REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2025/847 AL COMISIEI

din 6 mai 2025

de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește măsurile de răspuns la încălcările securității portofelelor europene pentru identitatea digitală

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 5e alineatul (5),

întrucât:

(1) Cadrul pentru identitatea digitală europeană (denumit în continuare „cadrul") instituit prin Regulamentul (UE) nr. 910/2014 este un element-cheie pentru instituirea unui ecosistem pentru identitatea digitală securizat și interoperabil în întreaga Uniune. Portofelele europene pentru identitatea digitală (denumite în continuare „portofelele") constituie temelia acestui cadru, care are drept scop facilitarea accesului la servicii în toate statele membre, asigurând în același timp protecția datelor cu caracter personal și a vieții private.

(2) Regulamentele (UE) 2016/679 ([2]) și (UE) 2018/1725 ([3]) ale Parlamentului European și ale Consiliului și, după caz, Directiva 2002/58/CE a Parlamentului European și a Consiliului ([4]) se aplică activităților de prelucrare a datelor cu caracter personal desfășurate în temeiul prezentului regulament. Normele privind evaluarea și furnizarea de informații stabilite în temeiul prezentului regulament nu aduc atingere obligației de a notifica încălcările securității datelor cu caracter personal autorității de supraveghere competente, după caz, în temeiul Regulamentului (UE) 2016/679 sau al Regulamentului (UE) 2018/1725, și nici obligației de a comunica persoanelor vizate încălcările securității datelor cu caracter personal, dacă este cazul, în temeiul acestor regulamente.

(3) Comisia evaluează periodic noile tehnologii, practici, standarde și specificații tehnice. Pentru a asigura cel mai înalt nivel de armonizare între statele membre în ceea ce privește dezvoltarea și certificarea portofelelor, specificațiile tehnice prevăzute în prezentul regulament se bazează pe activitatea desfășurată în temeiul Recomandării (UE) 2021/946 a Comisiei ([5]), în special pe arhitectura și cadrul de referință care fac parte din acesta. În conformitate cu considerentul 75 din Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului ([6]), Comisia ar trebui să revizuiască și, dacă este necesar, să actualizeze prezentul regulament, pentru a îl menține aliniat la evoluțiile mondiale și la arhitectura și cadrul de referință, precum și pentru a respecta cele mai bune practici de pe piața internă.

([1]) JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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).

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

([4]) 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).

([5]) Recomandarea (UE) 2021/946 a Comisiei din 3 iunie 2021 privind un set de instrumente comun al Uniunii pentru o abordare coordonată în direcția unui cadru european al identității digitale (JO L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) În cazul unei încălcări a securității sau al compromiterii soluțiilor pentru portofel ori a mecanismelor de validare menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 sau a sistemului de identificare electronică prin intermediul căruia sunt furnizate soluțiile pentru portofel, trebuie să se ia măsuri de răspuns la astfel de încălcări ale securității și compromiteri, într-un mod rapid, coordonat și sigur, în toate statele membre, pentru a proteja utilizatorii și pentru a menține încrederea în ecosistemul identității digitale. Acest lucru nu aduce atingere Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului ([7]) și Regulamentelor (UE) 2019/881 ([8]) și (UE) 2024/2847 ([9]) ale Parlamentului European și ale Consiliului, în special, în ceea ce privește gestionarea incidentelor sau a vulnerabilităților și considerarea lor drept încălcări ale securității. Prin urmare, statele membre ar trebui să asigure suspendarea în timp util a furnizării și utilizării portofelelor afectate de o încălcare a securității sau de o compromitere sau, după caz, retragerea acestor portofele.

