UNIUNEA EUROPEANĂ

PARLAMENTUL EUROPEAN **CONSILIUL**

Bruxelles, 11 aprilie 2024
(OR. en)

2021/0136(COD)
LEX 2318

PE-CONS 68/1/23
REV 1

TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237

REGULAMENT
AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI
DE MODIFICARE A REGULAMENTULUI (UE) NR. 910/2014
ÎN CEEA CE PRIVEȘTE INSTITUIREA
CADRULUI EUROPEAN PENTRU IDENTITATEA DIGITALĂ

REGULAMENTUL (UE) 2024/…
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

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 Comitetului Economic și Social European[1],

având în vedere avizul Comitetului Regiunilor[2],

hotărând în conformitate cu procedura legislativă ordinară[3],

---

1 JO C 105, 4.3.2022, p. 81.
2 JO C 61, 4.2.2022, p. 42.
3 Poziția Parlamentului European din 29 februarie 2024 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 26 martie 2024.

întrucât:

(1) Comunicarea Comisiei din 19 februarie 2020 intitulată „Conturarea viitorului digital al Europei” anunță o revizuire a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului[4] pentru a-i îmbunătăți eficacitatea, a extinde beneficiile acestuia la sectorul privat și a promova identitățile digitale de încredere pentru toți europenii.

(2) În concluziile sale din 1-2 octombrie 2020, Consiliul European a invitat Comisia să propună elaborarea unui cadru la nivelul întregii Uniuni referitor la identificarea electronică publică securizată, inclusiv semnăturile digitale interoperabile, cu scopul de a le oferi persoanelor controlul asupra identității și datelor lor online, precum și de a le permite accesul la servicii digitale publice, private și transfrontaliere.

(3) Programul de politică pentru 2030 privind deceniul digital, instituit prin Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului[5], stabilește obiectivele și țintele digitale ale unui cadru al Uniunii care, până în 2030, sunt menite să conducă la implementarea pe scară largă a unei identități digitale de încredere, voluntare și controlate de utilizator, care să fie recunoscută în întreaga Uniune și care să permită fiecărui utilizator să aibă controlul asupra propriilor date în cadrul interacțiunilor în mediul online.

---

4 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).

5 Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului din 14 decembrie 2022 de instituire a programului de politică pentru 2030 privind deceniul digital (JO L 323, 19.12.2022, p. 4).

(4) „Declarația europeană privind drepturile și principiile digitale pentru deceniul digital” proclamată de Parlamentul European, Consiliu și Comisie[6] (denumită în continuare „declarația”) subliniază dreptul fiecărei persoane de a avea acces la tehnologii, produse și servicii digitale care, din momentul conceperii, sunt sigure și securizate și protejează viața privată. Aceasta include asigurarea faptului că tuturor persoanelor care trăiesc în Uniune li se oferă o identitate digitală accesibilă, securizată și de încredere care să permită accesul la o gamă largă de servicii online și offline, protejată împotriva riscurilor de securitate cibernetică și a criminalității informatice, inclusiv împotriva încălcării securității datelor și a furtului de identitate sau a manipulării identității. Declarația prevede, de asemenea, că fiecare persoană are dreptul la protecția datelor sale cu caracter personal. Acest drept include controlul asupra modului în care sunt utilizate datele și asupra celor cu care sunt partajate datele.

(5) Toți cetățenii Uniunii și rezidenții din Uniune ar trebui să aibă dreptul la o identitate digitală care să se afle sub controlul lor exclusiv și care să le permită să își exercite drepturile în mediul digital și să participe la economia digitală. Pentru atingerea acestui obiectiv, ar trebui să fie instituit un cadru european pentru identitatea digitală care să le permită cetățenilor Uniunii și rezidenților din Uniune să aibă acces la servicii publice și private online și offline în întreaga Uniune.

(6) Un cadru armonizat privind identitatea digitală ar trebui să contribuie la crearea unei Uniuni mai integrate din punct de vedere digital, prin reducerea barierelor digitale dintre statele membre și prin capacitarea cetățenilor Uniunii și a rezidenților din Uniune să se bucure de avantajele digitalizării, sporind în același timp transparența și protecția drepturilor lor.

---

[6] JO C 23, 23.1.2023, p. 1.

(7) O abordare mai armonizată a identificării electronice ar trebui să reducă riscurile și costurile fragmentării actuale cauzate de utilizarea unor soluții naționale divergente sau, în unele state membre, de lipsa unor astfel de soluții de identificare electronică. O astfel de abordare ar trebui să consolideze piața internă, permițând cetățenilor Uniunii, rezidenților din Uniune, astfel cum sunt definiți în dreptul intern, și întreprinderilor să se identifice și să furnizeze autentificarea identității lor online și offline într-un mod sigur, demn de încredere, ușor de utilizat, convenabil, accesibil și armonizat în întreaga Uniune. Portofelul european pentru identitatea digitală ar trebui să ofere persoanelor fizice și juridice din întreaga Uniune un mijloc armonizat de identificare electronică care să permită autentificarea și partajarea datelor legate de identitatea lor. Orice persoană ar trebui să poată avea acces în condiții de siguranță la serviciile publice și private cu ajutorul unui ecosistem îmbunătățit de servicii de încredere și al unor dovezi ale identității și atestate electronice ale atributelor verificate, cum sunt de exemplu calificările academice, inclusiv diplomele universitare sau alte calificări educaționale sau profesionale. Cadrul european pentru identitatea digitală este menit să realizeze o tranziție de la utilizarea în mod exclusiv a soluțiilor naționale de identitate digitală la furnizarea de atestate electronice ale atributelor, valabile și recunoscute legal în întreaga Uniune. Furnizorii de atestate electronice ale atributelor ar trebui să beneficieze de un set de norme clar și uniform, în timp ce administrațiile publice ar trebui să se poată baza pe documente electronice într-un format determinat.

(8) O serie de state membre au implementat și utilizează mijloace de identificare electronică ce sunt acceptate de prestatorii de servicii din Uniune. În plus, s-au realizat investiții în soluții naționale și transfrontaliere pe baza Regulamentului (UE) nr. 910/2014, inclusiv în ceea ce privește interoperabilitatea sistemelor de identificare electronică notificate în temeiul regulamentului respectiv. Pentru a asigura complementaritatea și adoptarea rapidă a portofelelor europene pentru identitatea digitală de către utilizatorii actuali ai mijloacelor de identificare electronică notificate, precum și pentru a reduce la minim impactul asupra prestatorilor de servicii existenți, se consideră că portofelele europene pentru identitatea digitală ar trebui să fructifice experiența dobândită cu mijloacele de identificare electronică existente și să profite de infrastructura sistemelor de identificare electronică notificate implementate la nivelul Uniunii și la nivel național.

(9) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[7] și, după caz, Directiva 2002/58/CE a Parlamentului European și a Consiliului[8] se aplică tuturor activităților de prelucrare a datelor cu caracter personal în temeiul Regulamentului (UE) nr. 910/2014. Soluțiile în temeiul cadrului de interoperabilitate prevăzut în prezentul regulament respectă, de asemenea, normele respective. Dreptul Uniunii în materie de protecție a datelor prevede principii de protecție a datelor, cum ar fi principiul și obligațiile privind reducerea la minimum a datelor și limitarea scopului, cum ar fi protecția datelor începând cu momentul conceperii și în mod implicit.

---

7 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).

8 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).

(10) Pentru a sprijini competitivitatea întreprinderilor Uniunii, prestatorii de servicii atât online cât și offline ar trebui să se poată baza pe soluții de identitate digitală recunoscute în întreaga Uniune, indiferent de statul membru în care soluțiile respective sunt puse la dispoziție, și să beneficieze astfel de o abordare europeană armonizată în materie de încredere, securitate și interoperabilitate. Atât utilizatorii, cât și prestatorii de servicii ar trebui să poată beneficia de atestate electronice ale atributelor care să aibă aceeași valoare juridică în întreaga Uniune. Un cadru armonizat privind identitatea digitală este menit să creeze valoare economică prin facilitarea accesului la bunuri și servicii și prin reducerea semnificativă a costurilor operaționale legate de procedurile de identificare și de autentificare electronică, de exemplu în timpul integrării noilor clienți, prin reducerea potențialului de criminalitate informatică, cum ar fi furtul de identitate, furtul de date și frauda online, promovând astfel creșterea eficienței și transformarea digitală sigură a microîntreprinderilor și a întreprinderilor mici și mijlocii (IMM-uri) din Uniune.

(11) Portofelele europene pentru identitatea digitală ar trebui să faciliteze aplicarea principiului „doar o singură dată”, reducând astfel sarcina administrativă și sprijinind mobilitatea transfrontalieră a cetățenilor Uniunii și rezidenților din Uniune și a întreprinderilor din întreaga Uniune și promovând dezvoltarea unor servicii interoperabile de e-guvernare în întreaga Uniune.

(12) Regulamentul (UE) 2016/679, Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[9] și Directiva 2002/58/CE se aplică prelucrării datelor cu caracter personal în contextul punerii în aplicare a prezentului regulament. Prin urmare, prezentul regulament ar trebui să prevadă garanții specifice pentru a împiedica furnizorii de mijloace de identificare electronică și de atestare electronică a atributelor să combine datele cu caracter personal obținute atunci când prestează alte servicii cu datele cu caracter personal prelucrate pentru a presta serviciile care intră în domeniul de aplicare al prezentului regulament. Datele cu caracter personal legate de furnizarea de portofele europene pentru identitatea digitală ar trebui păstrate separate logic de orice alte date deținute de furnizorul portofelului european pentru identitatea digitală. Prezentul regulament nu ar trebui să îi împiedice pe furnizorii de portofele europene pentru identitatea digitală să aplice măsuri tehnice suplimentare care să contribuie la protecția datelor cu caracter personal, cum ar fi separarea fizică a datelor cu caracter personal legate de furnizarea portofelelor europene pentru identitatea digitală de orice alte date deținute de furnizor. Fără a aduce atingere Regulamentului (UE) 2016/679, prezentul regulament precizează mai detaliat aplicarea principiilor limitării scopului, reducerii la minimum a datelor și protecției datelor începând cu momentul conceperii și în mod implicit.

[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).

(13) Portofelele europene pentru identitatea digitală ar trebui să aibă încorporată prin concepție funcția de tablou de bord comun, pentru a asigura un grad mai mare de transparență, de protejare a vieții private și de control al utilizatorilor asupra datelor cu caracter personal proprii. Funcția respectivă ar trebui să ofere o interfață simplă și ușor de utilizat care să ofere o imagine de ansamblu a tuturor beneficiarilor cu care utilizatorul partajează date, inclusiv atribute, precum și tipul de date partajate cu fiecare beneficiar. Aceasta ar trebui să le permită utilizatorilor să urmărească toate tranzacțiile executate prin intermediul portofelului european pentru identitatea digitală cu cel puțin următoarele date: ora și data tranzacției, identificarea contrapărții, datele cu caracter personal solicitate și datele partajate. Informațiile respective ar trebui să fie stocate chiar dacă tranzacția nu a fost încheiată. Nu ar trebui să fie posibilă negarea autenticității informațiilor conținute în istoricul tranzacțiilor. O astfel de funcție ar trebui să fie activă în mod implicit. Aceasta ar trebui să le permită utilizatorilor să solicite cu ușurință ștergerea imediată de către un beneficiar a datele cu caracter personal în temeiul articolului 17 din Regulamentul (UE) 2016/679 și să raporteze cu ușurință beneficiarul autorității naționale competente pentru protecția datelor în cazul în care se primește o cerere presupus ilegală sau suspectă de date cu caracter personal, direct de la portofelul european pentru identitatea digitală.

