultă reciproc cu privire la entitățile critice, ori de câte ori acest lucru este necesar, în scopul asigurării aplicării consecvente a prezentei directive. Consultările respective au loc în special în ceea ce privește entitățile critice:

(a) care utilizează o infrastructură critică conectată fizic între două sau mai multe state membre;

(b) care fac parte din structuri corporative conectate cu entități critice din alte state membre sau legate de acestea;

(c) care au fost identificate drept entități critice într-un stat membru și furnizează servicii esențiale pentru alte state membre sau pe teritoriul acestora.

(2) Consultările menționate la alineatul (1) vizează consolidarea rezilienței entităților critice și, acolo unde este posibil, reducerea sarcinii administrative care incumbă acestora.

CAPITOLUL III

REZILIENȚA ENTITĂȚILOR CRITICE

Articolul 12

Evaluarea riscurilor efectuată de entitățile critice

(1) Prin excepție de la termenul prevăzut la articolul 6 alineatul (3) al doilea paragraf, statele membre se asigură că entitățile critice efectuează o evaluare a riscurilor în termen de nouă luni după primirea notificării menționate la articolul 6 alineatul (3) și, ulterior, ori de câte ori este necesar dar cel puțin o dată la fiecare patru ani, pe baza evaluărilor riscurilor efectuate de statele membre și a altor surse relevante de informații, în vederea evaluării tuturor riscurilor relevante care ar putea perturba furnizarea serviciilor lor esențiale (denumită în continuare „evaluarea riscurilor efectuată de entitatea critică”).

(2) Evaluarea riscurilor efectuată de entitatea critică ține seama de toate riscurile naturale și de cele provocate de om care ar putea provoca producerea unui incident, inclusiv cele intersectoriale sau transfrontaliere, accidentele, dezastrele naturale, situațiile de urgență din domeniul sănătății publice și amenințările hibride, precum și alte amenințări antagoniste, inclusiv infracțiunile de terorism prevăzute de Directiva (UE) 2017/541. Evaluarea riscurilor efectuată de entitatea critică ține seama de gradul de dependență al altor sectoare prevăzute în anexă față de serviciul esențial furnizat de entitatea critică și gradul de dependență al entității critice față de serviciile esențiale furnizate de alte entități în sectoarele respective inclusiv, după caz, în statele membre și țările terțe învecinate.

În cazul în care o entitate critică a efectuat alte evaluări ale riscurilor sau a întocmit documente în temeiul obligațiilor prevăzute în alte acte de drept care sunt relevante pentru evaluarea riscurilor efectuată de entitatea critică, aceasta poate utiliza evaluările și documentele respective pentru a îndeplini cerințele prevăzute la prezentul articol. Atunci când își exercită funcțiile de supraveghere, autoritatea competentă poate declara o evaluare existentă a riscurilor efectuată de o entitate critică care abordează riscurile și gradul de dependență menționate la primul paragraf de la prezentul alineat ca fiind conformă, integral sau parțial, cu obligațiile prevăzute la prezentul articol.

Articolul 13

Măsuri de reziliență luate de entitățile critice

(1) Statele membre se asigură că entitățile critice iau măsuri tehnice, de securitate și organizatorice adecvate și proporționale pentru a-și asigura reziliența, pe baza informațiilor relevante furnizate de statele membre în evaluarea riscurilor efectuată de statul membru precum și a rezultatelor evaluării riscurilor efectuată de entitatea critică, inclusiv măsuri necesare pentru:

(a) a preveni apariția incidentelor, luând în considerare în mod corespunzător măsuri de reducere a riscului de dezastre și de adaptare la schimbările climatice;

(b) a asigura o protecție fizică adecvată a spațiilor și a infrastructurii critice, luând în considerare în mod corespunzător de exemplu instalarea de garduri, bariere, instrumente și proceduri de monitorizare a perimetrului, echipamente pentru detectarea și controlul accesului;

(c) a răspunde, a rezista la consecințele incidentelor și a le atenua, luând în considerare în mod corespunzător implementarea unor proceduri și protocoale de gestionare a riscurilor și a crizelor și a unor proceduri de alertă;

(d) a se redresa în urma incidentelor, luând în considerare în mod corespunzător măsuri de asigurare a continuității activității și identificarea unor lanțuri de aprovizionare alternative, pentru a relua furnizarea serviciului esențial;

(e) a asigura gestionarea adecvată a securității în ceea ce privește angajații, luând în considerare în mod corespunzător măsuri precum determinarea categoriilor de personal care exercită funcții critice, stabilirea drepturilor de acces la spații, la infrastructura critică și la informațiile sensibile, stabilirea de proceduri de verificare a antecedentelor în conformitate cu articolul 14, desemnarea unor categorii de persoane care trebuie să facă obiectul unor astfel de verificări ale antecedentelor, precum și stabilirea unor cerințe de formare și calificări adecvate;

(f) a conștientiza personalul relevant cu privire la măsurile menționate la literele (a)-(e), luând în considerare în mod corespunzător cursuri de formare, materiale informative și exerciții.

În sensul literei (e) de la primul paragraf, statele membre se asigură că entitățile critice iau în considerare, atunci când determină categoriile de personal care exercită funcții critice, personalul prestatorilor externi de servicii.