(5) Pentru a asigura măsuri de răspuns adecvate la o încălcare a securității sau la o compromitere, statele membre ar trebui să evalueze dacă o astfel de încălcare sau compromitere a unei soluții pentru portofel, a mecanismelor de validare menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 sau a sistemului de identificare electronică prin intermediul căruia este furnizată o soluție pentru portofel afectează fiabilitatea respectivei soluții pentru portofel sau a altor soluții pentru portofel. O astfel de evaluare ar trebui să se bazeze pe criterii uniforme, cum ar fi numărul și categoria utilizatorilor portofelelor, ale persoanelor fizice și ale beneficiarilor portofelelor afectați, natura datelor afectate, durata compromiterii sau a încălcării securității, disponibilitatea limitată a unui serviciu și pierderile financiare, precum și potențiala compromitere a datelor cu caracter personal. Aceste criterii ar trebui să le ofere statelor membre o flexibilitate și o marjă de apreciere care să le permită să stabilească într-un mod proporțional dacă fiabilitatea unei soluții pentru portofel este afectată și dacă este oportun să suspende sau, în cazul în care acest lucru este justificat de gravitatea încălcării sau a compromiterii, să retragă soluția pentru portofel în cauză. Aceste criterii nu ar trebui să declanșeze retragerea automată a unei soluții pentru portofel sau suspendarea automată a furnizării și a utilizării unei soluții pentru portofel, ci ar trebui să fie luate în considerare în mod corespunzător de către statele membre atunci când acestea decid dacă este necesar să se retragă sau să se suspende furnizarea și utilizarea unei soluții pentru portofel.

(6) Având în vedere impactul și inconvenientele suspendării utilizării soluțiilor pentru portofel, statele membre vor trebui să evalueze dacă este necesar să revoce atestatele unității de portofel sau să ia orice alte măsuri suplimentare pentru a răspunde în mod adecvat la încălcarea securității sau la compromiterea în cauză.

(7) Pentru a informa utilizatorii portofelelor cu privire la statutul portofelelor lor, acestora trebuie să li se ofere informații adecvate cu privire la cazurile de încălcare a securității sau de compromitere a securității care le afectează portofelele. Întrucât și beneficiarii portofelelor înregistrați în Uniune pot fi afectați de încălcări ale securității și de compromiteri, informațiile relevante cu privire la încălcările securității și la compromiterile în cauză trebuie să le fie comunicate și acestora.

(8) Pentru a spori transparența și a consolida încrederea în ecosistemul identității digitale, informațiile cu privire la cazurile de încălcare a securității sau de compromitere și cu privire la consecințele acestora ar trebui să includă cel puțin informațiile cerute în temeiul prezentului regulament. Cu toate acestea, informațiile privind cazurile de încălcare a securității sau de compromitere comunicate utilizatorilor și beneficiarilor portofelelor ar trebui să fie evaluate cu atenție, astfel încât să se prevină și să se reducă la minimum riscul exploatării lor de către atacatori.

([7]) 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) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Pentru a permite utilizatorilor să aibă din nou acces la portofel după remedierea unei încălcări a securității sau a unei compromiteri, statul membru care a furnizat soluțiile pentru portofel va trebui să restabilească, fără întârzieri nejustificate, furnizarea și utilizarea respectivelor soluții pentru portofel. Acest lucru se poate realiza prin restabilirea unităților portofelului, prin emiterea unor unități de portofel furnizate în cadrul unei noi versiuni a soluțiilor pentru portofel sau prin reemiterea de noi atestate valabile ale unității de portofel. Utilizatorii afectați ai portofelelor, beneficiarii portofelelor, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1) din Regulamentul (UE) nr. 910/2014 și Comisia trebuie să fie informați în consecință.

(10) Pentru a garanta retragerea portofelelor în cazul în care o încălcare a securității sau o compromitere nu a fost remediată în termen de trei luni de la suspendare sau în cazul în care acest lucru este justificat de gravitatea încălcării securității sau a compromiterii, statul membru ar trebui să se asigure că atestatele unității de portofel în cauză sunt revocate și că acestea nu pot redeveni valabile și nici nu pot fi eliberate sau furnizate pentru unități de portofel existente. În plus, nu ar trebui să se furnizeze nicio unitate de portofel nouă în cadrul soluției pentru portofel afectate. Din motive de transparență, utilizatorii, beneficiarii, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1) din Regulamentul (UE) nr. 910/2014 și Comisia trebuie să fie informați cu privire la retragere. Informațiile care trebuie transmise în acest scop includ o descriere a impactului potențial asupra utilizatorilor portofelului și, în special, asupra gestionării atestatelor emise sau asupra beneficiarilor portofelului.