(14) Statele membre ar trebui să integreze diferite tehnologii de protejare a vieții private, cum ar fi dovada de zero cunoștințe („zero knowledge proof”), în portofelul european pentru identitatea digitală. Aceste metode criptografice ar trebui să permită unui beneficiar să valideze dacă o anumită declarație bazată pe datele de identificare ale persoanei și pe atestarea atributelor este adevărată, fără a dezvălui datele pe care se bazează declarația respectivă, protejând astfel viața privată a utilizatorului.

(15) Prezentul regulament stabilește condiții armonizate pentru instituirea unui cadru corespunzător pentru portofelele europene pentru identitatea digitală care urmează să fie furnizate de statele membre. Toți cetățenii Uniunii, precum și rezidenții din Uniune, astfel cum sunt definiți în dreptul intern, ar trebui să fie abilitați să solicite, să selecteze, să combine, să stocheze, să șteargă, să partajeze și să prezinte în condiții de siguranță date privind identitatea lor și să solicite ștergerea datelor lor cu caracter personal într-un mod ușor de utilizat și practic, exclusiv sub controlul utilizatorului, permițând în același timp divulgarea selectivă a datelor cu caracter personal. Prezentul regulament reflectă valorile europene comune și respectă drepturile fundamentale, garanțiile juridice și răspunderea, protejând astfel societățile democratice, cetățenii Uniunii și rezidenții din Uniune. Tehnologiile utilizate pentru atingerea acestor obiective ar trebui să fie dezvoltate cu scopul de a se atinge cel mai înalt nivel de securitate, de confidențialitate, de confort pentru utilizatori, de accesibilitate, de utilizare pe scară largă și de interoperabilitate neîntreruptă. Statele membre ar trebui să asigure accesul egal la identificarea electronică pentru toți cetățenii și rezidenții lor. Statele membre nu ar trebui să limiteze, în mod direct sau indirect, accesul la serviciile publice sau private pentru persoanele fizice sau juridice care nu optează pentru utilizarea portofelelor europene pentru identitatea digitală și ar trebui să pună la dispoziție soluții alternative adecvate.

(16) Statele membre ar trebui să se bazeze pe posibilitățile oferite de prezentul regulament pentru a furniza, sub responsabilitatea lor, portofele europene pentru identitatea digitală în vederea utilizării de către persoanele fizice și juridice care își au reședința pe teritoriul lor. Pentru a oferi statelor membre flexibilitate și a valorifica tehnologia de ultimă generație, prezentul regulament ar trebui să permită furnizarea portofelelor europene pentru identitatea digitală direct de către un stat membru, în temeiul unui mandat din partea unui stat membru sau independent de un stat membru, dar recunoscute de statul membru respectiv.

(17) În scopul înregistrării, beneficiarii ar trebui să furnizeze informațiile necesare pentru a permite identificarea și autentificarea lor electronică către portofelele europene pentru identitatea digitală. Atunci când declară utilizarea preconizată a portofelului european pentru identitatea digitală, beneficiarii ar trebui să furnizeze informații cu privire la datele pe care le vor solicita, dacă este cazul, pentru a-și furniza serviciile și la motivul cererii. Înregistrarea beneficiarului facilitează verificarea de către statele membre a legalității activităților beneficiarilor în conformitate cu dreptul Uniunii. Obligația de înregistrare prevăzută în prezentul regulament nu ar trebui să aducă atingere obligațiilor prevăzute în alte dispoziții de drept al Uniunii sau de drept intern, cum ar fi informațiile care trebuie să fie furnizate persoanelor vizate în temeiul Regulamentului (UE) 2016/679. Beneficiarii ar trebui să asigure garanțiile oferite de articolele 35 și 36 din regulamentul respectiv, în special prin realizarea unor evaluări ale impactului asupra protecției datelor și prin consultarea autorităților competente pentru protecția datelor înainte de prelucrarea datelor în cazul în care evaluările impactului asupra protecției datelor indică faptul că prelucrarea ar conduce la un risc ridicat. Astfel de garanții ar trebui să sprijine prelucrarea legală a datelor cu caracter personal de către beneficiari, în special în ceea ce privește categoriile speciale de date, cum ar fi datele privind sănătatea. Înregistrarea beneficiarilor este menită să sporească transparența și încrederea în utilizarea portofelelor europene pentru identitatea digitală. Înregistrarea ar trebui să fie eficientă din punctul de vedere al costurilor și proporțională cu riscurile aferente, pentru a asigura adoptarea de către prestatorii de servicii. În acest context, înregistrarea ar trebui să prevadă utilizarea unor proceduri automatizate, inclusiv recurgerea la registrele existente și utilizarea acestora de către statele membre, și nu ar trebui să implice un proces de preautorizare. Procesul de înregistrare ar trebui să permită o varietate de cazuri de utilizare care pot fi diferite în ceea ce privește modul de operare, fie online, fie offline, sau în ceea ce privește cerința de autentificare a dispozitivelor în scopul interfeței cu portofelul european pentru identitatea digitală. Înregistrarea ar trebui să se aplice exclusiv beneficiarilor care furnizează servicii prin intermediul interacțiunii digitale.

(18) Protejarea cetățenilor Uniunii și a rezidenților din Uniune împotriva utilizării neautorizate sau frauduloase a portofelelor europene pentru identitatea digitală este extrem de importantă pentru asigurarea încrederii în portofelele europene pentru identitatea digitală și pentru adoptarea pe scară largă a acestora. Utilizatorii ar trebui să beneficieze de o protecție eficace împotriva unei astfel de utilizări abuzive. În special, atunci când faptele care stau la baza utilizării frauduloase sau ilegale în alt mod a unui portofel european pentru identitatea digitală sunt constatate de o autoritate judiciară națională în contextul unei alte proceduri, organismele de supraveghere care sunt responsabile de emitenții portofelului european pentru identitatea digitală ar trebui, după notificare, să ia măsurile necesare pentru a se asigura că înregistrarea beneficiarului și includerea beneficiarilor în mecanismul de autentificare sunt retrase sau suspendate până când autoritatea de notificare confirmă că neregulile identificate au fost remediate.

(19) Toate portofelele europene pentru identitatea digitală ar trebui să le permită utilizatorilor identificarea și autentificarea electronică online și offline, la nivel transfrontalier, în vederea accesării unei game largi de servicii publice și private. Fără a aduce atingere prerogativelor statelor membre în ceea ce privește identificarea cetățenilor și rezidenților lor, portofelele europene pentru identitatea digitală pot răspunde și nevoilor instituționale ale administrațiilor publice, ale organizațiilor internaționale și ale instituțiilor, organelor, oficiilor și agențiilor Uniunii. Autentificarea offline ar fi importantă în numeroase sectoare, inclusiv în sectorul sănătății, unde serviciile sunt adesea furnizate prin interacțiune directă și unde verificarea autenticității prescripțiilor electronice ar trebui să se poată face cu ajutorul codurilor QR sau al unor tehnologii similare. Bazate fiind pe nivelul de asigurare ridicat în ceea ce privește sistemele de identificare electronică, portofelele europene pentru identitatea digitală ar trebui să profite de potențialul oferit de soluțiile inviolabile, cum ar fi elementele de securitate, pentru a respecta cerințele în materie de securitate prevăzute în prezentul regulament. De asemenea, portofelele europene pentru identitatea digitală ar trebui să le permită utilizatorilor să creeze și să utilizeze semnături și sigilii electronice calificate care sunt acceptate în întreaga Uniune. Odată ce s-au integrat în sistemul reprezentat de portofelul european pentru identitatea digitală, persoanele fizice ar trebui să îl poată utiliza pentru a semna cu semnături electronice calificate, în mod implicit și gratuit, fără a fi nevoite să parcurgă proceduri administrative suplimentare. Utilizatorii ar trebui să poată să semneze sau să sigileze afirmațiile sau atributele autorevendicate. Pentru a obține beneficii în materie de simplificare și de reducere a costurilor pentru persoanele și întreprinderile din întreaga Uniune, inclusiv prin validarea competențelor de reprezentare și a mandatelor electronice, statele membre ar trebui să furnizeze portofele europene pentru identitatea digitală care să se bazeze pe standarde și specificații tehnice comune pentru a asigura interoperabilitatea neîntreruptă și a spori în mod adecvat nivelul de securitate informatică, pentru a consolida robustețea împotriva atacurilor cibernetice și a reduce, astfel, în mod semnificativ riscurile potențiale ale digitalizării în curs pentru cetățenii Uniunii, rezidenții din Uniune și întreprinderi.

Numai autoritățile competente ale statelor membre pot oferi un nivel ridicat de încredere în stabilirea identității unei persoane și astfel pot oferi garanția că persoana care pretinde sau declară o anumită identitate este într-adevăr persoana care pretinde că este. Prin urmare, furnizarea portofelelor europene pentru identitatea digitală este necesar să se bazeze pe recurgerea la identitatea juridică a cetățenilor Uniunii, a rezidenților din Uniune sau a persoanelor juridice. Recurgerea la identitatea juridică nu ar trebui să împiedice utilizatorii portofelului european pentru identitatea digitală să acceseze servicii sub un pseudonim, în cazul în care nu există nicio cerință legală privind identitatea juridică pentru autentificare. Încrederea în portofelele europene pentru identitatea digitală ar fi consolidată prin faptul că părților emitente și celor care le gestionează li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura cel mai ridicat nivel de securitate care să fie proporțional cu riscurile la adresa drepturilor și libertăților persoanelor fizice, în conformitate cu Regulamentul (UE) 2016/679.

(20) Utilizarea unei semnături electronice calificate ar trebui să fie gratuită pentru toate persoanele fizice în scopuri neprofesionale. Statele membre ar trebui să aibă posibilitatea să prevadă măsuri de prevenire a utilizării gratuite a semnăturilor electronice calificate în scopuri profesionale de către persoanele fizice, asigurându-se, în același timp, că orice astfel de măsuri sunt proporționale cu riscurile identificate și sunt justificate.