(2) Statele membre se asigură că entitățile critice instituie și pun în aplicare un plan de reziliență sau un document sau documente echivalente, care descriu măsurile luate în temeiul alineatului (1). Atunci când entitățile critice au elaborat documente sau au luat măsuri în temeiul obligațiilor stabilite în alte acte de drept care sunt relevante pentru măsurile menționate la alineatul (1), acestea pot utiliza documentele și măsurile respective pentru a îndeplini cerințele prevăzute la prezentul articol. Atunci când își exercită funcțiile de supraveghere, autoritatea competentă poate declara măsurile existente de consolidare a rezilienței luate de o entitate critică, care abordează în mod adecvat și proporțional măsurile tehnice, de securitate și organizatorice menționate la alineatul (1), ca fiind conforme, integral sau parțial, cu obligațiile prevăzute la prezentul articol.

(3) Statele membre se asigură că fiecare entitate critică desemnează un ofițer de legătură sau un echivalent al acestuia ca punct de contact în relația cu autoritățile competente.

(4) La cererea statului membru care a identificat entitatea critică și cu acordul entității critice în cauză, Comisia organizează misiuni de consiliere, conform modalităților stabilite la articolul 18 alineatele (6), (8) și (9), pentru a oferi consultanță entității critice în cauză în vederea îndeplinirii obligațiilor care îi revin în temeiul capitolului III. Misiunea de consiliere raportează constatările sale Comisiei, statului membru respectiv și entității critice în cauză.

(5) După consultarea Grupului privind reziliența entităților critice menționat la articolul 19, Comisia adoptă orientări fără caracter obligatoriu pentru a detalia măsurile tehnice, de securitate și organizatorice care pot fi luate în temeiul alineatului (1) de la prezentul articol.

(6) Comisia adoptă acte de punere în aplicare pentru a stabili specificațiile tehnice și metodologice necesare privind aplicarea măsurilor menționate la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 24 alineatul (2).

Articolul 14

Verificările antecedentelor

(1) Statele membre precizează condițiile în care unei entități critice i se permite, în cazuri justificate în mod corespunzător și ținând seama de evaluarea riscurilor efectuată de statul membru, să depună cereri de verificare a antecedentelor persoanelor care:

(a) îndeplinesc roluri sensibile în cadrul entității critice sau în beneficiul acesteia, în special în ceea ce privește reziliența entității critice;

(b) sunt autorizate să aibă acces direct sau de la distanță în spațiile acesteia, la informațiile sale sau la sistemele sale de control, inclusiv în legătură cu securitatea entității critice;

(c) sunt avute în vedere pentru a fi recrutate în posturi care intră sub incidența criteriilor prevăzute la litera (a) sau (b).

(2) Cererile menționate la alineatul (1) de la prezentul articol sunt evaluate într-un termen rezonabil și prelucrate în conformitate cu dreptul și procedurile interne, precum și cu dreptul relevant și aplicabil al Uniunii, inclusiv cu Regulamentul (UE) 2016/679 și cu Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([37]). Verificările antecedentelor sunt proporționale și strict limitate la ceea ce este necesar. Acestea se efectuează exclusiv în scopul evaluării unui potențial risc de securitate pentru entitatea critică în cauză.

(3) O verificare a antecedentelor menționată la alineatul (1) îndeplinește cel puțin următoarele:

(a) confirmă identitatea persoanei care face obiectul verificării antecedentelor;

(b) verifică cazierul judiciar al persoanei vizate în ceea ce privește infracțiunile care ar fi relevante pentru o anumită funcție.

Atunci când efectuează verificarea antecedentelor, pentru a obține informații din cazierele judiciare păstrate în alte state membre, statele membre utilizează Sistemul european de informații cu privire la cazierele judiciare, în conformitate cu procedurile prevăzute în Decizia-cadru 2009/315/JAI și, dacă este relevant și aplicabil, în Regulamentul (UE) 2019/816. Autoritățile centrale prevăzute la articolul 3 alineatul (1) din Decizia-cadru 2009/315/JAI și la articolul 3 punctul 5 din Regulamentul (UE) 2019/816 răspund acestor cereri de informații în termen de 10 zile lucrătoare de la data primirii cererii, în conformitate cu articolul 8 alineatul (1) din Decizia-cadru 2009/315/JAI.

([37]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

Articolul 15

Notificarea incidentelor

(1) Statele membre se asigură că entitățile critice notifică fără întârzieri nejustificate autorității competente incidentele care perturbă în mod semnificativ sau care au potențialul de a perturba în mod semnificativ furnizarea serviciilor esențiale. Cu excepția cazului în care nu sunt în măsură din punct de vedere operațional să facă acest lucru, statele membre se asigură că entitățile critice transmit o notificare inițială în cel mult 24 de ore de la constatarea unui incident, urmată, după caz, de un raport detaliat prezentat ulterior în cel mult o lună. Pentru a determina importanța perturbării, se iau în considerare, în special, următorii parametri:

(a) numărul și proporția utilizatorilor afectați de perturbare;

(b) durata perturbării;

(c) zona geografică afectată de perturbare, ținând seama de eventuala izolare geografică a zonei respective.

În cazul unui incident care are sau ar putea avea un efect semnificativ asupra continuității furnizării de servicii esențiale pentru șase sau mai multe state membre sau pe teritoriul acestora, autoritățile competente ale statelor membre afectate de incident notifică incidentul respectiv Comisiei.

(2) Notificările menționate la primul paragraf de la alineatul (1) includ toate informațiile disponibile de care autoritatea competentă are nevoie pentru a înțelege natura, cauza și posibilele consecințe ale incidentului, inclusiv toate informațiile necesare pentru a determina orice efect transfrontalier al incidentului. Notificările respective nu agravează răspunderea entităților critice.