(11) Perioada de trei luni de la suspendarea furnizării și a utilizării unei soluții pentru portofel, în cursul căreia trebuie remediată încălcarea securității sau compromiterea care a condus la suspendarea respectivă, ar trebui să constituie termenul pentru remediere, la expirarea căruia soluția pentru portofel să fie retrasă în cazul în care nu a fost pusă în aplicare o măsură de remediere adecvată. Cu toate acestea, statele membre pot solicita ca încălcarea securității sau compromiterea în cauză să fie remediată într-un termen mai scurt de trei luni, ținând seama, în special și după caz, de amploarea, durata și consecințele respectivei încălcări a securității sau compromiteri. În cazul în care încălcarea securității sau compromiterea nu este sau nu poate fi remediată în termenul stabilit de statul membru, acesta poate solicita retragerea soluției pentru portofel înainte de expirarea perioadei de trei luni. Statele membre ar trebui să utilizeze această perioadă de timp în care trebuie remediată o încălcare a securității sau o compromitere care a condus la suspendarea furnizării și a utilizării unei soluții pentru portofel pentru a pregăti eventuala retragere a respectivei soluții pentru portofel și comunicările aferente.

(12) Pentru a reduce sarcina administrativă a statelor membre în ceea ce privește informațiile care trebuie furnizate, în conformitate cu prezentul regulament, Comisiei și altor state membre, statele membre ar trebui să utilizeze instrumentele de notificare existente, cum ar fi Sistemul de raportare și analiză a incidentelor cibernetice („CIRAS”), gestionat de Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”). În ceea ce privește canalele sau mijloacele alternative care trebuie utilizate pentru a informa utilizatorii portofelelor afectați de o încălcare a securității sau de o compromitere și beneficiarii portofelelor, statele membre ar trebui să se asigure că aceștia primesc informații relevante și că acestea sunt comunicate într-un mod clar, cuprinzător și ușor accesibil. Canalele utilizate pentru transmiterea acestor informații utilizatorilor afectați ai portofelelor și beneficiarilor portofelelor ar trebui să includă soluții adecvate pentru difuzarea pe site-uri web, urmărirea în timp real a actualizărilor site-urilor web și agregarea știrilor.

(13) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 și a emis un aviz la 31 ianuarie 2025.

(14) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit prin articolul 48 din Regulamentul (UE) nr. 910/2014,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect

Prezentul regulament stabilește norme privind măsurile de răspuns la încălcările securității portofelelor din cadrul mecanismelor de validare menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 și al sistemului de identificare electronică prin intermediul căruia sunt furnizate portofelele.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „soluție pentru portofel” înseamnă o combinație de software, hardware, servicii, setări și configurații, inclusiv instanțe ale portofelului, una sau mai multe aplicații criptografice securizate pentru portofel și unul sau mai multe dispozitive criptografice securizate pentru portofel;

2. „utilizator al portofelului” înseamnă un utilizator care deține controlul asupra unității de portofel;

3. „beneficiar al portofelului” înseamnă un beneficiar care intenționează să recurgă la unități de portofel pentru furnizarea de servicii publice sau private prin intermediul interacțiunii digitale;

4. „instanță a portofelului” înseamnă aplicația instalată și configurată pe dispozitivul sau în mediul unui utilizator al unui portofel, care face parte dintr-o unitate de portofel și pe care utilizatorul portofelului o folosește pentru a interacționa cu unitatea de portofel;

5. „aplicație criptografică securizată pentru portofel” înseamnă o aplicație care gestionează active critice prin faptul că este legată de funcțiile criptografice și necriptografice furnizate de dispozitivul criptografic securizat pentru portofel și că utilizează aceste funcții;

6. „dispozitiv criptografic securizat pentru portofel” înseamnă un dispozitiv inviolabil care oferă un mediu legat de aplicația criptografică securizată pentru portofel și utilizat de aceasta pentru a proteja activele critice și pentru a furniza funcții criptografice pentru executarea securizată a operațiunilor critice;

7. „furnizor de portofel” înseamnă o persoană fizică sau juridică care furnizează soluții pentru portofel;

8. „unitate de portofel” înseamnă o configurație unică a unei soluții pentru portofel care include instanțe ale portofelului, aplicații criptografice securizate pentru portofel și dispozitive criptografice securizate pentru portofel, furnizată de un furnizor de portofel unui utilizator individual al portofelului;

9. „active critice” înseamnă active din cadrul unei unități de portofel sau legate de o astfel de unitate care au o importanță atât de extraordinară încât, în cazul în care disponibilitatea, confidențialitatea sau integritatea lor este compromisă, acest lucru ar avea un efect foarte grav, de slăbire a capacității de a recurge la unitatea de portofel;

10. „atestat al unității de portofel” înseamnă un obiect de date care descrie componentele unității de portofel sau permite autentificarea și validarea componentelor respective.