(21) Este benefic să se faciliteze adoptarea pe scară largă și utilizarea portofelelor europene pentru identitatea digitală prin integrarea fără sincope a acestora în ecosistemul serviciilor digitale publice și private deja implementate la nivel național, local sau regional. Pentru a atinge acest obiectiv, ar trebui să fie posibil pentru statele membre să prevadă măsuri juridice și organizatorice pentru a spori flexibilitatea pentru furnizorii de portofele europene pentru identitatea digitală și pentru a permite funcționalități suplimentare ale portofelelor europene pentru identitatea digitală față de cele prevăzute în prezentul regulament, inclusiv printr-o interoperabilitate sporită cu mijloacele naționale de identificare electronică existente. Aceste funcționalități suplimentare nu ar trebui în niciun caz să fie în detrimentul asigurării funcțiilor de bază ale portofelelor europene pentru identitatea digitală prevăzute în prezentul regulament sau să promoveze soluțiile naționale existente în detrimentul portofelelor europene pentru identitatea digitală. Întrucât depășesc cadrul prezentului regulament, aceste funcționalități suplimentare nu intră sub incidența dispozițiilor privind utilizarea transfrontalieră a portofelelor europene pentru identitatea digitală prevăzute în prezentul regulament.

(22) Portofelele europene pentru identitatea digitală ar trebui să includă o funcționalitate care să genereze pseudonime alese și gestionate de utilizator, în vederea autentificării atunci când se accesează servicii online.

(23) Pentru a atinge un nivel ridicat de securitate și fiabilitate, prezentul regulament stabilește cerințele în ceea ce privește portofelele europene pentru identitate digitală. Conformitatea portofelelor europene pentru identitatea digitală cu cerințele respective ar trebui să fie certificată de organisme acreditate de evaluare a conformității desemnate de statele membre.

(24) Pentru a evita abordările divergente și a armoniza punerea în aplicare a cerințelor prevăzute în prezentul regulament, în vederea certificării portofelelor europene pentru identitatea digitală, Comisia ar trebui să adopte acte de punere în aplicare prin care să stabilească o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind exprimarea specificațiilor tehnice detaliate ale cerințelor respective. În măsura în care certificarea conformității portofelelor europene pentru identitatea digitală cu cerințele relevante în materie de securitate cibernetică nu intră sub incidența sistemelor existente de certificare a securității cibernetice menționate în prezentul regulament și în ceea ce privește cerințele care nu sunt de securitate cibernetică relevante pentru portofelele europene pentru identitatea digitală, statele membre ar trebui să instituie sisteme naționale de certificare în temeiul cerințelor armonizate prevăzute și adoptate în temeiul prezentului regulament. Statele membre ar trebui să transmită Grupului european de cooperare privind identitatea digitală proiectele lor de sisteme de certificare naționale, iar grupul de cooperare ar trebui să poată emite avize și recomandări.

(25) Certificarea conformității cu cerințele de securitate cibernetică stabilite în prezentul regulament ar trebui, dacă este disponibilă, să se bazeze pe sistemele europene de certificare a securității cibernetice relevante instituite în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului[10], care instituie un cadru european voluntar de certificare a securității cibernetice pentru produsele, procesele și serviciile TIC.

---

[10] 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).

(26) Pentru a evalua și a atenua în permanență riscurile legate de securitate, portofelele europene pentru identitatea digitală certificate ar trebui să facă obiectul unor evaluări periodice ale vulnerabilității menite să detecteze orice vulnerabilitate a componentelor legate de produse certificate, procese certificate și serviciile certificate ale portofelului european pentru identitatea digitală.

(27) Prin protejarea utilizatorilor și a întreprinderilor de riscurile de securitate cibernetică, cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament contribuie, de asemenea, la îmbunătățirea protecției datelor cu caracter personal și a vieții private a persoanelor. Ar trebui avute în vedere sinergii atât în ceea ce privește standardizarea, cât și certificarea cu privire la aspectele legate de securitatea cibernetică prin cooperarea dintre Comisie, organizațiile europene de standardizare, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Comitetul european pentru protecția datelor instituit prin Regulamentul (UE) 2016/679 și autoritățile naționale de supraveghere a protecției datelor.

(28) Integrarea cetățenilor Uniunii și a rezidenților din Uniune în sistemul reprezentat de portofelul european pentru identitatea digitală ar trebui să fie facilitată prin utilizarea mijloacelor de identificare electronică emise cu un nivel de asigurare ridicat. Mijloacele de identificare electronică emise cu un nivel de asigurare substanțial ar trebui să fie utilizate numai în cazul în care specificații tehnice și proceduri armonizate care utilizează mijloace de identificare electronică emise cu un nivel de asigurare substanțial în combinație cu alte mijloace suplimentare de verificare a identității vor permite îndeplinirea cerințelor prevăzute în prezentul regulament în ceea ce privește nivelul de asigurare ridicat. Astfel de mijloace suplimentare ar trebui să fie fiabile și ușor de utilizat și s-ar putea baza pe posibilitatea de a utiliza proceduri de integrare de la distanță, certificate calificate susținute de semnături electronice calificate, atestate electronice calificate ale atributelor sau o combinație a acestora. Pentru a asigura adoptarea pe scară suficient de largă a portofelelor europene pentru identitatea digitală, ar trebui stabilite, prin acte de punere în aplicare, specificații tehnice și proceduri armonizate pentru integrarea utilizatorilor prin utilizarea mijloacelor de identificare electronică, inclusiv a celor emise cu un nivel de asigurare substanțial.

(29) Obiectivul prezentului regulament este de a oferi utilizatorului un portofel european pentru identitatea digitală integral mobil, sigur și ușor de utilizat. Ca măsură tranzitorie până la apariția unor soluții certificate inviolabile, cum ar fi elementele de securitate încorporate în dispozitivele utilizatorilor, portofelele europene pentru identitatea digitală ar trebui să se poată baza pe elemente de securitate certificate externe pentru protecția materialului criptografic și a altor date cu caracter sensibil sau pe mijloace de identificare electronică notificate cu un nivel de asigurare ridicat pentru a demonstra conformitatea cu cerințele relevante ale prezentului regulament în ceea ce privește nivelul de asigurare al portofelului european pentru identitatea digitală. Prezentul regulament nu ar trebui să aducă atingere condițiilor naționale privind emiterea și utilizarea elementelor de securitate certificate externe în cazul în care măsura tranzitorie se bazează pe astfel de elemente.

(30) Portofelele europene pentru identitatea digitală ar trebui să asigure cel mai înalt nivel de protecție și de securitate a datelor în scopul identificării și autentificării electronice pentru a facilita accesul la serviciile publice și private, indiferent dacă aceste date sunt stocate la nivel local sau prin soluții de tip cloud, luând în considerare în mod corespunzător diferitele niveluri de risc.

(31) Portofelele europene pentru identitatea digitală ar trebui să fie securizate de la stadiul conceperii și ar trebui să pună în aplicare elemente de securitate avansate pentru a proteja împotriva furtului de identitate și de alte date, a refuzării serviciului și a oricărei alte amenințări cibernetice. O astfel de securitate ar trebui să includă metode de criptare și stocare de ultimă generație care să fie accesibile numai utilizatorului, care să poată fi decriptate numai de către utilizator și care să se bazeze pe comunicații criptate de la un capăt la altul cu alte portofele europene pentru identitatea digitală și cu beneficiarii. În plus, portofelele europene pentru identitatea digitală ar trebui să necesite o confirmare sigură, explicită și activă din partea utilizatorului pentru operațiunile efectuate prin intermediul portofelelor europene pentru identitatea digitală.

(32) Utilizarea gratuită a portofelelor europene pentru identitatea digitală nu ar trebui să conducă la o prelucrare a datelor mai mult decât este necesar pentru furnizarea de servicii specifice portofelelor europene pentru identitatea digitală. Prezentul regulament nu ar trebui să permită prelucrarea datelor cu caracter personal, stocate în portofelul european pentru identitatea digitală sau care rezultă din utilizarea acestuia, de către furnizorul portofelului european pentru identitatea digitală în alte scopuri decât furnizarea de servicii specifice portofelelor europene pentru identitatea digitală. Pentru a asigura protejarea vieții private, furnizorii de portofele europene pentru identitatea digitală ar trebui să asigure neobservabilitatea prin faptul că nu colectează date și nu cunosc tranzacțiile utilizatorilor portofelului european pentru identitatea digitală. Această neobservabilitate înseamnă că furnizorii nu pot vedea detaliile tranzacțiilor efectuate de utilizator. Cu toate acestea, în cazuri specifice, pe baza consimțământului prealabil explicit al utilizatorului în fiecare dintre aceste cazuri specifice și în deplină conformitate cu Regulamentul (UE) 2016/679, furnizorilor de portofele europene pentru identitatea digitală li s-ar putea acorda acces la informațiile necesare pentru furnizarea unui anumit serviciu legat de portofelele europene pentru identitatea digitală.

(33) Transparența portofelelor europene pentru identitatea digitală și responsabilitatea furnizorilor acestora reprezintă elemente esențiale pentru a crea încredere socială și a declanșa acceptarea cadrului. Prin urmare, funcționarea portofelelor europene pentru identitatea digitală ar trebui să fie transparentă și, în special, să permită prelucrarea verificabilă a datelor cu caracter personal. Pentru a realiza acest lucru, statele membre ar trebui să divulge codul sursă al componentelor de software ale aplicației pentru utilizatori a portofelelor europene pentru identitatea digitală, inclusiv cele care au legătură cu prelucrarea datelor cu caracter personal și a datelor persoanelor juridice. Publicarea acestui cod sursă sub o licență cu sursă deschisă ar trebui să permită societății, inclusiv utilizatorilor și dezvoltatorilor, să înțeleagă funcționarea, să auditeze și să revizuiască codul. Acest lucru ar spori încrederea utilizatorilor în ecosistem și ar contribui la securitatea portofelelor europene pentru identitatea digitală, dând posibilitatea oricărei persoane să raporteze vulnerabilități și erori identificate în cod. În general, acest lucru ar trebui să ofere furnizorilor un stimulent pentru a furniza și a menține un produs foarte sigur. Cu toate acestea, în anumite cazuri, divulgarea codului sursă pentru bibliotecile utilizate, canalul de comunicare sau alte elemente care nu sunt găzduite pe dispozitivul utilizatorului ar putea fi limitată de statele membre, din motive justificate în mod corespunzător, în special în scopul siguranței publice.

(34) Utilizarea portofelelor europene pentru identitatea digitală, precum și întreruperea utilizării acestora ar trebui să fie dreptul exclusiv și alegerea utilizatorilor. Statele membre ar trebui să elaboreze proceduri simple și sigure pentru ca utilizatorii să solicite revocarea imediată a valabilității portofelelor europene pentru identitatea digitală, inclusiv în caz de pierdere sau de furt. În cazul decesului utilizatorului sau al încetării activității unei persoane juridice, ar trebui să fie stabilit un mecanism care să permită autorității responsabile cu stabilirea succesiunii persoanei fizice sau a activelor persoanei juridice să solicite revocarea imediată a portofelelor europene pentru identitatea digitală.

(35) Pentru a promova adoptarea portofelelor europene pentru identitatea digitală și utilizarea pe scară mai largă a identităților digitale, statele membre ar trebui nu numai să promoveze beneficiile serviciilor relevante, ci și, în cooperare cu sectorul privat, cu cercetătorii și cu mediul academic, să dezvolte programe de instruire menite să întărească competențele digitale ale cetățenilor și rezidenților lor, în special pentru grupurile vulnerabile, cum ar fi persoanele cu dizabilități și persoanele în vârstă. Statele membre ar trebui de asemenea să informeze publicul despre beneficiile și riscurile portofelelor europene pentru identitatea digitală prin intermediul campaniilor de comunicare.