(3) Pe baza informațiilor furnizate de entitatea critică în notificarea menționată la alineatul (1), autoritatea competentă relevantă informează, prin intermediul punctului unic de contact, punctul unic de contact al altor state membre afectate dacă incidentul are sau ar putea avea un efect semnificativ asupra entităților critice și asupra continuității furnizării de servicii esențiale pentru unul sau mai multe alte state membre sau pe teritoriul acestora.

Atunci când transmit sau recepționează informații în temeiul primului paragraf, punctele unice de contact, tratează informațiile într-un mod care respectă confidențialitatea acestora și protejează securitatea și interesele comerciale ale entității critice în cauză, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(4) Cât mai rapid posibil în urma notificării menționate la alineatul (1), autoritatea competentă relevantă furnizează entității critice în cauză informații complementare relevante, inclusiv informații care ar putea contribui la răspunsul eficace al entității critice la incidentul în cauză. Statele membre informează publicul în cazul în care consideră că aceasta ar fi de interes public.

Articolul 16

Standarde

Pentru a promova punerea în aplicare convergentă a prezentei directive, statele membre încurajează, în cazul în care acest lucru este util și fără a impune sau a discrimina în favoarea utilizării unui anumit tip de tehnologie, utilizarea standardelor și specificațiilor tehnice europene și internaționale care sunt pertinente pentru măsurile de securitate și cele de reziliență aplicabile entităților critice.

CAPITOLUL IV

ENTITĂȚI CRITICE DE IMPORTANȚĂ EUROPEANĂ DEOSEBITĂ

Articolul 17

Identificarea entităților critice de importanță europeană deosebită

(1) O entitate este considerată entitate critică de importanță europeană deosebită atunci când:

(a) a fost identificată ca entitate critică în temeiul articolului 6 alineatul (1);

(b) furnizează servicii esențiale identice sau similare pentru șase sau mai multe state membre sau pe teritoriul acestora; și

(c) a fost notificată în temeiul alineatului (3) de la prezentul articol.

(2) Statele membre se asigură că, în urma notificării menționate la articolul 6 alineatul (3), o entitate critică informează autoritatea sa competentă atunci când furnizează servicii esențiale pentru șase sau mai multe state membre sau pe teritoriul acestora. În acest caz, statele membre se asigură că entitatea critică informează autoritatea sa competentă care sunt serviciile esențiale pe care le furnizează acelor state membre și care sunt statele membre cărora sau pe teritoriul cărora furnizează serviciile esențiale respective. Statele membre notifică Comisiei, fără întârzieri nejustificate, identitatea entităților critice în cauză și informațiile puse la dispoziție în temeiul prezentului alineat.

Comisia se consultă cu autoritatea competentă a statului membru care a identificat o entitate critică menționată la primul paragraf, cu autoritățile competente ale celorlalte state membre în cauză, precum și cu entitatea critică în cauză. În cadrul acestor consultări, fiecare stat membru comunică Comisiei dacă consideră că serviciile care îi sunt furnizate de entitatea critică sunt servicii esențiale.

(3) În cazul în care, pe baza consultărilor prevăzute la alineatul (2) de la prezentul articol, Comisia constată că entitatea critică în cauză furnizează servicii esențiale pentru șase sau mai multe state membre sau pe teritoriul acestora, aceasta notifică entității în cauză, prin intermediul autorității sale competente, faptul că este considerată o entitate critică de importanță europeană deosebită, informând-o cu privire la obligațiile care îi revin în temeiul prezentului capitol și cu privire la data de la care obligațiile respective i se aplică. De îndată ce Comisia a informat autoritatea competentă cu privire la decizia sa de a considera o entitate drept entitate critică de importanță europeană deosebită, autoritatea competentă transmite notificarea, fără întârzieri nejustificate, respectivei entități critice.

(4) Prezentul capitol se aplică respectivei entități critice de importanță europeană deosebită de la data primirii notificării menționate la alineatul (3) de la prezentul articol.

Articolul 18

Misiuni de consiliere

(1) La cererea unui stat membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1), Comisia poate organiza o misiune de consiliere în vederea evaluării măsurilor puse în aplicare de entitatea în cauză pentru a-și îndeplini obligațiile în temeiul capitolului III.

(2) Din proprie inițiativă sau la cererea unuia sau a mai multor state membre cărora sau pe teritoriul cărora este furnizat serviciul esențial, Comisia poate organiza, de asemenea, o misiune de consiliere menționată la alineatul (1) de la prezentul articol, cu condiția ca statul membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1) să fie de acord.

(3) La cererea motivată a Comisiei sau a unuia sau mai multor state membre cărora sau pe teritoriul cărora este furnizat serviciul esențial, statul membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1) pune la dispoziția Comisiei:

(a) părțile relevante ale evaluării riscurilor efectuate;

(b) o listă a măsurilor luate în conformitate cu articolul 13;

(c) măsurile de supraveghere sau de asigurare a respectării legislației, inclusiv evaluări ale conformității sau ordine emise, pe care autoritatea sa competentă le-a întreprins în temeiul articolelor 21 și 22 cu privire la entitatea critică respectivă.

(4) Misiunea de consiliere raportează constatările sale Comisiei, statului membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1), statelor membre cărora sau pe teritoriul cărora este furnizat serviciul esențial și entității critice în cauză în termen de trei luni de la încheierea misiunii de consiliere.

Statele membre cărora sau pe teritoriul cărora este furnizat serviciul esențial analizează raportul menționat la primul paragraf și, dacă este necesar, își transmit Comisiei opinia cu privire la respectarea sau nerespectarea de către entitatea critică de importanță europeană deosebită în cauză a obligațiilor care îi revin în temeiul capitolului III și, după caz, cu privire la măsurile care ar putea fi luate pentru a îmbunătăți reziliența entității critice respective.

