2024/1772

25.6.2024

REGULAMENTUL DELEGAT (UE) 2024/1772 AL COMISIEI

din 13 martie 2024

de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează criteriile de clasificare a incidentelor legate de TIC și a amenințărilor cibernetice, stabilesc pragurile de semnificație și detaliile rapoartelor privind incidentele majore

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 18 alineatul (4) al treilea paragraf,

întrucât:

(1) Regulamentul (UE) 2022/2554 urmărește să armonizeze și să raționalizeze cerințele de raportare a incidentelor legate de TIC și a incidentelor operaționale sau de securitate legate de plăți care privesc instituțiile de credit, instituțiile de plată, prestatorii de servicii de informare cu privire la conturi și instituțiile emitente de monedă electronică (denumite în continuare „incidente”). Având în vedere că cerințele de raportare privesc 20 de tipuri diferite de entități financiare, criteriile de clasificare și pragurile de semnificație pentru determinarea incidentelor majore și a amenințărilor cibernetice semnificative ar trebui precizate într-o manieră simplă, armonizată și coerentă, care să țină seama de particularitățile serviciilor și ale activităților tuturor entităților financiare relevante.

(2) Pentru a asigura proporționalitatea, criteriile de clasificare și pragurile de semnificație ar trebui să reflecte dimensiunea și profilul general de risc, precum și natura, amploarea și complexitatea serviciilor tuturor entităților financiare. În plus, criteriile și pragurile de semnificație ar trebui concepute astfel încât să se aplice în mod coerent tuturor entităților financiare, indiferent de dimensiunea și profilul lor de risc, și să nu reprezinte o sarcină de raportare disproporționată pentru entitățile financiare mai mici. Cu toate acestea, pentru a aborda situațiile în care un număr semnificativ de clienți sunt afectați de un incident care, ca atare, nu depășește pragul aplicabil, ar trebui stabilit un prag absolut care să vizeze în principal entitățile financiare mai mari.

(3) În ceea ce privește cadrele de raportare a incidentelor, care au existat înainte de intrarea în vigoare a Regulamentului (UE) 2022/2554, ar trebui asigurată continuitatea pentru entitățile financiare. Prin urmare, criteriile de clasificare și pragurile de semnificație ar trebui să fie conforme cu Ghidul ABE privind raportarea incidentelor majore în temeiul Directivei (UE) 2015/2366 a Parlamentului European și a Consiliului ([2]), cu Orientările privind informarea periodică și notificarea modificărilor semnificative care trebuie transmise ESMA de registrele centrale de tranzacții, cu Cadrul de raportare a incidentelor cibernetice al BCE/MUS și cu alte orientări relevante și ar trebui să se inspire din modelul acestora. Criteriile și pragurile de clasificare ar trebui, de asemenea, să fie adecvate pentru entitățile financiare care nu făceau obiectul unor cerințe de raportare a incidentelor înainte de intrarea în vigoare a Regulamentului (UE) 2022/2554.

(4) În ceea ce privește criteriul de clasificare „cuantumul și numărul tranzacțiilor afectate”, noțiunea de tranzacții este largă și acoperă diferite activități și servicii care fac obiectul unei multitudini de reglementări sectoriale aplicabile entităților financiare. În sensul acestui criteriu de clasificare, ar trebui să fie avute în vedere operațiunile de plată și toate formele de schimb de instrumente financiare, de criptoactive, de mărfuri sau de orice alte active, inclusiv sub formă de marje, garanții reale sau gajuri, atât contra numerar, cât și contra oricărui alt activ. Toate tranzacțiile care implică active a căror valoare poate fi exprimată în termeni monetari ar trebui avute în vedere în scopul clasificării.

([1]) JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Criteriile de clasificare ar trebui să garanteze faptul că sunt luate în considerare toate tipurile relevante de incidente majore. Este posibil ca multe criterii de clasificare să nu acopere neapărat atacurile cibernetice legate de intruziunea în rețele sau sisteme informatice. Cu toate acestea, ele sunt importante, deoarece orice intruziune în rețelele și sistemele informatice poate aduce prejudicii entității financiare. În consecință, criteriile de clasificare „servicii critice afectate" și „pierderi de date" ar trebui precizate astfel încât să acopere aceste tipuri de incidente majore, în special intruziunile neautorizate care, chiar dacă impactul lor nu este imediat cunoscut, pot avea consecințe grave, în special încălcări ale securității datelor și scurgeri de date.