(36) Pentru a se asigura faptul că, în ceea ce privește cadrul european pentru identitatea digitală, acesta este deschis inovării, dezvoltării tehnologice și este adaptat exigențelor viitorului, statele membre sunt încurajate să creeze, împreună, spații de testare comune pentru a testa soluții inovatoare într-un mediu controlat și sigur, în special pentru a îmbunătăți funcționalitatea, protecția datelor cu caracter personal, securitatea și interoperabilitatea soluțiilor, precum și pentru a fundamenta viitoarele actualizări în materie de referințe tehnice și cerințe legale. Mediul respectiv ar trebui să încurajeze includerea IMM-urilor, a întreprinderilor nou-înființate și a inovatorilor și cercetătorilor individuali, precum și a părților interesate relevante din industrie. Astfel de inițiative ar trebui să contribuie la respectarea reglementărilor și la robustețea tehnică a portofelelor europene pentru identitatea digitală, și să le consolideze, portofele care urmează să fie furnizate cetățenilor Uniunii și rezidenților din Uniune, prevenind astfel dezvoltarea de soluții care nu respectă dreptul Uniunii privind protecția datelor sau care sunt deschise vulnerabilităților în materie de securitate.

(37) Regulamentul (UE) 2019/1157 al Parlamentului European și al Consiliului[11] prevede întărirea securității cărților de identitate cu elemente de securitate mărită până în august 2021. Statele membre ar trebui să ia în considerare posibilitatea notificării acestora în cadrul sistemelor de identificare electronică, în scopul extinderii disponibilității transfrontaliere a mijloacelor de identificare electronică.

(38) Procesul de notificare a sistemelor de identificare electronică ar trebui să fie simplificat și să fie accelerat pentru a promova accesul la soluții de autentificare și identificare practice, fiabile, sigure și inovatoare și, după caz, pentru a încuraja furnizorii privați de mijloace de identificare să pună la dispoziția autorităților statelor membre sisteme de identificare electronică pentru notificare ca sisteme naționale de identificare electronică în temeiul Regulamentului (UE) nr. 910/2014.

(39) Simplificarea procedurilor actuale de notificare și de evaluare *inter pares* va preveni abordările eterogene ale evaluării diferitelor sisteme de identificare electronică notificate și va facilita consolidarea încrederii între statele membre. Mecanismele noi, simplificate, sunt menite să încurajeze cooperarea dintre statele membre în ceea ce privește securitatea și interoperabilitatea sistemelor de identificare electronică notificate ale acestora.

(40) Statele membre ar trebui să beneficieze de instrumente noi și flexibile pentru a asigura conformitatea cu cerințele prezentului regulament și ale actelor de punere în aplicare relevante adoptate în temeiul acestuia. Prezentul regulament ar trebui să permită statelor membre să utilizeze rapoartele și evaluările efectuate de organismele acreditate de evaluare a conformității, astfel cum se prevede în contextul sistemelor de certificare ce urmează a fi instituite la nivelul Uniunii în temeiul Regulamentului (UE) 2019/881, pentru a-și fundamenta afirmațiile privind alinierea sistemelor sau a unor părți ale acestora la Regulamentul (UE) nr. 910/2014.

---

[11] Regulamentul (UE) 2019/1157 al Parlamentului European și al Consiliului din 20 iunie 2019 privind consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la liberă circulație (JO L 188, 12.7.2019, p. 67).

(41) Prestatorii de servicii publice utilizează datele de identificare personală disponibile prin mijloacele de identificare electronică în temeiul Regulamentului (UE) nr. 910/2014 pentru a corela identitatea electronică a utilizatorilor din alte state membre cu datele de identificare personală furnizate utilizatorilor respectivi în statul membru care efectuează procesul de corelare transfrontalieră a identităților. Cu toate acestea, în multe cazuri, în pofida utilizării setului minim de date furnizate în cadrul sistemelor de identificare electronică notificate, asigurarea unei corespondențe exacte a identității atunci când statele membre acționează în calitate de beneficiari necesită informații suplimentare cu privire la utilizator și proceduri specifice de identificare unică complementară care trebuie efectuate la nivel național. Pentru a sprijini în continuare posibilitățile de utilizare a mijloacelor de identificare electronică, pentru a oferi servicii publice online mai bune și pentru a spori securitatea juridică în ceea ce privește identitatea electronică a utilizatorilor, Regulamentul (UE) nr. 910/2014 ar trebui să solicite statelor membre să ia măsuri online specifice pentru a asigura corelarea fără echivoc a identității atunci când utilizatorii intenționează să acceseze servicii publice transfrontaliere online.

(42) La elaborarea portofelelor europene pentru identitatea digitală, este esențial să fie luate în considerare nevoile utilizatorilor. Ar trebui să fie disponibile cazuri de utilizare și servicii online importante care să se bazeze pe portofelele europene pentru identitatea digitală. Pentru confortul utilizatorilor și pentru a asigura disponibilitatea transfrontalieră a unor astfel de servicii, este important să fie întreprinse acțiuni pentru a facilita o abordare similară în ceea ce privește proiectarea, dezvoltarea și implementarea serviciilor online în toate statele membre. Orientările fără caracter obligatoriu privind modul de proiectare, elaborare și implementare a serviciilor online care se bazează pe portofelele europene pentru identitatea digitală ar putea deveni un instrument util pentru atingerea acestui obiectiv. Astfel de orientări ar trebui să fie elaborate ținând seama de cadrul de interoperabilitate al Uniunii. Statele membre ar trebui să aibă un rol principal în adoptarea acestor orientări.

(43) În conformitate cu Directiva (UE) 2019/882 a Parlamentului European și a Consiliului[12], persoanele cu dizabilități ar trebui să poată utiliza portofelele europene pentru identitatea digitală, serviciile de încredere și produsele destinate utilizatorului final utilizate la prestarea serviciilor respective, în aceleași condiții ca și ceilalți utilizatori.

(44) Pentru a asigura aplicarea eficace a prezentului regulament, ar trebui să se stabilească un nivel minim al amenzilor administrative maxime atât pentru prestatorii de servicii de încredere calificați, cât și pentru cei necalificați. Statele membre ar trebui să prevadă sancțiuni efective, proporționale și cu efect de descurajare. La stabilirea sancțiunilor, ar trebui să se țină seama în mod corespunzător de dimensiunea entităților afectate, de modelele lor de afaceri și de gravitatea încălcărilor.

(45) Statele membre ar trebui să stabilească norme privind sancțiunile care se aplică în cazul unor încălcări cum sunt practicile directe sau indirecte care creează confuzie între serviciile de încredere necalificate și cele calificate sau care conduc la utilizarea abuzivă a mărcii de încredere a UE de către prestatori de servicii de încredere necalificate. Marca de încredere a UE nu ar trebui să fie utilizată în condiții care, în mod direct sau indirect, dau impresia că orice servicii de încredere necalificate oferite de astfel de prestatori ar fi calificate.

(46) Prezentul regulament nu ar trebui să reglementeze aspectele privind încheierea și valabilitatea contractelor sau a altor obligații juridice, în cazul în care există cerințe cu privire la formă prevăzute de dreptul Uniunii sau dreptul intern. Mai mult, prezentul regulament nu ar trebui să afecteze cerințele naționale cu privire la formă aferente registrelor publice, în special registrelor comerțului și cadastrelor.

---

[12] Directiva (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor (JO L 151, 7.6.2019, p. 70).

(47) Prestarea și utilizarea serviciilor de încredere și beneficiile aduse în ceea ce privește confortul și securitatea juridică în contextul tranzacțiilor transfrontaliere, în special atunci când sunt utilizate servicii de încredere calificate, capătă o importanță sporită pentru comerțul și cooperarea la nivel internațional. Partenerii internaționali ai Uniunii instituie cadre de încredere inspirate din Regulamentul (UE) nr. 910/2014. Pentru a facilita recunoașterea serviciilor de încredere calificate și a prestatorilor acestora, Comisia poate adopta acte de punere în aplicare pentru a stabili condițiile în care cadrele de încredere ale țărilor terțe ar putea fi considerate echivalente cu cadrul de încredere pentru serviciile de încredere calificate și prestatorii de servicii de încredere calificați care fac obiectul prezentului regulament. O astfel de abordare ar trebui să completeze posibilitatea de recunoaștere reciprocă a serviciilor de încredere și a prestatorilor acestora stabiliți în Uniune și în țări terțe în conformitate cu articolul 218 din Tratatul privind funcționarea Uniunii Europene (TFUE). Atunci când sunt stabilite condițiile în care cadrele de încredere ale țărilor terțe ar putea fi considerate echivalente cu cadrul de încredere pentru serviciile de încredere calificate și prestatorii de servicii de încredere calificați în temeiul Regulamentului (UE) nr. 910/2014, ar trebui să se asigure respectarea dispozițiilor relevante din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[13] și din Regulamentul (UE) 2016/679, precum și utilizarea listelor sigure ca elemente esențiale pentru consolidarea încrederii.

[13] 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).

(48) Prezentul regulament ar trebui să încurajeze alegerea și posibilitatea de a trece de la un portofel european pentru identitatea digitală la altul în cazul în care un stat membru a aprobat mai multe soluții pentru portofele europene pentru identitatea digitală pe teritoriul său. Pentru a evita efectele de blocare în astfel de situații, atunci când acest lucru este fezabil din punct de vedere tehnic, furnizorii de portofele europene pentru identitatea digitală ar trebui să asigure, la cererea utilizatorilor portofelului european pentru identitatea digitală, portabilitatea efectivă a datelor și nu ar trebui să li se permită acestor furnizori să utilizeze bariere contractuale, economice sau tehnice pentru a împiedica sau a descuraja trecerea efectivă de la un portofel european pentru identitatea digitală la altul.

(49) Pentru a asigura buna funcționare a portofelelor europene pentru identitatea digitală, furnizorii de portofele europene pentru identitatea digitală au nevoie de interoperabilitate efectivă și de condiții echitabile, rezonabile și nediscriminatorii pentru ca portofelele europene pentru identitatea digitală să acceseze componente de hardware și de software specifice ale dispozitivelor mobile. Componentele respective ar putea include în special antene de comunicare în câmp apropiat și elemente de securitate, inclusiv carduri cu circuit integrat universal, elemente de securitate încorporate, carduri microSD și Bluetooth cu consum redus de energie. Accesul la componentele respective ar putea fi sub controlul operatorilor de rețele mobile și al producătorilor de echipamente. Prin urmare, în cazul în care este necesar pentru a presta serviciile specifice portofelelor europene pentru identitatea digitală, producătorii de echipamente originale de dispozitive mobile sau furnizorii de servicii de comunicații electronice nu ar trebui să refuze accesul la astfel de componente. În plus, întreprinderilor desemnate drept controlori de acces pentru serviciile de platformă esențiale, astfel cum sunt indicate de Comisie în temeiul Regulamentului (UE) 2022/1925 al Parlamentului European și al Consiliului[14], ar trebui să li se aplice în continuare dispozițiile specifice ale regulamentului menționat, pe baza articolului 6 alineatul (7) din regulamentul respectiv.