Articolul 3

Stabilirea unei încălcări a securității sau a unei compromiteri

(1) Fără a aduce atingere Directivei (UE) 2022/2555 și Regulamentelor (UE) 2019/881 și (UE) 2024/2847, statele membre țin seama în mod corespunzător de criteriile stabilite în anexa I la prezentul regulament pentru a evalua dacă o încălcare a securității sau o compromitere a unei soluții pentru portofel, a mecanismelor de validare menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 sau a sistemului de identificare electronică prin intermediul căruia este furnizată soluția pentru portofel afectează fiabilitatea respectivei soluții sau a altor soluții pentru portofel.

(2) În cazul în care un stat membru stabilește, pe baza evaluării prevăzute la alineatul (1), că o încălcare a securității sau o compromitere afectează fiabilitatea unei soluții pentru portofel și suspendă furnizarea și utilizarea soluției respective, statul membru în cauză ia măsurile prevăzute la articolele 4 și 5. În cazul în care un stat membru revocă soluția pentru portofel, acesta ia măsurile prevăzute la articolele 8 și 9.

(3) În cazul în care când un stat membru ia cunoștință de informații legate de o posibilă încălcare a securității sau de o compromitere care ar putea afecta fiabilitatea uneia sau mai multor soluții pentru portofel furnizate de un alt stat membru, statul membru în cauză comunică, fără întârzieri nejustificate, acest fapt Comisiei și punctelor unice de contact din statele membre afectate desemnate în temeiul articolului 46c alineatul (1) din Regulamentul (UE) nr. 910/2014. Comunicarea respectivă include informațiile prevăzute la articolul 5 alineatul (2).

(4) Statul membru care primește informațiile furnizate în temeiul alineatului (3) ia, fără întârzieri nejustificate, măsurile prevăzute la alineatele (1) și (2).

Articolul 4

Suspendarea furnizării și a utilizării portofelelor și alte măsuri de remediere

(1) Statele membre se asigură că în cadrul unei soluții pentru portofel suspendate nu se furnizează, utilizează sau activează nicio unitate de portofel.

(2) Statele membre evaluează dacă, pentru a reacționa în mod adecvat la o încălcare a securității sau la o compromitere, este necesar să revoce atestatele unităților de portofel afectate de suspendarea unei soluții pentru portofel sau să ia orice altă măsură de remediere suplimentară.

(3) Măsurile prevăzute la alineatele (1) și (2) sunt luate fără întârzieri nejustificate și, în orice caz, în termen de cel mult 24 de ore de la suspendarea furnizării și a utilizării soluției pentru portofel afectate de încălcarea securității sau de compromiterea în cauză.

(4) Măsurile prevăzute la alineatele (1) și (2) nu îi împiedică pe utilizatorii portofelelor să își exercite dreptul la portabilitatea datelor prevăzut la articolul 5a alineatul (4) litera (g) din Regulamentul (UE) nr. 910/2014. Acest lucru este condiționat de faptul că dreptul menționat poate fi exercitat de utilizatorii portofelelor fără a afecta securitatea activelor critice ale unităților de portofel afectate, în special având în vedere motivele suspendării și necesitatea de a asigura protecția efectivă a activelor respective împotriva utilizării abuzive.

Articolul 5

Informații privind suspendările și măsurile de remediere

(1) Se transmit, fără întârzieri nejustificate și în termen de cel mult 24 de ore de la suspendarea furnizării și a utilizării unei soluții pentru portofel, informații clare, cuprinzătoare și ușor accesibile cu privire la respectiva suspendare către:

(a) punctele unice de contact desemnate în temeiul articolului 46c alineatul (1) din Regulamentul (UE) nr. 910/2014;

(b) Comisie;

(c) utilizatorii de portofele afectați;

(d) beneficiarii portofelelor înregistrați în conformitate cu articolul 5b din Regulamentul (UE) nr. 910/2014.