(6) Întrucât instituțiile de credit sunt supuse atât cadrului de clasificare a incidentelor în temeiul articolului 18 din Regulamentul (UE) 2022/2554, cât și al cadrului privind riscul operațional în temeiul Regulamentului delegat (UE) 2018/959 al Comisiei ([3]), abordările în ceea ce privește evaluarea impactului economic al unui incident pe baza calculului costurilor și al pierderilor ar trebui să fie, în cea mai mare măsură posibilă, coerente în ambele cadre pentru a se evita introducerea unor cerințe incompatibile sau contradictorii.

(7) Criteriul referitor la întinderea geografică a unui incident, prevăzut la articolul 18 alineatul (1) litera (c) din Regulamentul (UE) 2022/2554, ar trebui să se axeze pe impactul transfrontalier al incidentului, întrucât impactul unui incident asupra activităților unei entități financiare din cadrul unei singure jurisdicții va fi reflectat de celelalte criterii prevăzute la articolul respectiv.

(8) Întrucât criteriile de clasificare sunt interdependente și legate între ele, abordarea în ceea ce privește identificarea incidentelor majore care trebuie raportate în conformitate cu articolul 19 alineatul (1) din Regulamentul (UE) 2022/2554 ar trebui să se bazeze pe o combinație de criterii, în care unele criterii care sunt strâns legate de definițiile incidentelor legate de TIC și ale incidentelor majore legate de TIC, astfel cum sunt prevăzute la articolul 3 punctele 8 și 10 din Regulamentul (UE) 2022/2554, ar trebui să aibă o importanță mai mare în clasificarea incidentelor majore decât alte criterii.

(9) Pentru a se asigura faptul că rapoartele și notificările incidentelor majore primite de autoritățile competente în temeiul articolului 19 alineatul (1) din Regulamentul (UE) 2022/2554 servesc atât în scopuri de supraveghere, cât și de prevenire a contagiunii în întregul sector financiar, pragurile de semnificație ar trebui să permită identificarea incidentelor majore, concentrându-se, printre altele, pe impactul asupra serviciilor critice specifice entității, pe pragurile absolute și relative specifice ale clienților sau ale contrapărților financiare, pe tranzacțiile care indică un impact semnificativ asupra entității financiare și pe importanța impactului în alte state membre.

(10) Incidentele care afectează serviciile TIC sau rețelele și sistemele informatice care sprijină funcții critice sau importante ori care afectează serviciile financiare care necesită autorizare sau situațiile în care are loc un acces rău-intenționat neautorizat la rețele și sisteme informatice care sprijină funcții critice sau importante ar trebui considerate incidente care afectează serviciile critice ale entităților financiare. Accesul rău-intenționat neautorizat la rețele și sisteme informatice care sprijină funcții critice sau importante ale entităților financiare prezintă riscuri grave pentru entitatea financiară și, întrucât poate afecta alte entități financiare, ar trebui să fie întotdeauna considerat un incident major care trebuie raportat.

(11) Incidentele recurente care sunt legate printr-o cauză principală aparentă similară și care, luate izolat, nu sunt incidente majore, pot indica existența unor deficiențe și slăbiciuni semnificative în procedurile de gestionare a incidentelor și a riscurilor ale entității financiare. Prin urmare, incidentele recurente ar trebui considerate colectiv ca fiind majore atunci când apar în mod repetat într-o anumită perioadă de timp.

(12) Având în vedere că amenințările cibernetice pot avea un impact negativ asupra entității financiare și a sectorului financiar, amenințările cibernetice semnificative pe care entitățile financiare le pot semnala ar trebui să indice probabilitatea materializării lor și caracterul critic al impactului lor potențial. În consecință, pentru a se asigura o evaluare clară și coerentă a importanței amenințărilor cibernetice, clasificarea unei amenințări cibernetice ca fiind semnificativă ar trebui să depindă de probabilitatea îndeplinirii criteriilor pentru clasificarea unui incident ca incident major și a atingerii pragului corespunzător în cazul în care s-ar materializa amenințarea, de tipul de amenințare cibernetică și de informațiile de care dispune entitatea financiară.