---

[14] Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului din 14 septembrie 2022 privind piețe contestabile și echitabile în sectorul digital și de modificare a Directivelor (UE) 2019/1937 și (UE) 2020/1828 (Regulamentul privind piețele digitale) (JO L 265, 12.10.2022, p. 1).

(50) Pentru a raționaliza obligațiile în materie de securitate cibernetică impuse prestatorilor de servicii de încredere, precum și pentru a permite acestor prestatori și autorităților lor competente să beneficieze de cadrul juridic instituit prin Directiva (UE) 2022/2555, se impune serviciilor de încredere să ia măsuri tehnice și organizatorice adecvate în temeiul directivei menționate, cum ar fi măsuri ce vizează defecțiuni ale sistemelor, erori umane, acțiuni răuvoitoare sau fenomene naturale, pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care prestatorii respectivi le utilizează pentru a furniza servicii, precum și pentru a notifica incidente și amenințări cibernetice semnificative în conformitate cu directiva respectivă. În ceea ce privește raportarea incidentelor, prestatorii de servicii de încredere ar trebui să notifice orice incident care are un impact semnificativ asupra prestării serviciilor lor, inclusiv cele cauzate de furtul sau pierderea de dispozitive, de deteriorarea cablurilor de rețea sau de incidentele care survin în contextul identificării persoanelor. Cerințele de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare în temeiul Directivei (UE) 2022/2555 ar trebui să fie considerate complementare cerințelor impuse prestatorilor de servicii de încredere în temeiul prezentului regulament. După caz, autoritățile competente desemnate în temeiul Directivei (UE) 2022/2555 ar trebui să aplice în continuare practicile sau orientările naționale existente în legătură cu punerea în aplicare a cerințelor în materie de securitate și raportare și cu supravegherea conformității cu aceste cerințe în temeiul Regulamentului (UE) nr. 910/2014. Prezentul regulament nu aduce atingere obligației de notificare a încălcărilor securității datelor cu caracter personal în temeiul Regulamentului (UE) 2016/679.

(51) Ar trebui să se acorde o atenție deosebită asigurării unei cooperări eficace între organismele de supraveghere desemnate în temeiul articolului 46b din Regulamentul (UE) nr. 910/2014 și autoritățile competente desemnate sau înființate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555. În cazul în care un astfel de organism de supraveghere este altul decât o astfel de autoritate competentă, organismul de supraveghere și autoritatea competentă ar trebui să coopereze îndeaproape, în timp util, prin efectuarea unui schimb de informații relevante, pentru a asigura supravegherea eficace și respectarea de către prestatorii de servicii de încredere a cerințelor prevăzute în Regulamentul (UE) nr. 910/2014 și în Directiva (UE) 2022/2555. În special, organismele de supraveghere desemnate în temeiul Regulamentului (UE) nr. 910/2014 ar trebui să aibă dreptul de a solicita autorităților competente desemnate sau înființate în temeiul Directivei (UE) 2022/2555 să furnizeze informațiile relevante necesare pentru a acorda statutul de calificat și pentru a desfășura acțiuni de supraveghere în scopul de a verifica respectarea de către prestatorii de servicii de încredere a cerințelor relevante în temeiul Directivei (UE) 2022/2555 sau de a le solicita să remedieze situațiile de nerespectare.

(52) Este esențial să se prevadă un cadru juridic pentru a facilita recunoașterea transfrontalieră între sistemele juridice naționale existente în ceea ce privește serviciile de distribuție electronică înregistrată. Acest cadru ar putea genera, de asemenea, noi oportunități de piață pentru ca prestatorii de servicii de încredere ai Uniunii să ofere noi servicii de distribuție electronică înregistrată în întreaga Uniune. Pentru a se asigura că datele care utilizează un serviciu de distribuție electronică înregistrată calificat sunt furnizate destinatarului corect, serviciile de distribuție electronică înregistrată calificate ar trebui să asigure cu deplină certitudine identificarea destinatarului, în timp ce un nivel ridicat de încredere ar fi suficient în ceea ce privește identificarea expeditorului. Prestatorii de servicii de distribuție electronică înregistrată calificate ar trebui să fie încurajați de statele membre să facă în așa fel încât serviciile lor să fie interoperabile cu serviciile de distribuție electronică înregistrată calificate furnizate de alți prestatori de servicii de încredere calificați, pentru a transfera cu ușurință datele înregistrate în format electronic între doi sau mai mulți prestatori de servicii de încredere calificați și pentru a promova practici echitabile pe piața internă.

(53) În majoritatea cazurilor, cetățenii Uniunii și rezidenții din Uniune nu pot face, la nivel transfrontalier, schimb digital de informații referitoare la identitatea lor, cum ar fi adresa lor, vârstă, calificări profesionale, permis de conducere și alte date privind plăți și permise, în condiții de siguranță și cu un nivel ridicat de protecție a datelor.

(54) Ar trebui să fie posibil să se elibereze și gestioneze atribute electronice de încredere și să se contribuie la reducerea sarcinii administrative, oferindu-se cetățenilor Uniunii și rezidenților din Uniune posibilitatea de a le utiliza în tranzacțiile lor private și publice. Cetățenii Uniunii și rezidenții din Uniune ar trebui să fie în măsură, de exemplu, să demonstreze că sunt posesori ai unui permis de conducere valabil eliberat de o autoritate dintr-un stat membru, iar autoritățile relevante din alte state membre ar trebui să poată verifica permisul și să se poată baza pe acesta; cetățenii Uniunii și rezidenții din Uniune ar trebui totodată să se poată baza pe credențialele lor în materie de securitate socială sau pe viitoare documente de călătorie digitale în context transfrontalier.

(55) Orice prestator de servicii care emite atestate electronice ale atributelor, cum ar fi diplome, licențe, certificate de naștere sau împuterniciri și mandate de a reprezenta persoane fizice sau juridice sau de a acționa în numele acestora, ar trebui să fie considerată prestator de servicii de încredere de atestare electronică a atributelor. Unui atestat electronic al atributelor nu ar trebui să i se refuze efectul juridic din motiv că acesta este în format electronic sau că nu îndeplinește cerințele pentru atestatul electronic calificat al atributelor. Ar trebui să fie stabilite cerințe generale pentru a garanta că un atestat electronic calificat al atributelor are efect juridic echivalent cu cel al atestatelor emise în mod legal în format tipărit. Cu toate acestea, cerințele respective ar trebui să se aplice fără a aduce atingere dreptului Uniunii sau dreptului intern care stabilește cerințe sectoriale suplimentare în ceea ce privește forma cu efecte juridice subiacente și, în special, recunoașterea transfrontalieră a atestatului electronic calificat al atributelor, după caz.

(56) Disponibilitatea și utilizarea pe scară largă a portofelelor europene pentru identitatea digitală ar trebui să sporească gradul de acceptare și încrederea în acestea atât de către persoanele fizice, cât și de către prestatorii privați de servicii. Prin urmare, beneficiarii privați care prestează servicii de exemplu în domeniile transporturilor, energiei, serviciilor bancare și financiare, securității sociale, sănătății, apei potabile, serviciilor poștale, infrastructurii digitale, telecomunicațiilor sau educației ar trebui să accepte utilizarea portofelelor europene pentru identitatea digitală pentru prestarea serviciilor atunci când autentificarea strictă a utilizatorilor pentru identificarea online este obligatorie în temeiul dreptului Uniunii sau al dreptului intern ori al unei obligații contractuale. Orice solicitare din partea beneficiarului de informații de la utilizatorul unui portofel european pentru identificarea digitală ar trebui să fie necesară și proporțională cu utilizarea preconizată într-un anumit caz, ar trebui să respecte principiul reducerii la minimum a datelor și ar trebui să asigure transparența în ceea ce privește datele care sunt partajate și scopurile în care sunt partajate. Pentru a facilita utilizarea și acceptarea portofelelor europene pentru identitatea digitală, la implementarea lor ar trebui să se țină seama de standardele și specificațiile din industrie acceptate pe scară largă.

(57) În cazul în care platformele online foarte mari în sensul articolului 33 alineatul (1) din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului[15], impun utilizatorilor să fie autentificați pentru a accesa servicii online, aceste platforme ar trebui să aibă obligația să accepte utilizarea portofelelor europene pentru identitatea digitală la cererea voluntară a utilizatorului. Utilizatorii nu ar trebui să fie obligați să utilizeze un portofel european pentru identitatea digitală pentru a accesa servicii private, iar accesul lor la servicii nu ar trebui să fie restricționat sau împiedicat pe motiv că nu utilizează un portofel european pentru identitatea digitală. Cu toate acestea, dacă utilizatorii doresc să utilizeze portofele europene pentru identitatea digitală, platformele online foarte mari ar trebui să le accepte în acest scop, respectând în același timp principiul reducerii la minimum a datelor și dreptul utilizatorilor de a utiliza pseudonime alese în mod liber. Având în vedere importanța platformelor online foarte mari, datorită amplorii lor, în special în ceea ce privește numărul de destinatari ai serviciului și tranzacțiile economice, obligația de a accepta portofele europene pentru identitatea digitală este necesară pentru a spori protecția utilizatorilor împotriva fraudei și pentru a asigura un nivel ridicat de protecție a datelor.

(58) Ar trebui să fie elaborate coduri de conduită la nivelul Uniunii pentru a contribui la disponibilitatea și utilizarea pe scară largă a mijloacelor de identificare electronică, inclusiv a portofelelor europene pentru identitatea digitală în cadrul domeniului de aplicare al prezentului regulament. Codurile de conduită ar trebui să faciliteze acceptarea pe scară largă a mijloacelor de identificare electronică, inclusiv a portofelelor europene pentru identitatea digitală, de către prestatorii de servicii care nu se califică drept platforme foarte mari și care se bazează pe servicii de identificare electronică furnizate de terți pentru autentificarea utilizatorilor.

---

[15] 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).

(59) Divulgarea selectivă este un concept care permite proprietarului datelor să divulge numai anumite părți ale unui set de date mai mare, astfel încât entitatea destinatară să obțină numai acele informații care sunt necesare pentru furnizarea unui serviciu solicitat de utilizatorul în cauză. Portofelul european pentru identitatea digitală ar trebui să permită din punct de vedere tehnic divulgarea selectivă a atributelor către beneficiari. Ar trebui să fie posibil din punct de vedere tehnic pentru utilizator să divulge selectiv atribute, inclusiv din mai multe atestate electronice distincte, să le combine și să le prezinte fără întreruperi beneficiarilor. Această caracteristică ar trebui să devină un element de proiectare de bază al portofelelor europene pentru identitatea digitală, consolidând astfel confortul și protecția datelor cu caracter personal, inclusiv reducerea la minimum a datelor.