(2) Informațiile furnizate în conformitate cu alineatul (1) includ cel puțin următoarele:

(a) numele furnizorului soluției pentru portofel ale cărei furnizare și utilizare au fost suspendate;

(b) denumirea și identificatorul de referință ale respectivei soluții pentru portofel, astfel cum sunt menționate în lista portofelelor certificate întocmită în temeiul articolului 5d din Regulamentul (UE) nr. 910/2014 și, după caz, versiunile aferente;

(c) data și ora la care a fost detectată încălcarea securității sau compromiterea;

(d) dacă se cunosc, data și ora la care încălcarea securității sau compromiterea a devenit efectivă, pe baza jurnalelor de rețea sau de sistem sau a altor surse de date;

(e) data și ora suspendării soluției pentru portofel;

(f) datele de contact, inclusiv cel puțin o adresă de e-mail și un număr de telefon pentru statul membru notificator și, în cazul în care acestea sunt diferite, pentru furnizorul portofelului menționat la litera (a);

(g) o descriere a încălcării securității sau a compromiterii;

(h) o descriere a datelor compromise, inclusiv, după caz, categoriile de date cu caracter personal definite la articolul 9 alineatul (1) și la articolul 10 din Regulamentul (UE) 2016/679;

(i) dacă este posibil, o estimare a numărului aproximativ al utilizatorilor de portofele afectați și al altor persoane fizice afectate;

(j) o descriere a impactului potențial asupra beneficiarilor sau a utilizatorilor portofelelor și, în acest din urmă caz, dacă este relevant, orice indicații privind măsurile pe care utilizatorii portofelelor le pot lua pentru a atenua respectivul impact potențial;

(k) o descriere a măsurilor luate sau planificate pentru a remedia încălcarea sau compromiterea securității, împreună cu o planificare și un termen pentru o astfel de remediere;

(l) atunci când este posibil și adecvat, o descriere a măsurilor luate sau planificate pentru transferarea utilizatorilor de portofele afectați către alte soluții pentru portofel sau servicii.

Articolul 6

Restabilirea furnizării și a utilizării portofelelor

Dacă este necesar pentru a asigura restabilirea furnizării, a activării și a utilizării unei soluții pentru portofel, statele membre întreprind, fără întârzieri nejustificate, următoarele acțiuni:

1. restabilesc furnizarea și utilizarea unităților de portofel furnizate în cadrul respectivei soluții pentru portofel prin emiterea, pentru toți utilizatorii afectați, a unei unități de portofel în cadrul unei noi versiuni a soluției portofelului;

2. emit noi atestate ale unității de portofel pentru noi unități de portofel sau, dacă este cazul, pentru unități de portofel emise anterior, cu condiția ca respectivele unitățile de portofel să îndeplinească cerințele de securitate în vigoare după remedierea încălcării securității sau a compromiterii;

3. abrogă orice măsură care a fost pusă în aplicare în temeiul articolului 4 și care împiedică furnizarea de noi unități de portofel în cadrul soluției de portofel afectate, în cazul în care măsura respectivă a fost legată exclusiv de încălcarea sau compromiterea securității remediată între timp.

Articolul 7

Informații privind restabilirea

Atunci când un stat membru restabilește o soluție pentru portofel, acesta se asigură că:

1. aduce acest fapt, fără întârzieri nejustificate, la cunoștința tuturor părților care au primit informații privind suspendarea furnizării și a utilizării respectivei soluției pentru portofel în conformitate cu articolul 5 alineatul (1);

2. informațiile furnizate în conformitate cu punctul 1 includ cel puțin elementele menționate la articolul 5 alineatul (2) literele (a), (b) și (f)-(h), precum și următoarele elemente:

   (a) data și ora la care a fost remediată încălcarea sau compromiterea securității;

   (b) data și ora restabilirii soluției pentru portofel afectate și, după caz, a unităților de portofel afectate furnizate în cadrul respectivei soluții pentru portofel;

   (c) o descriere a măsurilor luate pentru a remedia încălcarea sau compromiterea securității;

   (d) o descriere a impactului rezidual potențial asupra beneficiarilor portofelelor sau asupra utilizatorilor portofelelor și, în acest din urmă caz, dacă este relevant, orice indicații privind măsurile pe care utilizatorii portofelelor le pot lua pentru a atenua respectivele impacturi reziduale potențiale.