([3]) Regulamentul delegat (UE) 2018/959 al Comisiei din 14 martie 2018 de completare a Regulamentului (UE) nr. 575/2013 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare referitoare la specificarea metodologiei de evaluare pe baza căreia autoritățile competente permit instituțiilor să utilizeze abordări avansate de evaluare pentru riscul operațional (JO L 169, 6.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Având în vedere că autoritățile competente din alte state membre trebuie să fie notificate cu privire la incidentele care au un impact asupra entităților financiare și a clienților din jurisdicția lor, evaluarea impactului într-o altă jurisdicție în conformitate cu articolul 19 alineatul (7) din Regulamentul (UE) 2022/2554 ar trebui să se bazeze pe cauza principală a incidentului, pe potențiala contagiune prin intermediul furnizorilor terți și pe infrastructurile pieței financiare, precum și pe impactul incidentului asupra grupurilor semnificative de clienți sau contrapărți financiare.

(14) Procesele de raportare și notificare menționate la articolul 19 alineatele (6) și (7) din Regulamentul (UE) 2022/2554 ar trebui să permită destinatarilor respectivi să evalueze impactul incidentelor. Prin urmare, informațiile transmise ar trebui să includă toate detaliile cuprinse în rapoartele privind incidentele transmise de entitatea financiară autorității competente.

(15) În cazul în care un incident constituie o încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) și cu Directiva 2002/58/CE a Parlamentului European și a Consiliului ([5]), prezentul regulament nu ar trebui să aducă atingere obligațiilor de înregistrare și notificare în cazul încălcării securității datelor cu caracter personal prevăzute în respectivele acte legislative ale Uniunii. 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 în Directiva 2002/58/CE.

(16) Prezentul regulament se bazează pe proiectele de standarde tehnice de reglementare prezentate Comisiei de către autoritățile europene de supraveghere, în consultare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și cu Banca Centrală Europeană (BCE).

(17) Comitetul comun al autorităților europene de supraveghere menționat la articolul 54 din Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([6]), la articolul 54 din Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ([7]) și la articolul 54 din Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului ([8]) a efectuat consultări publice deschise cu privire la proiectul de standarde tehnice de reglementare pe care se bazează prezentul regulament, a analizat costurile și beneficiile potențiale ale standardelor propuse și a solicitat avizul Grupului părților interesate din domeniul bancar, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1093/2010, al Grupului părților interesate din domeniul asigurărilor și reasigurărilor și al Grupului părților interesate din domeniul pensiilor ocupaționale, instituite în conformitate cu articolul 37 din Regulamentul (UE) nr. 1094/2010, precum și al Grupului părților interesate din domeniul valorilor mobiliare și pieților, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1095/2010.

([4]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) 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, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) 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 ([9]) și a emis un aviz la 24 ianuarie 2024,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

CRITERII DE CLASIFICARE

Articolul 1

Clienți, contrapărți financiare și tranzacții

(1) Numărul clienților afectați de incident, astfel cum este menționat la articolul 18 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, reflectă numărul tuturor clienților afectați, indiferent dacă sunt persoane fizice sau juridice, care nu pot sau nu au putut să utilizeze serviciul furnizat de entitatea financiară în timpul incidentului sau care au fost afectați negativ de incident. Acest număr trebuie să îi includă și pe terții vizați în mod explicit de acordul contractual dintre entitatea financiară și client în calitate de beneficiari ai serviciului afectat.

(2) Numărul contrapărților financiare afectate de incident, astfel cum este menționat la articolul 18 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, reflectă numărul tuturor contrapărților financiare afectate care au încheiat un acord contractual cu entitatea financiară.

(3) În ceea ce privește relevanța clienților și a contrapărților financiare afectate de incident, astfel cum se menționează la articolul 18 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, entitatea financiară ia în considerare măsura în care impactul asupra unui client sau a unei contrapărți financiare va afecta punerea în aplicare a obiectivelor de activitate ale entității financiare, precum și impactul potențial al incidentului asupra eficienței pieței.