Pe baza opiniei menționate la al doilea paragraf de la prezentul alineat, Comisia transmite statului membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1), statelor membre cărora sau pe teritoriul cărora este furnizat serviciul esențial și entității critice în cauză avizul său cu privire la respectarea sau nerespectarea de către entitatea critică în cauză a obligațiilor care îi revin în temeiul capitolului III și, după caz, cu privire la măsurile care ar putea fi luate pentru a îmbunătăți reziliența entității critice respective.

Statul membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1) se asigură că autoritatea sa competentă și entitatea critică în cauză țin seama în mod corespunzător de avizul menționat la al treilea paragraf de la prezentul alineat și furnizează informații Comisiei și statelor membre cărora sau pe teritoriul cărora este furnizat serviciul esențial cu privire la măsurile pe care le-a luat în temeiul avizului respectiv.

(5) Fiecare misiune de consiliere este alcătuită din experți ai statului membru în care este situată entitatea critică de importanță europeană deosebită, din experți ai statelor membre cărora sau pe teritoriul cărora este furnizat serviciul esențial și din reprezentanți ai Comisiei. Statele membre respective pot propune candidați care să facă parte dintr-o misiune de consiliere. În urma consultărilor cu statul membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1), Comisia selectează și numește membrii fiecărei misiuni de consiliere în funcție de capacitatea lor profesională, asigurând, dacă este posibil, o reprezentare echilibrată din punct de vedere geografic a tuturor statelor membre interesate. Ori de câte ori este necesar, membrii misiunii de consiliere dețin o autorizare de securitate valabilă și adecvată. Comisia suportă costurile legate de participarea la misiunea de consiliere.

Comisia organizează programul fiecărei misiuni de consiliere în consultare cu membrii respectivei misiuni de consiliere și în acord cu statul membru care a identificat o entitate critică de importanță europeană deosebită ca entitate critică în temeiul articolului 6 alineatul (1).

(6) Comisia adoptă un act de punere în aplicare prin care sunt stabilite norme procedurale cu privire la cererile de organizare a misiunilor de consiliere și la tratarea acestor cereri, la desfășurarea misiunilor de consiliere și la rapoartele prezentate de acestea, precum și la gestionarea comunicării cu privire la avizul Comisiei menționat la alineatul (4) al treilea paragraf de la prezentul articol și la măsurile luate, ținând seama în mod corespunzător de confidențialitatea și de sensibilitatea comercială a informațiilor în cauză. Respectivul act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 24 alineatul (2).

(7) Statele membre se asigură că entitatea critică de importanță europeană deosebită asigură misiunii de consiliere acces la informațiile, sistemele și instalațiile legate de furnizarea serviciilor sale esențiale care sunt necesare pentru desfășurarea misiunii de consiliere.

(8) Misiunile de consiliere se desfășoară în conformitate cu dreptul intern aplicabil al statului membru în care acestea au loc, respectând responsabilitatea statului membru respectiv în ceea ce privește securitatea națională și protecția intereselor sale în materie de securitate.

(9) Atunci când organizează misiuni de consiliere, Comisia ia în considerare rapoartele tuturor inspecțiilor efectuate de Comisie în temeiul Regulamentelor (CE) nr. 725/2004 și (CE) nr. 300/2008, precum și rapoartele privind orice monitorizare efectuată de Comisie în temeiul Directivei 2005/65/CE în ceea ce privește entitatea critică respectivă.

(10) Comisia informează Grupul privind reziliența entităților critice menționat la articolul 19 ori de câte ori se organizează o misiune de consiliere. Statul membru în care are loc misiunea de consiliere și Comisia informează, de asemenea, Grupul privind reziliența entităților critice cu privire la principalele constatări ale misiunii de consiliere și la lecțiile desprinse în vederea promovării învățării reciproce.

CAPITOLUL V

COOPERARE ȘI RAPORTARE

Articolul 19

Grupul privind reziliența entităților critice

(1) În temeiul prezentei directive se constituie Grupul privind reziliența entităților critice. Grupul sprijină Comisia și facilitează cooperarea dintre statele membre și schimbul de informații privind aspectele referitoare la prezenta directivă.

(2) Grupul privind reziliența entităților critice este alcătuit din reprezentanți ai statelor membre și ai Comisiei care dețin autorizarea de securitate, după caz. Dacă este relevant pentru îndeplinirea sarcinilor sale, Grupul privind reziliența entităților critice poate invita părți interesate relevante să participe la lucrările sale. La cererea Parlamentului European, Comisia poate invita, de asemenea, experți ai Parlamentului să participe la reuniunile Grupului privind reziliența entităților critice.

Reprezentantul Comisiei prezidează Grupul privind reziliența entităților critice.