Articolul 8

Retragerea portofelelor

(1) În cazul în care o încălcare a securității sau o compromitere care a condus la suspendarea furnizării și a utilizării unei soluții pentru portofel nu este remediată în termen de trei luni de la data suspendării furnizării și a utilizării respectivei soluții pentru portofel, statul membru care furnizează soluția pentru portofel în cauză asigură, fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la expirarea perioadei de trei luni, retragerea soluției pentru portofel afectate și revocarea validității acesteia.

(2) Atunci când un stat membru revocă o soluție pentru portofel, acesta se asigură că:

(a) atestatele unității de portofel din cadrul soluției pentru portofel care a fost afectată sunt revocate;

(b) atestatele de unitate ale portofelului nu pot redeveni valabile;

(c) nu se poate elibera niciun nou atestat al unității de portofel pentru unitățile de portofel existente furnizate în cadrul soluției pentru portofel afectate;

(d) în plus, nu ar trebui să se furnizeze nicio unitate de portofel nouă în cadrul soluției pentru portofel afectate.

(3) Măsurile prevăzute la alineatele (1) și (2) nu îi împiedică pe utilizatorii portofelelor să își exercite dreptul la portabilitatea datelor prevăzut la articolul 5a alineatul (4) litera (g) din Regulamentul (UE) nr. 910/2014. Acest lucru este condiționat de faptul că acest drept poate fi exercitat de utilizatorii portofelelor fără a compromite securitatea activelor critice ale unităților de portofel afectate, în special având în vedere motivele retragerii și necesitatea de a asigura protecția efectivă a activelor respective împotriva utilizării abuzive.

Articolul 9

Informații privind retragerea

(1) Se transmit, fără întârzieri nejustificate și în termen de cel mult 24 de ore de la retragerea unei soluții pentru portofel, informații clare, cuprinzătoare și ușor accesibile cu privire la retragerea respectivei soluții pentru portofel către:

(a) punctele unice de contact desemnate în temeiul articolului 46c alineatul (1) din Regulamentul (UE) nr. 910/2014;

(b) Comisie;

(c) utilizatorii afectați ai portofelelor;

(d) beneficiarii portofelelor înregistrați în conformitate cu articolul 5b din Regulamentul (UE) nr. 910/2014.

(2) Informațiile furnizate în conformitate cu alineatul (1) includ cel puțin următoarele:

(a) numele furnizorului soluției pentru portofel care a fost retrasă;

(b) denumirea și identificatorul de referință ale respectivei soluții pentru portofel, astfel cum sunt menționate în lista portofelelor certificate întocmită în temeiul articolului 5d din Regulamentul (UE) nr. 910/2014 și, după caz, în versiunile aferente;

(c) data și ora detectării încălcării securității sau a compromiterii care a condus la retragerea soluției pentru portofel afectate ca urmare a gravității acesteia sau a faptului că nu a fost remediată în termen de trei luni;

(d) dacă se cunosc, data și ora la care încălcarea securității sau compromiterea a devenit efectivă, pe baza jurnalelor de rețea sau de sistem sau a altor surse de date;

(e) data și ora retragerii soluției pentru portofel și a revocării efective a atestatelor unităților de portofel furnizate în cadrul soluției pentru portofel;

(f) o mențiune prin care se arată dacă retragerea este rezultatul gravității încălcării securității sau al gravității compromiterii sau este consecința faptului că respectiva încălcare a securității sau compromitere nu a fost remediată;

(g) datele de contact, inclusiv cel puțin o adresă de e-mail și un număr de telefon pentru statul membru notificator și, în cazul în care acestea sunt diferite, pentru furnizorul portofelului menționat la litera (a);

(h) o descriere a încălcării securității sau a compromiterii;

(i) o descriere a datelor compromise, inclusiv, după caz, categoriile de date cu caracter personal, astfel cum sunt specificate la articolul 9 alineatul (1) și la articolul 10 din Regulamentul (UE) 2016/679;

(j) dacă este posibil, o estimare a numărului aproximativ al utilizatorilor de portofele afectați și al altor persoane fizice afectate;

(k) o descriere a impactului potențial asupra beneficiarilor sau a utilizatorilor portofelelor și, în acest din urmă caz, dacă este relevant, orice indicații privind măsurile pe care utilizatorii portofelelor le pot lua pentru a atenua respectivul impact potențial;

(l) o descriere a măsurilor luate sau planificate pentru direcționarea utilizatorilor de portofele afectați către soluții sau servicii alternative pentru portofel, atunci când acest lucru este posibil și oportun.