(4) În ceea ce privește cuantumul sau numărul tranzacțiilor afectate de incident, astfel cum este menționat la articolul 18 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, entitatea financiară ia în considerare toate tranzacțiile afectate care implică o valoare monetară și în care cel puțin o parte a tranzacției se desfășoară în Uniune.

(5) În cazul în care numărul real al clienților sau al contrapărților financiare afectate sau numărul real ori cuantumul real al tranzacțiilor afectate nu poate fi determinat, entitatea financiară estimează aceste numere sau cuantumuri pe baza datelor disponibile din perioadele de referință comparabile.

Articolul 2

Impactul asupra reputației

(1) În scopul stabilirii impactului incidentului asupra reputației, astfel cum se menționează la articolul 18 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, entitățile financiare consideră că a avut loc un impact asupra reputației atunci când este îndeplinit cel puțin unul dintre următoarele criterii:

(a) incidentul a fost reflectat în mass-media;

(b) incidentul a dus la formularea unor plângeri repetitive din partea unor clienți diferiți sau a unor contrapărți financiare diferite cu privire la serviciile care presupun contact direct cu clienții sau la relațiile de afaceri critice;

(c) entitatea financiară nu va fi în măsură sau este probabil că nu va fi în măsură să îndeplinească cerințele reglementare ca urmare a incidentului;

(d) entitatea financiară va pierde sau este probabil că va pierde clienți sau contrapărți financiare, ceea ce va avea un impact semnificativ asupra activității sale ca urmare a incidentului.

([9]) 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, http://data.europa.eu/eli/reg/2018/1725/oj).

(2) Atunci când evaluează impactul incidentului asupra reputației, entitățile financiare iau în considerare nivelul de vizibilitate pe care incidentul l-a dobândit sau este probabil să îl dobândească în raport cu fiecare criteriu enumerat la alineatul (1).

Articolul 3

Durata incidentului și perioada de indisponibilitate a serviciului

(1) Entitățile financiare măsoară durata unui incident, astfel cum se menționează la articolul 18 alineatul (1) litera (b) din Regulamentul (UE) 2022/2554, din momentul în care acesta survine și până în momentul în care acesta este soluționat.

În cazul în care entitățile financiare nu sunt în măsură să stabilească momentul în care a survenit incidentul, acestea măsoară durata incidentului din momentul în care acesta a fost detectat. În cazul în care iau cunoștință de faptul că incidentul a survenit înainte de detectarea sa, entitățile financiare măsoară durata din momentul în care incidentul este înregistrat în jurnalele de rețea sau de sistem sau în alte surse de date.

În cazul în care entitățile financiare nu știu încă când va fi soluționat incidentul sau nu sunt în măsură să verifice înregistrările din jurnale sau din alte surse de date, acestea aplică estimări.

(2) Entitățile financiare măsoară perioada de indisponibilitate a serviciului în cazul unui incident, astfel cum se menționează la articolul 18 alineatul (1) litera (b) din Regulamentul (UE) 2022/2554, din momentul în care serviciul este total sau parțial indisponibil pentru clienți, pentru contrapărțile financiare sau pentru alți utilizatori interni sau externi până în momentul în care activitățile sau operațiunile obișnuite au fost readuse la nivelul serviciului care a fost furnizat înainte de incident. În cazul în care perioada de indisponibilitate a serviciului cauzează o întârziere în furnizarea serviciului după restabilirea activităților sau a operațiunilor obișnuite, perioada de indisponibilitate se măsoară de la începutul incidentului până în momentul în care serviciul întârziat este furnizat integral.

În cazul în care nu sunt în măsură să stabilească momentul în care a început perioada de indisponibilitate a serviciului, entitățile financiare măsoară perioada de indisponibilitate a serviciului din momentul în care aceasta a fost detectată.

Articolul 4

Întinderea geografică

În scopul stabilirii întinderii geografice în ceea ce privește zonele afectate de incident, astfel cum se menționează la articolul 18 alineatul (1) litera (c) din Regulamentul (UE) 2022/2554, entitățile financiare evaluează dacă incidentul are sau a avut un impact în alte state membre și, în special, importanța impactului în legătură cu oricare dintre următoarele elemente:

(a) clienții și contrapărțile financiare din alte state membre;

(b) sucursalele sau alte entități financiare din cadrul grupului care desfășoară activități în alte state membre;

(c) infrastructurile pieței financiare sau furnizorii terți, care pot afecta entitățile financiare din alte state membre cărora le furnizează servicii, în măsura în care aceste informații sunt disponibile.