(60) Cu excepția cazului în care norme specifice de drept al Uniunii sau de drept intern impun utilizatorilor să se identifice, accesul la servicii prin utilizarea unui pseudonim nu ar trebui să fie interzis.

(61) Atributele furnizate de prestatorii de servicii de încredere calificați în cadrul atestatului calificat al atributelor ar trebui să fie verificate prin compararea lor cu surse autentice, fie direct de către prestatorul de servicii de încredere calificat, fie prin intermediari desemnați, recunoscuți la nivel național în conformitate cu dreptul Uniunii sau cu dreptul intern, în scopul schimbului securizat de atribute atestate între prestatorii de servicii de identificare sau de atestare a atributelor și beneficiarii acestor servicii. Statele membre ar trebui să instituie mecanisme adecvate la nivel național pentru a se asigura că prestatorii de servicii de încredere calificați care emit atestate electronice calificate ale atributelor sunt în măsură, pe baza consimțământului persoanei căreia i se emite atestatul, să verifice autenticitatea atributelor bazându-se pe surse autentice. Ar trebui să fie posibil ca mecanisme adecvate să includă recurgerea la intermediari specifici sau la soluții tehnice în conformitate cu dreptul intern care permite accesul la surse autentice. Asigurarea disponibilității unui mecanism care permite verificarea atributelor prin compararea lor cu surse autentice este menit să faciliteze respectarea de către prestatorii de servicii de încredere calificați care emit atestate electronice calificate ale atributelor a obligațiilor care le revin în temeiul Regulamentului (UE) nr. 910/2014. O nouă anexă la regulamentul respectiv ar trebui să conțină o listă a categoriilor de atribute în privința cărora statele membre trebuie să se asigure că se iau măsuri pentru a permite prestatorilor calificați care emit atestate electronice ale atributelor să verifice prin mijloace electronice, la cererea utilizatorului, autenticitatea acestora prin comparare cu sursa autentică relevantă.

(62) Identificarea electronică securizată și furnizarea de atestate ale atributelor ar trebui să ofere flexibilitate și soluții suplimentare pentru sectorul serviciilor financiare în scopul de a permite identificarea clienților și schimbul de atribute specifice necesare pentru a respecta, de exemplu, cerințele de precauție privind clientela în temeiul unui viitor regulament privind înființarea Autorității pentru Combaterea Spălării Banilor și cerințele privind caracterul adecvat care decurg din legislația privind protecția investitorilor, sau în scopul de a sprijini îndeplinirea unor cerințe de autentificare strictă a clienților în cazul identificării online în scopul intrării în cont și al inițierii tranzacțiilor în domeniul serviciilor de plată.

(63) Efectul juridic al unei semnături electronice nu se contestă pe motivul că aceasta este în format electronic sau că nu îndeplinește cerințele pentru semnătura electronică calificată. Prezentul regulament prevede ca o semnătură electronică calificată să fie considerată echivalentă cu o semnătură olografă. Cu toate acestea, efectul juridic al semnăturilor electronice se stabilește prin dreptul intern, cu excepția cerințelor prevăzute de prezentul regulament potrivit cărora efectul juridic al unei semnături electronice calificate se consideră ca fiind echivalent cu cel al unei semnături olografe. Atunci când stabilesc efectele juridice ale semnăturilor electronice, statele membre ar trebui să țină seama de principiul proporționalității între valoarea juridică a unui document care urmează să fie semnat și nivelul de securitate și costurile pe care le impune o semnătură electronică. Pentru a spori accesibilitatea și utilizarea semnăturilor electronice, statele membre sunt încurajate să ia în considerare utilizarea semnăturilor electronice avansate în tranzacțiile zilnice pentru care oferă un nivel suficient de securitate și încredere.

(64) Pentru a asigura consecvența practicilor de certificare în întreaga Uniune, Comisia ar trebui să emită orientări privind certificarea și recertificarea dispozitivelor calificate de creare a semnăturilor electronice și a dispozitivelor calificate de creare a sigiliilor electronice, inclusiv privind valabilitatea și limitările în timp ale acestora. Prezentul regulament nu împiedică organismele publice sau private să recertifice temporar astfel de dispozitive pentru o perioadă scurtă de valabilitate a certificării, pe baza rezultatelor celei mai recente proceduri de certificare, atunci când o astfel de recertificare nu poate avea loc în termenul stabilit prin lege pentru orice alt motiv decât o încălcare a securității sau un incident de securitate și fără a aduce atingere obligației de a efectua o evaluare a vulnerabilității și fără a aduce atingere practicii de certificare aplicabile.

(65) Emiterea certificatelor pentru autentificarea site-urilor internet este destinată să ofere utilizatorilor o garanție cu un nivel ridicat de încredere în ceea ce privește identitatea entității care se află în spatele site-ului internet, indiferent ce platformă este folosită pentru afișarea identității respective. Certificatele respective ar trebui să contribuie la construirea încrederii în desfășurarea de activități comerciale online, întrucât utilizatorii ar avea încredere într-un site internet care a fost autentificat. Utilizarea unor astfel de certificate de către site-uri internet ar trebui să fie voluntară. Pentru ca autentificarea unui site internet să devină un mijloc prin care se sporește încrederea, se oferă utilizatorului o experiență mai bună și se stimulează creșterea economică pe piața internă, prezentul regulament prevede un cadru de încredere care include obligații minime în materie de securitate și răspundere pentru furnizorii certificatelor calificate pentru autentificarea site-urilor internet și cerințe pentru emiterea certificatelor respective. Listele sigure naționale ar trebui să confirme statutul de calificat al serviciilor de autentificare a unui site internet și al prestatorilor lor de servicii de încredere, inclusiv conformitatea deplină a acestora cu cerințele prezentului regulament în ceea ce privește emiterea certificatelor calificate pentru autentificarea unui site internet. Recunoașterea certificatelor calificate pentru autentificarea unui site internet înseamnă că furnizorii de browsere web nu ar trebui să refuze autenticitatea certificatelor calificate pentru autentificarea unui site internet numai cu scopul de a atesta legătura dintre numele de domeniu al site-ului internet și persoana fizică sau juridică căreia i se emite certificatul sau de a confirma identitatea persoanei respective. Furnizorii de browsere web ar trebui să afișeze utilizatorului final datele de identitate certificate și celelalte atribute atestate într-un mod ușor de utilizat în mediul browserului, utilizând mijloacele tehnice alese de aceștia. În acest scop, furnizorii de browsere web ar trebui să asigure asistență și interoperabilitate pentru certificatele calificate pentru autentificarea unui site internet emise cu deplina respectare a prezentului regulament.

Obligația de recunoaștere, interoperabilitate și asistență pentru certificatele calificate pentru autentificarea unui site internet nu afectează libertatea furnizorilor de browsere web de a asigura securitatea web, autentificarea domeniilor și criptarea traficului web în maniera și prin intermediul tehnologiei pe care o consideră cea mai adecvată. Pentru a contribui la securitatea online a utilizatorilor finali, furnizorii de browsere web ar trebui, în circumstanțe excepționale, să poată lua măsuri de precauție care sunt atât necesare, cât și proporționale ca răspuns la preocupări motivate referitoare la încălcări ale securității sau la pierderea integrității unui certificat identificat sau a unui set de certificate identificate. În cazul în care iau astfel de măsuri de precauție, furnizorii de browsere web ar trebui să notifice fără întârzieri nejustificate Comisiei, organismului național de supraveghere, entității căreia i-a fost emis certificatul și prestatorului de servicii de încredere calificat care a emis certificatul sau setul de certificate cu privire la orice preocupare referitoare la o astfel de încălcare a securității sau de pierdere a integrității, precum și cu privire la măsurile luate cu privire la certificat sau la setul de certificate. Măsurile respective nu ar trebui să aducă atingere obligației furnizorilor de browsere web de a recunoaște certificatele calificate pentru autentificarea unui site internet în conformitate cu listele sigure naționale. Pentru a proteja suplimentar cetățenii Uniunii și rezidenții din Uniune și pentru a promova utilizarea certificatelor calificate pentru autentificarea unui site internet, autoritățile publice din statele membre ar trebui să ia în considerare includerea certificatelor calificate pentru autentificarea unui site internet în site-urile lor internet. Măsurile prevăzute de prezentul regulament care vizează asigurarea unei coerențe sporite între abordările și practicile divergente ale statelor membre în ceea ce privește procedurile de supraveghere sunt menite să contribuie la îmbunătățirea încrederii în securitatea, calitatea și disponibilitatea certificatelor calificate pentru autentificarea unui site internet.

(66) Numeroase state membre au introdus cerințe naționale pentru serviciile care oferă arhivare electronică sigură și fiabilă, pentru a permite conservarea pe termen lung a datelor electronice și a documentelor electronice și a serviciilor de încredere conexe. Pentru a asigura securitatea juridică, încrederea și armonizarea între statele membre, ar trebui să fie instituit un cadru juridic pentru serviciile calificate de arhivare electronică, inspirat de cadrul aferent celorlalte servicii de încredere prevăzute în prezentul regulament. Cadrul juridic pentru serviciile calificate de arhivare electronică ar trebui să ofere prestatorilor de servicii de încredere și utilizatorilor un set eficient de instrumente care să includă cerințe funcționale pentru serviciul de arhivare electronică, precum și efecte juridice clare atunci când se utilizează un serviciu calificat de arhivare electronică. Dispozițiile respective ar trebui să se aplice datelor electronice și documentelor constituite în format electronic, precum și documentelor pe suport de hârtie care au fost scanate și digitalizate. Atunci când este necesar, dispozițiile respective ar trebui să permită ca datele electronice și documentele electronice păstrate să fie transferate pe diferite suporturi sau în diferite formate în scopul prelungirii durabilității și lizibilității acestora dincolo de perioada de valabilitate tehnologică, împiedicând în același timp, în cea mai mare măsură posibilă, pierderile și modificările. Atunci când datele electronice și documentele electronice transmise serviciului de arhivare electronică conțin una sau mai multe semnături electronice calificate sau sigilii electronice calificate, serviciul ar trebui să utilizeze proceduri și tehnologii capabile să le extindă fiabilitatea pe toată perioada de păstrare a acestor date, eventual bazându-se pe utilizarea altor servicii de încredere calificate instituite prin prezentul regulament. Pentru a crea dovezi ale conservării în cazul în care se utilizează semnături electronice, sigilii electronice sau mărci temporale electronice, ar trebui să fie utilizate servicii de încredere calificate. În măsura în care serviciile de arhivare electronică nu sunt armonizate prin prezentul regulament, statele membre ar trebui să poată menține sau introduce dispoziții de drept intern, conforme cu dreptul Uniunii, referitoare la aceste servicii, cum ar fi dispoziții specifice pentru serviciile integrate într-o organizație și utilizate exclusiv în scopul arhivării interne în cadrul organizației respective. Prezentul regulament nu ar trebui să facă distincție între datele electronice și documentele constituite în format electronic și documentele fizice care au fost digitalizate.