Articolul 10

Sistemul de informații

Statele membre transmit informațiile prevăzute la articolele 3, 5, 7 și 9 Comisiei și punctelor unice de contact ale statelor membre desemnate în temeiul articolului 46c alineatul (1) din Regulamentul (UE) nr. 910/2014, prin intermediul sistemului CIRAS gestionat de ENISA sau al unui sistem echivalent aprobat de statele membre și de Comisie.

Articolul 11

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, cu excepția articolului 10, care se aplică de la 7 mai 2026.

Adoptat la Bruxelles, 6 mai 2025.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXĂ

Criterii de evaluare a unei încălcări a securității sau a unei compromiteri

1. Statele membre își bazează evaluările privind o încălcare a securității sau o compromitere pe următoarele criterii:

   (a) încălcarea securității sau compromiterea a cauzat sau poate cauza decesul unei persoane fizice sau daune considerabile asupra sănătății unei persoane fizice;

   (b) a avut loc sau poate avea loc cu succes un acces presupus răuvoitor sau neautorizat la rețeaua și la sistemele informatice ale unui furnizor de portofel, ale unui furnizor al mecanismelor de validare menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 sau al unui furnizor al unui sistem de identificare electronică în cadrul căruia este furnizată o soluție pentru portofel („entitățile în cauză"), într-un mod care poate cauza perturbări operaționale grave, iar sistemele respective sunt componente critice ale soluției pentru portofel afectate, ale mecanismelor de validare afectate menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 sau ale sistemului de identificare electronică afectat în cadrul căruia este furnizată o soluție pentru portofel;

   (c) o soluție pentru portofel, un mecanism de validare astfel cum este menționat la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 sau un sistem de identificare electronică în cadrul căruia este furnizată o soluție pentru portofel sau o parte a acestora:

      — este complet indisponibil sau se preconizează că va fi complet indisponibil pentru utilizatorii portofelelor sau pentru beneficiarii portofelelor timp de mai mult de 12 ore consecutive;

      — este indisponibil sau se preconizează că va fi indisponibil pentru utilizatorii portofelelor sau pentru beneficiarii portofelelor timp de mai mult de 16 ore într-o săptămână calendaristică;

   (d) se suspectează că peste 1 % dintre utilizatorii portofelelor sau beneficiarii portofelelor sunt afectați sau se preconizează că aceștia vor fi afectați de disponibilitatea limitată a soluției pentru portofel sau a serviciilor furnizate de entitățile în cauză în ceea ce privește soluția pentru portofel;

   (e) există o capacitate de compromitere sau a existat o compromitere în ceea ce privește accesul fizic (limitat la personalul de încredere al entităților în cauză) sau în ceea ce privește protecția unui astfel de acces fizic la una sau mai multe dintre locațiile rețelelor și ale sistemelor informatice care sprijină soluția pentru portofel, furnizarea mecanismelor de validare menționate la articolul 5a alineatul (8) din Regulamentul (UE) nr. 910/2014 aferente unei soluții pentru portofel sau sistemul de identificare electronică în cadrul căruia este furnizată o soluție pentru portofel;

   (f) caracterul privat, integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate în soluția pentru portofel sunt compromise sau pot fi compromise în unul sau mai multe dintre următoarele moduri:

      — incidentul are un impact asupra a peste 1 % dintre utilizatorii portofelelor din cadrul soluției pentru portofel afectate sau asupra a peste 100 000 dintre respectivii utilizatori ai portofelului, luându-se în considerare numărul cel mai mic;

      — incidentul este rezultatul unei activități despre care se presupune că a fost răuvoitoare și care și-a atins scopul;

      — incidentul este rezultatul sau este probabil să fie rezultatul uneia sau mai multor vulnerabilități cunoscute, inclusiv al celor gestionate în conformitate cu Regulamentul de punere în aplicare (UE) 2024/2981 al Comisiei ([1]);

      — este probabil ca incidentul să aibă un impact asupra datelor cu caracter personal într-un mod care este probabil să conducă la apariția unor riscuri la adresa drepturilor și libertăților persoanei fizice în cauză, în special în cazul unei încălcări a confidențialității datelor cu caracter personal astfel cum sunt definite la articolul 9 alineatul (1) și la articolul 10 din Regulamentul (UE) 2016/679;