(3) Grupului privind reziliența entităților critice îi revin următoarele sarcini:

(a) să sprijine Comisia în ceea ce privește asistența acordată statelor membre pentru consolidarea capacității acestora de a contribui la asigurarea rezilienței entităților critice în conformitate cu prezenta directivă;

(b) să analizeze strategiile în vederea identificării bunelor practici în ceea ce privește strategiile respective;

(c) să faciliteze schimbul de bune practici în ceea ce privește identificarea entităților critice de către statele membre în temeiul articolului 6 alineatul (1), inclusiv în legătură cu dependențele transfrontaliere și intersectoriale și în ceea ce privește riscurile și incidentele;

(d) după caz, să contribuie, cu privire la aspectele legate de prezenta directivă, la documentele privind reziliența la nivelul Uniunii;

(e) să contribuie la elaborarea orientărilor menționate la articolul 7 alineatul (3) și articolul 13 alineatul (5) și, la cerere, a oricăror acte delegate sau de punere în aplicare adoptate în temeiul prezentei directive;

(f) să analizeze rapoartele de sinteză menționate la articolul 9 alineatul (3) în vederea promovării schimbului de bune practici cu privire la măsurile luate în conformitate cu articolul 15 alineatul (3);

(g) să asigure schimbul de bune practici în legătură cu notificarea incidentelor menționată la articolul 15;

(h) să discute rapoartele de sinteză ale misiunilor de consiliere și lecțiile desprinse în conformitate cu articolul 18 alineatul (10);

(i) să asigure schimbul de informații și de bune practici privind inovarea, cercetarea și dezvoltarea referitoare la reziliența entităților critice, în conformitate cu prezenta directivă;

(j) după caz, să asigure schimbul de informații privind aspecte legate de reziliența entităților critice cu instituțiile, organismele, oficiile și agențiile relevante ale Uniunii.

(4) Până la 17 ianuarie 2025 și, ulterior, la fiecare doi ani, Grupul privind reziliența entităților critice stabilește un program de lucru cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și sarcinilor sale. Programul său de lucru trebuie să fie în concordanță cu cerințele și obiectivele prezentei directive.

(5) Grupul privind reziliența entităților critice se reunește periodic și cel puțin o dată pe an cu grupul de cooperare constituit în temeiul Directivei (UE) 2022/2555 pentru a promova și facilita cooperarea și schimbul de informații.

(6) Comisia poate adopta acte de punere în aplicare prin care sunt stabilite normele procedurale necesare pentru funcționarea Grupului privind reziliența entităților critice, cu respectarea articolului 1 alineatul (4). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 24 alineatul (2).

(7) Comisia prezintă Grupului privind reziliența entităților critice un raport de sinteză privind informațiile furnizate de statele membre în temeiul articolului 4 alineatul (3) și al articolului 5 alineatul (4) până la 17 ianuarie 2027 și, ulterior, atunci când este necesar și cel puțin o dată la fiecare patru ani.

Articolul 20

Sprijinul acordat de Comisie autorităților competente și entităților critice

(1) Comisia sprijină, după caz, statele membre și entitățile critice în vederea îndeplinirii obligațiilor care le revin în temeiul prezentei directive. Comisia elaborează o imagine de ansamblu la nivelul Uniunii a riscurilor transfrontaliere și intersectoriale la adresa furnizării serviciilor esențiale, organizează misiunile de consiliere menționate la articolul 13 alineatul (4) și la articolul 18 și facilitează schimbul de informații între statele membre și experții din întreaga Uniune.

(2) Comisia completează activitățile menționate la articolul 10 ale statelor membre prin elaborarea de bune practici, materiale de orientare și metodologii, precum și prin activități de formare și exerciții transfrontaliere pentru a testa reziliența entităților critice.

(3) Comisia informează statele membre cu privire la resursele financiare la nivelul Uniunii aflate la dispoziția statelor membre pentru consolidarea rezilienței entităților critice.

CAPITOLUL VI

SUPRAVEGHERE ȘI ASIGURAREA RESPECTĂRII LEGISLAȚIEI

Articolul 21

Supraveghere și asigurarea respectării legislației

(1) Pentru a evalua respectarea de către entitățile pe care statele membre le-au identificat drept entități critice în temeiul articolului 6 alineatul (1) a obligațiilor care le revin în temeiul prezentei directive, statele membre se asigură că autoritățile competente dispun de competențele și de mijloacele necesare pentru:

(a) a efectua inspecții *in situ* ale infrastructurii critice și ale spațiilor pe care le utilizează entitatea critică pentru a-și furniza serviciile esențiale, precum și a supraveghea *ex situ* măsurile luate de entitățile critice în conformitate cu articolul 13;

(b) a efectua sau a ordona audituri ale entităților critice respective.

(2) Statele membre se asigură că autoritățile competente dispun de competențele și mijloacele necesare pentru a solicita, atunci când este necesar pentru îndeplinirea sarcinilor care le revin în temeiul prezentei directive, ca entitățile în temeiul Directivei (UE) 2022/2555 pe care statele membre le-au identificat ca entități critice în temeiul prezentei directive să transmită, într-un termen rezonabil stabilit de autoritățile respective:

(a) informațiile necesare pentru a evalua dacă măsurile luate de entitățile respective pentru a-și asigura reziliența îndeplinesc cerințele prevăzute la articolul 13;

(b) dovada punerii în aplicare efective a măsurilor respective, inclusiv rezultatele unui audit efectuat de un auditor independent și calificat selectat de entitatea respectivă și efectuat pe cheltuiala acesteia.

Atunci când solicită aceste informații, autoritățile competente declară scopul solicitării și precizează informațiile solicitate.

(3) Fără a aduce atingere posibilității de a aplica sancțiuni în conformitate cu articolul 22, autoritățile competente pot, în urma acțiunilor de supraveghere menționate la alineatul (1) de la prezentul articol sau după evaluarea informațiilor menționate la alineatul (2) de la prezentul articol, să ordone entităților critice în cauză să ia măsurile necesare și proporționale pentru a remedia orice încălcare identificată a prezentei directive, într-un termen rezonabil stabilit de autoritățile respective, și să furnizeze autorităților respective informații cu privire la măsurile luate. Aceste ordine țin seama, în special, de gravitatea încălcării.