(67) Activitățile arhivelor naționale și ale instituțiilor dedicate conservării trecutului, în calitatea lor de organizații dedicate conservării patrimoniului documentar în interes public, sunt, de obicei, reglementate în dreptul intern și nu furnizează neapărat servicii de încredere în sensul prezentului regulament. Atât timp cât aceste instituții nu furnizează astfel de servicii de încredere, prezentul regulament nu aduce atingere funcționării lor.

(68) Registrele electronice reprezintă o secvență de înregistrări electronice de date care ar trebui să asigure integritatea acestora și acuratețea ordonării lor cronologice. Registrele electronice ar trebui să stabilească o secvență cronologică de înregistrări de date. Împreună cu alte tehnologii, acestea ar trebui să contribuie la găsirea de soluții pentru servicii publice mai eficiente și transformatoare, cum ar fi votul electronic, cooperarea transfrontalieră a autorităților vamale, cooperarea transfrontalieră a institutelor academice și înregistrarea dreptului de proprietate asupra bunurilor imobiliare în registre funciare descentralizate. Registrele electronice calificate ar trebui să stabilească o prezumție legală pentru ordonarea cronologică secvențială unică și exactă și pentru integritatea înregistrărilor de date din registre. Datorită specificului acestora, cum ar fi ordonarea cronologică secvențială a înregistrărilor de date, registrele electronice ar trebui să se distingă de alte servicii de încredere, cum ar fi mărcile temporale electronice și serviciile de distribuție electronică înregistrată. Pentru a asigura securitatea juridică și a promova inovarea, ar trebui să se instituie un cadru juridic la nivelul Uniunii care să prevadă recunoașterea transfrontalieră a serviciilor de încredere pentru înregistrarea datelor în registrele electronice. Acest lucru ar trebui să împiedice în mod suficient copierea și vânzarea aceluiași activ digital de mai multe ori unor părți diferite. Procesul de creare și actualizare a unui registru electronic depinde de tipul de registru utilizat, și anume dacă este centralizat sau distribuit. Prezentul regulament ar trebui să asigure neutralitatea tehnologică, și anume să nu favorizeze și nici să nu discrimineze nicio tehnologie utilizată pentru punerea în aplicare a noului serviciu de încredere pentru registrele electronice. În plus, Comisia ar trebui să țină seama de indicatorii de durabilitate cu privire la orice efect negativ asupra climei sau la alte efecte negative legate de mediu, utilizând metodologii adecvate, atunci când pregătește actele de punere în aplicare care precizează cerințele pentru registrele electronice calificate.

(69) Rolul prestatorilor de servicii de încredere pentru registrele electronice ar trebui să fie cel de a verifica înregistrarea secvențială a datelor în registru. Prezentul regulament nu aduce atingere niciunei obligații legale a utilizatorilor registrelor electronice în temeiul dreptului Uniunii sau al dreptului intern. De exemplu, cazurile de utilizare care implică prelucrarea datelor cu caracter personal ar trebui să respecte Regulamentul (UE) 2016/679, iar cazurile de utilizare care se referă la servicii financiare ar trebui să respecte legislația relevantă a Uniunii privind serviciile financiare.

(70) Pentru a evita fragmentarea pieței interne și obstacolele pe această piață, cauzate de standarde divergente și de restricții tehnice, precum și pentru a asigura un proces coordonat în scopul de a evita să fie afectată punerea în aplicare a cadrului european pentru identitatea digitală, este necesar să existe un proces de cooperare strânsă și structurată între Comisie, statele membre, societatea civilă, mediul academic și sectorul privat. Pentru a atinge acest obiectiv, statele membre și Comisia ar trebui să coopereze în cadrul stabilit prin Recomandarea (UE) 2021/946 a Comisiei[16] pentru a identifica un set comun de instrumente la nivelul Uniunii vizând cadrul european pentru identitatea digitală. În acest context, statele membre ar trebui să ajungă la un acord cu privire la o arhitectură tehnică cuprinzătoare și un cadru de referință, un set de standarde comune și de referințe tehnice comune, inclusiv standarde existente recunoscute, precum și un set de orientări și descrieri de bune practici care să privească cel puțin toate funcționalitățile și interoperabilitatea portofelelor europene pentru identitatea digitală, inclusiv semnăturile electronice, și ale prestatorilor de servicii de încredere calificați pentru atestarea electronică a atributelor, astfel cum se prevede în prezentul regulament. În acest context, statele membre ar trebui, de asemenea, să ajungă la un acord cu privire la elementele comune ale unui model de afaceri și ale structurii taxelor aferente portofelelor europene pentru identitatea digitală, pentru a facilita adoptarea acestora, în special de către IMM-uri, în context transfrontalier. Conținutul setului de instrumente ar trebui să evolueze în paralel cu rezultatul discuțiilor și al procesului de adoptare a cadrului european pentru identitatea digitală și să reflecte rezultatele acestora.

---

[16] 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).

(71) Prezentul regulament prevede un nivel armonizat de calitate, fiabilitate și securitate a serviciilor de încredere calificate, indiferent de locul în care se desfășoară operațiunile. Astfel, un prestator de servicii de încredere calificat ar trebui să fie autorizat să își externalizeze operațiunile legate de prestarea unui serviciu de încredere calificat într-o țară terță, cu condiția ca țara terță respectivă să prevadă garanții adecvate care să asigure că activitățile de supraveghere și auditurile pot fi puse în aplicare ca și cum ar fi efectuate în Uniune. Atunci când respectarea prezentului regulament nu poate fi asigurată pe deplin, organismele de supraveghere ar trebui să poată adopta măsuri proporționate și justificate, inclusiv retragerea statutului de calificat al serviciului de încredere prestat.

(72) Pentru a asigura securitatea juridică cu privire la valabilitatea semnăturilor electronice avansate bazate pe certificate calificate, este esențial să fie precizată în detaliu evaluarea efectuată de beneficiarul care efectuează validarea respectivei semnături electronice avansate bazate pe certificate calificate.

(73) Prestatorii de servicii de încredere ar trebui să utilizeze metode criptografice care să reflecte bunele practici actuale și să le implementeze într-un mod demn de încredere pentru a asigura securitatea și fiabilitatea serviciilor lor de încredere.

(74) Prezentul regulament prevede obligația prestatorilor de servicii de încredere calificați de a verifica identitatea unei persoane fizice sau juridice căreia i se emite certificatul calificat sau atestatul electronic calificat al atributelor pe baza mai multor metode armonizate în întreaga Uniune. Pentru a se asigura că certificatele calificate și atestatele electronice calificate ale atributelor sunt emise persoanei căreia îi aparțin și că acestea atestă setul corect și unic de date care reprezintă identitatea persoanei respective, prestatorii de servicii de încredere calificați care emit certificate calificate sau atestate electronice calificate ale atributelor ar trebui, la momentul emiterii certificatelor și atestatelor respective, să asigure cu certitudine deplină identificarea persoanei respective. În plus, pe lângă verificarea obligatorie a identității persoanei, dacă este cazul pentru emiterea certificatelor calificate și atunci când emit un atestat electronic calificat al atributelor, prestatorii de servicii de încredere calificați ar trebui să asigure cu certitudine deplină corectitudinea și exactitatea atributelor atestate ale persoanei căreia i se emite certificatul calificat sau atestatul electronic calificat al atributelor. Aceste obligații privind rezultatul și certitudinea deplină în ceea ce privește verificarea datelor atestate ar trebui să fie susținute prin mijloace adecvate, inclusiv prin utilizarea unei metode specifice sau, dacă este necesar, a unei combinații de metode specifice prevăzute de prezentul regulament. Ar trebui să fie posibilă combinarea metodelor respective pentru a oferi o bază adecvată pentru verificarea identității persoanei căreia i se emite certificatul calificat sau un atestat electronic calificat al atributelor. O astfel de combinație ar trebui să poată include recurgerea la mijloace de identificare electronică care îndeplinesc cerințele privind nivelul de asigurare substanțial în combinație cu alte mijloace de verificare a identității care ar permite îndeplinirea cerințelor armonizate prevăzute în prezentul regulament în ceea ce privește nivelul de asigurare ridicat ca parte a procedurilor armonizate suplimentare la distanță, asigurând identificarea cu un nivel ridicat de încredere. Aceste metode ar trebui să includă posibilitatea ca prestatorul de servicii de încredere calificat care emite un atestat electronic calificat al atributelor să verifice atributele care urmează să fie atestate prin mijloace electronice la cererea utilizatorului, în conformitate cu dreptul Uniunii sau cu dreptul intern, inclusiv din surse autentice.

(75) Pentru a menține prezentul regulament aliniat la evoluțiile mondiale și pentru a respecta bunele practici de pe piața internă, actele delegate și actele de punere în aplicare adoptate de Comisie ar trebui să fie revizuite și, dacă este necesar, actualizate periodic. Evaluarea necesității acestor actualizări ar trebui să țină seama de noile tehnologii, practici, standarde sau specificații tehnice.

(76) Întrucât obiectivele prezentului regulament, și anume dezvoltarea cadrului european pentru identitatea digitală și a unui cadru privind serviciile de încredere la nivelul Uniunii, nu pot fi realizate în mod satisfăcător de către statele membre, dar, având în vedere amploarea și efectele lor, acestea 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, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor respective.

(77) Autoritatea Europeană pentru Protecția Datelor a fost consultată în temeiul articolului 42 alineatul (1) din Regulamentul (UE) 2018/1725.

(78) Prin urmare, Regulamentul (UE) nr. 910/2014 trebuie să fie modificat în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Modificarea Regulamentului (UE) nr. 910/2014

Regulamentul (UE) nr. 910/2014 se modifică după cum urmează:

1. Articolul 1 se înlocuiește cu următorul text:

„*Articolul 1*

Obiect

Prezentul regulament urmărește să asigure buna funcționare a pieței interne și să asigure un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere utilizate în întreaga Uniune, pentru a permite și a facilita exercitarea de către persoanele fizice și juridice a dreptului de a participa la societatea digitală în condiții de siguranță și de a accesa servicii publice și private online în întreaga Uniune. În acest scop, prezentul regulament:

(a) stabilește condițiile în care statele membre recunosc mijloacele de identificare electronică a persoanelor fizice și juridice care intră sub incidența unui sistem notificat de identificare electronică al unui alt stat membru și furnizează și recunosc portofelele europene pentru identitatea digitală;

(b) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice;

(c) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate, serviciile de certificare pentru autentificarea unui site internet, arhivarea electronică, atestarea electronică a atributelor, dispozitivele de creare a semnăturilor, dispozitivele de creare a sigiliilor electronice, precum și pentru registrele electronice.”

2. Articolul 2 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Prezentul regulament se aplică sistemelor de identificare electronică care sunt notificate de către un stat membru, portofelelor europene pentru identitatea digitală care sunt furnizate de un stat membru și prestatorilor de servicii de încredere cu sediul în Uniune.”;

(b) alineatul (3) se înlocuiește cu următorul text:

„(3) Prezentul regulament nu aduce atingere dreptului Uniunii sau dreptului intern privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma, ori cerințelor sectoriale privind forma.

(4) Prezentul regulament nu aduce atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului*.

---

* 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).”