Articolul 5

Pierderi de date

În scopul stabilirii pierderilor de date pe care le implică incidentul, astfel cum se menționează la articolul 18 alineatul (1) litera (d) din Regulamentul (UE) 2022/2554, entitățile financiare iau în considerare următoarele:

(a) în ceea ce privește disponibilitatea datelor, dacă incidentul a făcut ca datele cerute de entitatea financiară, clienții săi sau contrapărțile acesteia să fie inaccesibile sau inutilizabile temporar ori permanent;

(b) în ceea ce privește autenticitatea datelor, dacă incidentul a compromis credibilitatea sursei de date;

(c) în ceea ce privește integritatea datelor, dacă incidentul a dus la modificarea neautorizată a datelor, ceea ce a făcut ca acestea să fie inexacte sau incomplete;

(d) în ceea ce privește confidențialitatea datelor, dacă incidentul a avut ca rezultat accesarea sau divulgarea datelor de către o parte sau un sistem neautorizat.

Articolul 6

Caracterul critic al serviciilor afectate

În scopul stabilirii caracterului critic al serviciilor afectate, astfel cum se menționează la articolul 18 alineatul (1) litera (e) din Regulamentul (UE) 2022/2554, entitățile financiare evaluează dacă incidentul:

(a) afectează sau a afectat serviciile TIC sau rețelele și sistemele informatice care sprijină funcții critice sau importante ale entității financiare;

(b) afectează sau a afectat serviciile financiare furnizate de entitatea financiară care necesită autorizare, înregistrare sau care sunt supravegheate de autoritățile competente;

(c) constituie sau a constituit un acces reușit, rău-intenționat și neautorizat la rețeaua și la sistemele informatice ale entității financiare.

Articolul 7

Impactul economic

(1) În scopul stabilirii impactului economic al incidentului, astfel cum se menționează la articolul 18 alineatul (1) litera (f) din Regulamentul (UE) 2022/2554, entitățile financiare iau în considerare, fără a ține seama de recuperările financiare, următoarele tipuri de costuri directe și indirecte și pierderi pe care le-au suportat ca urmare a incidentului:

(a) fondurile expropriate sau activele financiare pentru care sunt răspunzătoare, inclusiv activele pierdute în urma furtului;

(b) costurile de înlocuire sau mutare a software-ului, hardware-ului sau infrastructurii;

(c) costurile cu personalul, inclusiv costurile asociate înlocuirii sau mutării personalului, recrutării de personal suplimentar, remunerării orelor suplimentare și recuperării competențelor pierdute sau afectate;

(d) taxele datorate ca urmare a nerespectării obligațiilor contractuale;

(e) costurile aferente reparațiilor și despăgubirilor datorate clienților;

(f) pierderile datorate veniturilor nerealizate;

(g) costurile aferente comunicării interne și externe;

(h) costurile de consiliere, inclusiv costurile aferente consilierii juridice, serviciilor de expertiză criminalistică și serviciilor de remediere.

(2) Costurile și pierderile menționate la alineatul (1) nu includ costurile care sunt necesare pentru funcționarea curentă a activității, în special următoarele:

(a) costurile pentru întreținerea generală a infrastructurii, a echipamentelor, a hardware-ului și a software-ului, precum și costurile pentru actualizarea competențelor personalului;

(b) costurile interne sau externe pentru consolidarea activității după incident, inclusiv cele aferente modernizărilor, îmbunătățirilor și inițiativelor de evaluare a riscurilor;

(c) primele de asigurare.

(3) Entitățile financiare calculează cuantumurile costurilor și pierderilor pe baza datelor disponibile la momentul raportării. În cazul în care cuantumul real al costurilor și al pierderilor nu poate fi determinat, entitățile financiare estimează cuantumurile respective.

(4) Atunci când evaluează impactul economic al incidentului, entitățile financiare însumează costurile și pierderile menționate la alineatul (1).