(4) Statele membre se asigură că competențele prevăzute la alineatele (1), (2) și (3) pot fi exercitate numai sub rezerva unor garanții adecvate. Garanțiile respective asigură, în special, faptul că o astfel de exercitare are loc în mod obiectiv, transparent și proporțional și că drepturile și interesele legitime ale entităților critice afectate, cum ar fi protecția secretelor comerciale și de afaceri, sunt protejate în mod corespunzător, inclusiv dreptul acestora de a fi ascultate, dreptul la apărare și dreptul la o cale de atac efectivă în fața unei instanțe independente.

(5) Statele membre se asigură că, atunci când o autoritate competentă în temeiul prezentei directive evaluează în temeiul prezentului articol respectarea de către o entitate critică a obligațiilor care îi revin, autoritatea competentă respectivă informează autoritățile competente în temeiul Directivei (UE) 2022/2555 ale statelor membre interesate. În acest scop, statele membre se asigură că autoritățile competente în temeiul prezentei directive pot solicita autorităților competente în temeiul Directivei (UE) 2022/2555 să își exercite competențele de supraveghere și de asigurare a respectării legislației în legătură cu o entitate care intră sub incidența directivei menționate care a fost identificată drept entitate critică în temeiul prezentei directive. Statele membre se asigură că autoritățile competente în temeiul prezentei directive cooperează și fac schimb de informații în acest scop cu autoritățile competente în temeiul Directivei (UE) 2022/2555.

Articolul 22

Sancțiuni

Statele membre adoptă normele privind sancțiunile care se aplică în cazul nerespectării dispozițiilor de drept intern adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura aplicarea acestora. Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre notifică normele și măsurile respective Comisiei până la 17 octombrie 2024 și îi comunică acesteia, fără întârziere, orice modificare ulterioară a acestora.

CAPITOLUL VII

ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 23

Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Competența de a adopta acte delegate menționată la articolul 5 alineatul (1) se conferă Comisiei pe o perioadă de cinci ani, începând cu 16 ianuarie 2023.

(3) Delegarea de competențe menționată la articolul 5 alineatul (1) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 5 alineatul (1) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 24

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

CAPITOLUL VIII

DISPOZIȚII FINALE

Articolul 25

Raportare și revizuire

Până la 17 iulie 2027, Comisia prezintă Parlamentului European și Consiliului un raport în care evaluează măsura în care fiecare stat membru a luat măsurile necesare pentru a se conforma prezentei directive.

Comisia examinează periodic funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul respectiv evaluează în special valoarea adăugată a prezentei directive, impactul acesteia în ceea ce privește asigurarea rezilienței entităților critice, precum și dacă anexa la prezenta directivă ar trebui să fie modificată. Comisia transmite primul raport până la 17 iunie 2029. Comisia ia în considerare documentele relevante ale Grupului privind reziliența entităților critice în scopul raportării în temeiul prezentului articol.

Articolul 26

Transpunere

(1) Statele membre adoptă și publică, până la 17 octombrie 2024, dispozițiile necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta.

Statele membre aplică dispozițiile respective de la 18 octombrie 2024.

(2) Atunci când statele membre adoptă dispozițiile menționate la alineatul (1), acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

Articolul 27

Abrogarea Directivei 2008/114/CE

Directiva 2008/114/CE se abrogă de la 18 octombrie 2024.

Trimiterile la directiva abrogată se interpretează drept trimiteri la prezenta directivă.

Articolul 28

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 29

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Strasbourg, 14 decembrie 2022.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	M. BEK

ANEXĂ

Sectoare, subsectoare și categorii de entități

Sectoare	Subsectoare	Categorii de entități
1. Energie	(a) Energie electrică	— Întreprinderile din domeniul energiei electrice în sensul definiției de la articolul 2 punctul 57 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului ([1]) care îndeplinesc funcția de „furnizare" în sensul definiției de la articolul 2 punctul 12 din directiva respectivă
		— Operatorii de distribuție în sensul definiției de la articolul 2 punctul 29 din Directiva (UE) 2019/944
		— Operatorii de transport și de sistem în sensul definiției de la articolul 2 punctul 35 din Directiva (UE) 2019/944
		— Producătorii în sensul definiției de la articolul 2 punctul 38 din Directiva (UE) 2019/944
		— Operatorii pieței de energie electrică desemnați în sensul definiției de la articolul 2 punctul 8 din Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului ([2])
		— Participanții la piața energiei electrice în sensul definiției de la articolul 2 punctul 25 din Regulamentul (UE) 2019/943 care furnizează serviciile de agregare, de consum dispecerizabil sau de stocare de energie în sensul definiției de la articolul 2 punctele 18, 20 și 59 din Directiva (UE) 2019/944
	(b) Sisteme de încălzire și răcire centralizată	— Operatorii de sisteme de încălzirea sau răcire centralizată în sensul definiției de la articolul 2 punctul 19 din Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului ([3])
	(c) Petrol	— Operatorii de conducte de transport al petrolului
		— Operatorii instalațiilor de producție, de rafinare și de tratare, de depozitare și de transport a petrolului
		— Entitățile centrale de stocare în sensul definiției de la articolul 2 litera (f) din Directiva 2009/119/CE a Consiliului ([4])