([1]) Regulamentul de punere în aplicare (UE) 2024/2981 al Comisiei din 28 noiembrie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește integritatea și funcționalitățile de bază ale portofelelor europene pentru identitatea digitală (JO L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— incidentul este probabil să aibă un impact asupra comunicațiilor electronice personale;

— incidentul este probabil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice;

— incidentul este probabil să aibă un impact asupra unor persoane fizice vulnerabile;

(g) certificarea soluției pentru portofel a fost anulată sau se preconizează că va fi anulată;

(h) încălcarea sau compromiterea securității a cauzat sau poate cauza pierderi financiare directe pentru o entitate în cauză, iar aceste pierderi depășesc 500 000 EUR sau, dacă este cazul, 5 % din cifra de afaceri anuală totală a entității în cauză aferentă exercițiului financiar anterior, reținându-se valoarea cea mai mică.

2. Statele membre nu iau în considerare consecințele planificate ale unei operațiuni de întreținere efectuate de entitățile în cauză sau în numele acestora, cu condiția ca o astfel de operațiune de întreținere:

(a) să nu fi fost notificată în prealabil utilizatorilor de portofele potențial afectați, beneficiarilor portofelelor și organismelor de supraveghere competente relevante;

(b) să nu îndeplinească niciunul dintre criteriile stabilite la punctul 1 din prezenta anexă.

3. În ceea ce privește punctul 1 litera (c), durata unui incident care afectează disponibilitatea se măsoară din momentul în care furnizarea corespunzătoare a serviciului afectat este perturbată până în momentul în care serviciul este restabilit și redevine operațional. În cazul în care o entitate în cauză nu este în măsură să determine momentul în care a început perturbarea, durata incidentului este măsurată din momentul în care a fost detectat incidentul sau din momentul în care a fost înregistrat incidentul în jurnalele de rețea sau de sistem sau în alte surse de date, luându-se în considerare data care survine mai întâi. Indisponibilitatea completă a unui serviciu este măsurată din momentul în care serviciul este complet indisponibil pentru utilizatori până în momentul în care activitățile sau operațiunile obișnuite au fost restabilite la nivelul serviciului furnizat înainte de incident. În cazul în care o entitate în cauză nu este în măsură să determine momentul în care a început indisponibilitatea completă unui serviciu, indisponibilitatea este evaluată din momentul în care a fost detectată de entitatea respectivă.

4. În ceea ce privește punctul 1 litera (d), se consideră că o situație de disponibilitate limitată a unui serviciu se produce în special atunci când un serviciu este mult mai lent decât timpul mediu de răspuns sau atunci când nu sunt disponibile toate funcționalitățile unui serviciu. Atunci când este posibil, pentru a evalua întârzierile în ceea ce privește timpul de răspuns ar trebui utilizate criterii obiective bazate pe timpii medii de răspuns ai serviciilor.

5. În scopul stabilirii pierderilor financiare rezultate în urma unei încălcări sau a unei compromiteri menționate la punctul 1 litera (h), entitățile în cauză iau în considerare toate pierderile financiare pe care le-au suferit ca urmare a incidentului, cum ar fi costurile pentru înlocuirea sau mutarea software-ului, a hardware-ului sau a infrastructurii, costurile cu personalul, inclusiv costurile asociate înlocuirii sau mutării personalului, recrutării de personal suplimentar, remunerării orelor suplimentare și recuperării competențelor pierdute sau afectate, taxele datorate ca urmare a nerespectării obligațiilor contractuale, costurile aferente reparațiilor și despăgubirilor datorate clienților, pierderile cauzate de veniturile nerealizate, costurile aferente comunicării interne și externe și costurile de consiliere, inclusiv costurile aferente consilierii juridice, serviciilor de expertiză criminalistică și serviciilor de remediere. Costurile necesare pentru funcționarea zilnică a activității, cum ar fi costurile pentru întreținerea generală a infrastructurii, a echipamentelor, a hardware-ului și a software-ului și pentru îmbunătățiri și inițiativele de evaluare a riscurilor, precum și costurile aferente primelor de asigurare nu sunt considerate pierderi financiare rezultate în urma unui incident. Entitățile în cauză calculează cuantumurile pierderilor financiare pe baza datelor disponibile și, în cazul în care cuantumurile efective ale pierderilor financiare nu pot fi determinate, entitățile estimează cuantumurile respective.