CAPITOLUL II

INCIDENTE MAJORE ȘI PRAGURI DE SEMNIFICAȚIE

Articolul 8

Incidente majore

(1) Un incident este considerat incident major în sensul articolului 19 alineatul (1) din Regulamentul (UE) 2022/2554 dacă a afectat serviciile critice, astfel cum se menționează la articolul 6 și dacă este îndeplinită oricare dintre următoarele condiții:

(a) este atins pragul de semnificație menționat la articolul 9 alineatul (5) litera (b);

(b) sunt atinse două sau mai multe dintre celelalte praguri de semnificație menționate la articolul 9 alineatele (1)-(6).

(2) Incidentele recurente care, în mod individual, nu sunt considerate incidente majore în conformitate cu alineatul (1) sunt considerate ca fiind un singur incident major dacă îndeplinesc toate condițiile următoare:

(a) au avut loc cel puțin de două ori într-o perioadă de 6 luni;

(b) au aceeași cauză principală aparentă ca cea menționată la articolul 20 primul alineat litera (b) din Regulamentul (UE) 2022/2554;

(c) îndeplinesc în mod colectiv criteriile pentru a fi considerate incidente majore prevăzute la alineatul (1).

Entitățile financiare evaluează lunar existența incidentelor recurente.

Prezentul alineat nu se aplică microîntreprinderilor și nici entităților financiare enumerate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554.

Articolul 9

Praguri de semnificație pentru determinarea incidentelor majore

(1) Pragul de semnificație pentru criteriul „clienți, contrapărți financiare și tranzacții” este îndeplinit dacă este îndeplinită oricare dintre următoarele condiții:

(a) numărul clienților afectați reprezintă mai mult de 10 % din totalul clienților care utilizează serviciul afectat;

(b) numărul clienților afectați care utilizează serviciul afectat este mai mare de 100 000;

(c) numărul contrapărților financiare afectate reprezintă mai mult de 30 % din totalul contrapărților financiare care desfășoară activități legate de furnizarea serviciului afectat;

(d) numărul tranzacțiilor afectate reprezintă mai mult de 10 % din numărul mediu zilnic de tranzacții efectuate de entitatea financiară în legătură cu serviciul afectat;

(e) cuantumul tranzacțiilor afectate reprezintă mai mult de 10 % din valoarea medie zilnică de tranzacții efectuate de entitatea financiară în legătură cu serviciul afectat;

(f) au fost afectați clienți sau contrapărți financiare care au fost identificați (identificate) ca fiind relevanți (relevante) în conformitate cu articolul 1 alineatul (3).

În cazul în care numărul real al clienților sau al contrapărților financiare afectate sau numărul real ori cuantumul real al tranzacțiilor afectate nu poate fi determinat, entitatea financiară estimează aceste numere sau cuantumuri pe baza datelor disponibile din perioadele de referință comparabile.

(2) Pragul de semnificație pentru criteriul „impact asupra reputației” este îndeplinit dacă este întrunită oricare dintre condițiile prevăzute la articolul 2 literele (a)-(d).

(3) Pragul de semnificație pentru criteriul „durata incidentului și perioada de indisponibilitate a serviciului” este îndeplinit dacă este întrunită oricare dintre următoarele condiții:

(a) durata incidentului este mai mare de 24 de ore;

(b) perioada de indisponibilitate a serviciului este de peste 2 ore pentru serviciile TIC care sprijină funcții critice sau importante.

(4) Pragul de semnificație pentru criteriul „întindere geografică” este îndeplinit dacă incidentul are un impact în două sau mai multe state membre, în conformitate cu articolul 4.

(5) Pragul de semnificație pentru criteriul „pierderi de date” este îndeplinit dacă este întrunită oricare dintre următoarele condiții:

(a) orice impact, astfel cum este menționat la articolul 5, asupra disponibilității, a autenticității, a integrității sau a confidențialității datelor are sau va avea un impact negativ asupra punerii în aplicare a obiectivelor de activitate ale entității financiare sau asupra capacității acesteia de a îndeplini cerințele reglementare;

(b) are loc un acces reușit, rău-intenționat și neautorizat la rețelele și sistemele informatice, acces care nu intră sub incidența literei (a), în cazul în care un astfel de acces poate duce la pierderi de date.

(6) Pragul de semnificație pentru criteriul „impact economic” este îndeplinit în cazul în care costurile și pierderile suportate de entitatea financiară din cauza incidentului au depășit sau este probabil să depășească suma de 100 000 EUR.