Sectoare	Subsectoare	Categorii de entități
	(d) Gaze	— Întreprinderile de furnizare în sensul definiției de la articolul 2 punctul 8 din Directiva 2009/73/CE a Parlamentului European și a Consiliului ([5])
		— Operatorii de distribuție în sensul definiției de la articolul 2 punctul 6 din Directiva 2009/73/CE
		— Operatorii de transport și de sistem în sensul definiției de la articolul 2 punctul 4 din Directiva 2009/73/CE
		— Operatorii de înmagazinare în sensul definiției de la articolul 2 punctul 10 din Directiva 2009/73/CE
		— Operatorii de sistem GNL în sensul definiției de la articolul 2 punctul 12 din Directiva 2009/73/CE
		— Întreprinderile din sectorul gazelor naturale în sensul definiției de la articolul 2 punctul 1 din Directiva 2009/73/CE
		— Operatorii de instalație de rafinare și de tratare a gazelor naturale
	(e) Hidrogen	— Operatorii de producție, stocare și transport de hidrogen
2. Transporturi	(a) Transport aerian	— Transportatorii aerieni în sensul definiției de la articolul 3 punctul 4 din Regulamentul (CE) nr. 300/2008 care operează în scop comercial
		— Organele de administrare a aeroportului în sensul definiției de la articolul 2 punctul 2 din Directiva 2009/12/CE a Parlamentului European și a Consiliului ([6]), aeroporturile în sensul definiției de la articolul 2 punctul 1 din directiva respectivă, inclusiv aeroporturile din cadrul rețelei centrale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 ([7]), precum și entități care operează instalații auxiliare în cadrul aeroporturilor
		— Operatorii de control al gestionării traficului care prestează serviciile de control al traficului aerian (ATC) în sensul definiției de la articolul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului ([8])

Sectoare	Subsectoare	Categorii de entități
	(b) Transport feroviar	— Administratorii de infrastructură în sensul definiției de la articolul 3 punctul 2 din Directiva 2012/34/UE a Parlamentului European și a Consiliului ([9])
		— Întreprinderile feroviare în sensul definiției de la articolul 3 punctul 1 din Directiva 2012/34/UE și operatorii unor infrastructuri de servicii în sensul definiției de la articolul 3 punctul 12 din directiva respectivă
	(c) Transport pe apă	— Companiile de transport de pasageri și de mărfuri pe ape interioare, maritime și de coastă astfel cum sunt definite în domeniul transportului maritim în anexa I la Regulamentul (CE) nr. 725/2004, cu excepția navelor individuale operate de companiile respective
		— Organismele de gestionare a porturilor în sensul definiției de la articolul 3 punctul 1 din Directiva 2005/65/CE, inclusiv instalațiile portuare ale acestora în sensul definiției de la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, și entitățile care operează lucrări și echipamente în cadrul porturilor
		— Operatorii de servicii de trafic maritim (STM) în sensul definiției de la articolul 3 litera (o) din Directiva 2002/59/CE a Parlamentului European și a Consiliului ([10])
	(d) Transport rutier	— Autoritățile rutiere în sensul definiției de la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei ([11]) responsabile cu controlul gestionării traficului, cu excepția entităților publice în cazul cărora gestionarea traficului sau operarea de sisteme de transport inteligente reprezintă doar o parte neesențială a activității lor generale
		— Operatorii de sisteme de transport inteligente în sensul definiției de la articolul 4 punctul 1 din Directiva 2010/40/UE a Parlamentului European și a Consiliului ([12])
	(e) Transport public	— Operatorii de servicii publice în sensul definiției de la articolul 2 litera (d) din Regulamentul (CE) nr. 1370/2007 al Parlamentului European și al Consiliului ([13])
3. Sectorul bancar		— Instituțiile de credit în sensul definiției de la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013
4. Infrastructuri ale pieței financiare		— Operatorii de locuri de tranzacționare în sensul definiției de la articolul 4 punctul 24 din Directiva 2014/65/UE
		— Contrapărțile centrale (CPC) în sensul definiției de la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012

Sectoare	Subsectoare	Categorii de entități
5. Sectorul sănătății		— Furnizorii de servicii medicale în sensul definiției de la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului ([14])
		— Laboratoarele de referință ale UE menționate la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului ([15])
		— Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor în sensul definiției de la articolul 1 punctul 2 din Directiva 2001/83/CE a Parlamentului European și a Consiliului ([16])
		— Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în NACE Rev. 2 secțiunea C diviziunea 21
		— Entitățile care fabrică dispozitive medicale considerate esențiale în contextul unei urgențe de sănătate publică („lista dispozitivelor esențiale pentru urgența de sănătate publică") în sensul articolului 22 din Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului ([17])
		— Entitățile titulare ale unei autorizații de distribuție menționate la articolul 79 din Directiva 2001/83/CE
6. Apă potabilă		— Furnizorii și distribuitorii de apă destinată consumului uman în sensul definiției de la articolul 2 punctul 1 litera (a) din Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului ([18]), cu excepția distribuitorilor pentru care distribuția de apă destinată consumului uman reprezintă o parte neesențială din activitatea lor generală de distribuție a altor produse de bază și bunuri
7. Ape uzate		— Întreprinderile care colectează, evacuează sau tratează ape urbane reziduale, ape menajere uzate și ape industriale uzate în sensul definiției de la articolul 2 punctele 1, 2 și 3 din Directiva 91/271/CEE a Consiliului ([19]), cu excepția întreprinderilor pentru care colectarea, evacuarea sau tratarea apelor urbane reziduale, a apelor menajere uzate și a apelor industriale uzate reprezintă o parte neesențială a activității lor generale

Sectoare	Subsectoare	Categorii de entități
8. Infrastructură digitală		— Furnizorii de internet exchange points în sensul definiției de la articolul 6 punctul 18 din Directiva (UE) 2022/2555
		— Furnizorii de servicii DNS în sensul definiției de la articolul 6 punctul 20 din Directiva (UE) 2022/2555, cu excepția operatorilor de servere de nume primare
		— Furnizorii de registre de nume de domenii de prim nivel în sensul definiției de la articolul 6 punctul 21 din Directiva (UE) 2022/2555
		— Furnizorii de servicii de cloud computing în sensul definiției de la articolul 6 punctul 30 din Directiva (UE) 2022/2555
		— Furnizorii de servicii de centre de date în sensul definiției de la articolul 6 punctul 31 din Directiva (UE) 2022/2555
		— Furnizorii de rețele de furnizare de conținut în sensul definiției de la articolul 6 punctul 32 din Directiva (UE) 2022/2555
		— Prestatorii de servicii de încredere în sensul definiției de la articolul 3 punctul 19 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([20])
		— Furnizorii de rețele publice de comunicații electronice în sensul definiției de la articolul 2 punctul 8 din Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului ([21])
		— furnizorii de servicii de comunicații electronice în sensul definiției de la articolul 2 punctul 4 din Directiva (UE) 2018/1972, în măsura în care serviciile acestora sunt destinate publicului
9. Administrație publică		— Entități ale administrației publice din administrația centrală, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern
10. Spațiu		— Operatorii de infrastructură terestră deținută, gestionată și operată de statele membre sau de părți private, care sprijină furnizarea de servicii spațiale, cu excepția furnizorilor de rețele publice de comunicații electronice în sensul definiției de la articolul 2 punctul 8 din Directiva (UE) 2018/1972

Sectoare	Subsectoare	Categorii de entități
11. Producția, prelucrarea și distribuția de alimente		— Întreprinderile cu profil alimentar în sensul definiției de la articolul 3 punctul 2 din Regulamentul (CE) nr. 178/2002 al Parlamentului European și al Consiliului ([22]) care își desfășoară activitatea exclusiv în domeniul logisticii și distribuției angro și al producției și prelucrării industriale la scară largă

([1]) Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).
([2]) Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului din 5 iunie 2019 privind piața internă de energie electrică (JO L 158, 14.6.2019, p. 54).
([3]) Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului din 11 decembrie 2018 privind promovarea utilizării energiei din surse regenerabile (JO L 328, 21.12.2018, p. 82).
([4]) Directiva 2009/119/CE a Consiliului din 14 septembrie 2009 privind obligația statelor membre de a menține un nivel minim de rezerve de țiței și/sau de produse petroliere (JO L 265, 9.10.2009, p. 9).
([5]) Directiva 2009/73/CE a Parlamentului European și a Consiliului din 13 iulie 2009 privind normele comune pentru piața internă în sectorul gazelor naturale și de abrogare a Directivei 2003/55/CE (JO L 211, 14.8.2009, p. 94).
([6]) Directiva 2009/12/CE a Parlamentului European și a Consiliului din 11 martie 2009 privind tarifele de aeroport (JO L 70, 14.3.2009, p. 11).
([7]) Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea rețelei transeuropene de transport și de abrogare a Deciziei nr. 661/2010/UE (JO L 348, 20.12.2013, p. 1).
([8]) Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea Cerului unic european (regulament-cadru) (JO L 96, 31.3.2004, p. 1).
([9]) Directiva 2012/34/UE a Parlamentului European și a Consiliului din 21 noiembrie 2012 privind instituirea spațiului feroviar unic european (JO L 343, 14.12.2012, p. 32).
([10]) Directiva 2002/59/CE a Parlamentului European și a Consiliului din 27 iunie 2002 de instituire a unui sistem comunitar de monitorizare și informare privind traficul navelor maritime și de abrogare a Directivei 93/75/CEE a Consiliului (JO L 208, 5.8.2002, p. 10).
([11]) Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic (JO L 157, 23.6.2015, p. 21).
([12]) Directiva 2010/40/UE a Parlamentului European și a Consiliului din 7 iulie 2010 privind cadrul pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport (JO L 207, 6.8.2010, p. 1).
([13]) Regulamentul (CE) nr. 1370/2007 al Parlamentului European și al Consiliului din 23 octombrie 2007 privind serviciile publice de transport feroviar și rutier de călători și de abrogare a Regulamentelor (CEE) nr. 1191/69 și nr. 1107/70 ale Consiliului (JO L 315, 3.12.2007, p. 1).
([14]) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).
([15]) Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului din 23 noiembrie 2022 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE (JO L 314, 6.12.2022, p. 26).
([16]) Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman (JO L 311, 28.11.2001, p. 67).
([17]) Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului din 25 ianuarie 2022 privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora (JO L 20, 31.1.2022, p. 1).
([18]) Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului din 16 decembrie 2020 privind calitatea apei destinate consumului uman (JO L 435, 23.12.2020, p. 1).
([19]) Directiva 91/271/CEE a Consiliului din 21 mai 1991 privind tratarea apelor urbane reziduale (JO L 135, 30.5.1991, p. 40).
([20]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).
([21]) Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).
([22]) Regulamentul (CE) nr. 178/2002 al Parlamentului European și al Consiliului din 28 ianuarie 2002 de stabilire a principiilor și a cerințelor generale ale legislației alimentare, de instituire a Autorității Europene pentru Siguranța Alimentară și de stabilire a procedurilor în domeniul siguranței produselor alimentare (JO L 31, 1.2.2002, p. 1).

ISSN 1977-0782 (ediție electronică)
ISSN 1830-3625 (ediție tipărită)

Oficiul pentru Publicații
al Uniunii Europene
L-2985 Luxemburg
LUXEMBURG

RO