CAPITOLUL III

AMENINȚĂRI CIBERNETICE SEMNIFICATIVE

Articolul 10

Praguri de semnificație ridicată pentru stabilirea amenințărilor cibernetice semnificative

În sensul articolului 18 alineatul (2) din Regulamentul (UE) 2022/2554, o amenințare cibernetică este considerată semnificativă în cazul în care sunt îndeplinite toate condițiile următoare:

(a) amenințarea cibernetică, dacă se materializează, ar putea afecta sau ar fi putut afecta funcțiile critice sau importante ale entității financiare sau ar putea afecta alte entități financiare, furnizori terți, clienți sau contrapărți financiare, pe baza informațiilor de care dispune entitatea financiară;

(b) amenințarea cibernetică are o probabilitate ridicată de materializare în cadrul entității financiare sau al altor entități financiare, ținând seama cel puțin de următoarele elemente:

(i) riscurile aplicabile legate de amenințarea cibernetică menționată la litera (a), inclusiv vulnerabilitățile potențiale ale sistemelor entității financiare care pot fi exploatate;

(ii) capacitățile și intenția actorilor care generează amenințări, în măsura în care sunt cunoscute de entitatea financiară;

(iii) persistența amenințării și orice cunoștințe acumulate cu privire la incidentele care au afectat entitatea financiară sau furnizorul terț, clienții sau contrapărțile financiare ale acesteia;

(c) dacă s-ar materializa, amenințarea cibernetică ar putea îndeplini oricare dintre următoarele:

(i) criteriul privind caracterul critic al serviciilor prevăzut la articolul 18 alineatul (1) litera (e) din Regulamentul (UE) 2022/2554, astfel cum este specificat la articolul 6 din prezentul regulament;

(ii) pragul de semnificație prevăzut la articolul 9 alineatul (1);

(iii) pragul de semnificație prevăzut la articolul 9 alineatul (4).

În cazul în care, în funcție de tipul de amenințare cibernetică și de informațiile disponibile, entitatea financiară concluzionează că ar putea fi atinse pragurile de semnificație prevăzute la articolul 9 alineatele (2), (3), (5) și (6), pragurile respective pot fi avute, de asemenea, în vedere.

CAPITOLUL IV

RELEVANȚA INCIDENTELOR MAJORE PENTRU AUTORITĂȚILE COMPETENTE DIN ALTE STATE MEMBRE ȘI DETALIILE RAPOARTELOR CARE TREBUIE COMUNICATE ALTOR AUTORITĂȚI COMPETENTE

Articolul 11

Relevanța incidentelor majore pentru autoritățile competente din alte state membre

Pentru a evalua măsura în care incidentul major este relevant pentru autoritățile competente din alte state membre, astfel cum se menționează la articolul 19 alineatul (7) din Regulamentul (UE) 2022/2554, se determină dacă incidentul are o cauză principală care își are originea într-un alt stat membru sau dacă incidentul are sau a avut un impact semnificativ într-un alt stat membru asupra oricărora dintre următoarele:

(a) clienți sau contrapărți financiare;

(b) o sucursală a entității financiare sau o altă entitate financiară din cadrul grupului;

(c) o infrastructură a pieței financiare sau un furnizor terț care poate afecta entitățile financiare cărora le furnizează servicii.

Articolul 12

Detalii privind incidentele majore care trebuie să fie comunicate altor autorități competente

Detaliile privind incidentele majore pe care autoritățile competente trebuie să le transmită altor autorități competente în conformitate cu articolul 19 alineatul (6) din Regulamentul (UE) 2022/2554 și notificările care trebuie transmise de ABE, ESMA sau EIOPA și BCE autorităților competente relevante din alte state membre în conformitate cu articolul 19 alineatul (7) din regulamentul respectiv conțin același nivel de informații, fără nicio anonimizare, ca notificările și rapoartele privind incidentele majore primite de la entități financiare în conformitate cu articolul 19 alineatul (4) din Regulamentul (UE) 2022/2554.

CAPITOLUL V

DISPOZIȚII FINALE

Articolul 13

Intrare în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 13 martie 2024.

Pentru Comisie
Președinta
Ursula VON DER LEYEN