3. Articolul 3 se modifică după cum urmează:

(a) punctele 1-5 se înlocuiesc cu următorul text:

„1. «identificare electronică» înseamnă procesul de utilizare a datelor de identificare personală în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică;

2. «mijloace de identificare electronică» înseamnă o unitate materială și/sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării pentru un serviciu online sau, după caz, pentru un serviciu offline;

3. «date de identificare personală» înseamnă un set de date care este emis în conformitate cu dreptul Uniunii sau cu dreptul intern și care permite stabilirea identității unei persoane fizice sau juridice ori a unei persoane fizice care reprezintă o altă persoană fizică sau o persoană juridică;

4. «sistem de identificare electronică» înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice ori pentru persoane fizice care reprezintă alte persoane fizice sau persoane juridice;

5. «autentificare» înseamnă un proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau confirmarea originii și integrității unor date în format electronic;”;

(b) se introduce următorul punct:

„5a. «utilizator» înseamnă o persoană fizică sau juridică ori o persoană fizică care reprezintă o altă persoană fizică sau o persoană juridică, care utilizează servicii de încredere sau mijloace de identificare electronică, puse la dispoziție în conformitate cu prezentul regulament;”;

(c) punctul 6 se înlocuiește cu următorul text:

„6. «beneficiar» înseamnă o persoană fizică sau juridică care beneficiază de identificarea electronică, de portofelele europene pentru identitatea digitală sau de alte mijloace de identificare electronică sau de un serviciu de încredere;”;

(d) punctul 16 se înlocuiește cu următorul text:

„16. «serviciu de încredere» înseamnă un serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în oricare din următoarele:

(a) emiterea certificatelor pentru semnături electronice, a certificatelor pentru sigilii electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere;

(b) validarea certificatelor pentru semnăturile electronice, a certificatelor pentru sigiliile electronice, a certificatelor pentru autentificarea unui site internet sau a certificatelor pentru prestarea altor servicii de încredere;

(c) crearea semnăturilor electronice sau a sigiliilor electronice;

(d) validarea semnăturilor electronice sau a sigiliilor electronice;

(e) păstrarea semnăturilor electronice, a sigiliilor electronice, a certificatelor pentru semnăturile electronice sau a certificatelor pentru sigiliile electronice;

(f) gestionarea dispozitivelor pentru crearea semnăturilor electronice la distanță sau a dispozitivelor pentru crearea sigiliilor electronice la distanță;

(g) emiterea atestatelor electronice ale atributelor;

(h) validarea atestatelor electronice a atributelor;

(i) crearea mărcilor temporale electronice;

(j) validarea mărcilor temporale electronice;

(k) prestarea serviciilor de distribuție electronică înregistrate;

(l) validarea datelor transmise prin intermediul serviciilor de distribuție electronică înregistrate și a probelor aferente;

(m) arhivarea electronică a datelor electronice;

(n) înregistrarea într-un registru electronic a datelor electronice și a documentelor în format electronic;”;

(e) punctul 18 se înlocuiește cu următorul text:

„18. «organism de evaluare a conformității» înseamnă un organism de evaluare a conformității în sensul definiției de la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care este acreditat în conformitate cu regulamentul respectiv ca fiind competent să efectueze evaluarea conformității unui prestator de servicii de încredere calificat și a serviciilor de încredere calificate pe care acesta le prestează ori ca fiind competent să efectueze certificarea portofelelor europene pentru identitatea digitală sau a mijloacelor de identificare electronică;”;

(f) punctul 21 se înlocuiește cu următorul text:

„21. «produs» înseamnă hardware sau software ori componente relevante de hardware sau de software destinate să fie utilizate pentru prestarea de servicii de identificare electronică și de servicii de încredere;”;

(g) se introduc următoarele puncte:

„23a. «dispozitiv calificat de creare a semnăturii electronice la distanță» înseamnă un dispozitiv calificat de creare a semnăturii electronice care este gestionat de un prestator de servicii de încredere calificat în conformitate cu articolul 29a în numele unui semnatar;

23b. «dispozitiv calificat de creare a sigiliului electronic la distanță» înseamnă un dispozitiv calificat de creare a sigiliului electronic care este gestionat de un prestator de servicii de încredere calificat în conformitate cu articolul 39a în numele unui creator de sigilii;”;

(h) punctul 38 se înlocuiește cu următorul text:

„38. «certificat pentru autentificarea unui site internet» înseamnă un atestat electronic care face posibilă autentificarea unui site internet și face legătura între site-ul internet și persoana fizică sau juridică căreia i s-a emis certificatul;”;

(i) punctul 41 se înlocuiește cu următorul text:

„41. «validare» înseamnă procesul prin care se verifică și se confirmă validitatea datelor în format electronic în conformitate cu prezentul regulament;”;

(j) se adaugă următoarele puncte:

„42. «portofel european pentru identitatea digitală» înseamnă un mijloc de identificare electronică care permite utilizatorului să stocheze, să gestioneze și să valideze în condiții de siguranță datele de identificare personală și atestatele electronice ale atributelor cu scopul de a le furniza beneficiarilor și altor utilizatori ai portofelelor europene pentru identitatea digitală și să semneze prin intermediul semnăturilor electronice calificate sau să sigileze prin intermediul sigiliilor electronice calificate;

43. «atribut» înseamnă o caracteristică, o calitate, un drept sau o permisiune a unei persoane fizice sau juridice sau a unui obiect;

44. «atestat electronic al atributelor» înseamnă un atestat în format electronic care permite atributelor să fie autentificate;

45. «atestat electronic calificat al atributelor» înseamnă un atestat electronic al atributelor care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa V;

46. «atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele acestuia» înseamnă un atestat electronic al atributelor emis de un organism din sectorul public care este responsabil de o sursă autentică ori de un organism din sectorul public care este desemnat de statul membru să emită astfel de atestate ale atributelor în numele organismelor din sectorul public responsabile de sursele autentice în conformitate cu articolul 45f și cu anexa VII;

47. «sursă autentică» înseamnă un registru sau un sistem, aflat în responsabilitatea unui organism din sectorul public sau a unei entități private, care conține și pune la dispoziție atribute referitoare la o persoană fizică sau juridică ori la un obiect și care este considerat a fi o sursă primară a informațiilor respective sau care este recunoscut ca fiind autentic în conformitate cu dreptul Uniunii sau cu dreptul intern, inclusiv cu practica administrativă;

48. «arhivare electronică» înseamnă un serviciu care asigură primirea, stocarea, recuperarea și ștergerea datelor electronice și a documentelor electronice pentru a asigura durabilitatea și lizibilitatea acestora, precum și pentru a păstra integritatea, confidențialitatea și dovada originii acestora pe parcursul întregii perioade de păstrare;

49. «serviciu calificat de arhivare electronică» înseamnă un serviciu de arhivare electronică care este prestat de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la articolul 45j;

50. «marca de încredere a portofelului UE pentru identitatea digitală» înseamnă o indicație verificabilă, simplă și ușor de recunoscut, care se comunică în mod clar, a faptului că un portofel european pentru identitatea digitală a fost pus la dispoziție în conformitate cu prezentul regulament;

51. «autentificarea strictă a utilizatorilor» înseamnă o autentificare care se bazează pe utilizarea a cel puțin doi factori de autentificare din categoriile diferite ale cunoștințelor, ceva ce doar utilizatorul cunoaște, ale posesiei, ceva ce doar utilizatorul posedă sau ale inerenței, ceva ce reprezintă utilizatorul, care sunt independenți, în sensul că încălcarea securității unuia dintre factori nu compromite fiabilitatea celorlalți, și care este concepută în așa fel încât să protejeze confidențialitatea datelor de autentificare;

52. «registru electronic» înseamnă o secvență de înregistrări electronice de date, care asigură integritatea înregistrărilor respective și acuratețea ordinii cronologice a înregistrărilor respective;

53. «registru electronic calificat» înseamnă o un registru electronic care este pus la dispoziție de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la articolul 45l;

54. «date cu caracter personal» înseamnă orice informație în sensul definiției de la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

55. «corelarea identității» înseamnă un proces prin care datele de identificare personală sau mijloacele de identificare electronică sunt corelate sau asociate cu un cont existent care aparține aceleiași persoane;

56. «înregistrare de date» înseamnă date electronice înregistrate împreună cu metadatele aferente care susțin prelucrarea datelor;

57. «mod offline» înseamnă, în ceea ce privește utilizarea portofelelor europene pentru identitatea digitală, o interacțiune între un utilizator și o terță parte într-un loc fizic care utilizează tehnologii de proximitate imediată, fără ca portofelul european pentru identitatea digitală să fie necesar pentru accesarea unor sisteme la distanță prin intermediul rețelelor de comunicații electronice în scopul interacțiunii respective.”

4. Articolul 5 se înlocuiește cu următorul text:

„*Articolul 5*
Pseudonime în tranzacțiile electronice

Fără a aduce atingere normelor specifice din dreptul Uniunii sau din dreptul intern care impun utilizatorilor să se identifice sau efectelor juridice conferite pseudonimelor în temeiul dreptului intern, utilizarea pseudonimelor alese de utilizator nu este interzisă.”

5. În capitolul II, se introduce următoarea secțiune:

„SECȚIUNEA 1
PORTOFELUL EUROPEAN PENTRU IDENTITATEA DIGITALĂ

Articolul 5a
Portofelele europene pentru identitatea digitală

(1) În scopul garantării faptului că toate persoanele fizice și juridice din Uniune au un acces transfrontalier securizat, fiabil și neîntrerupt la servicii publice și private, păstrând totodată controlul deplin asupra datelor lor, fiecare stat membru furnizează cel puțin un portofel european pentru identitatea digitală în termen de 24 de luni de la data intrării în vigoare a actelor de punere în aplicare menționate la alineatul (23) de la prezentul articol și la articolul 5c alineatul (6).

(2) Portofelele europene pentru identitatea digitală sunt furnizate în unul sau mai multe dintre următoarele moduri:

(a) direct de către un stat membru;

(b) pe baza unui mandat din partea unui stat membru;

(c) în mod independent de un stat membru, dar fiind recunoscute de respectivul stat membru.

(3) Codul sursă al componentelor de software ale aplicației portofelelor europene pentru identitatea digitală face obiectul unei licențe cu sursă deschisă. Statele membre pot prevedea ca, din motive justificate în mod corespunzător, codul sursă al anumitor componente, altele decât cele instalate pe dispozitivele utilizatorilor, să nu fie divulgat.

(4) Portofelele europene pentru identitatea digitală permit utilizatorului, într-un mod transparent și ușor de utilizat și de urmărit de către acesta:

(a) să solicite, să obțină, să selecteze, să combine, să stocheze, să șteargă, să partajeze și să prezinte în condiții de siguranță, exclusiv sub controlul utilizatorului, datele de identificare personală și, după caz, în combinație cu atestate electronice ale atributelor, să se autentifice beneficiarilor online și, după caz, în mod offline, pentru a accesa servicii publice și private, asigurând, în același timp, că este posibilă divulgarea selectivă a datelor;

(b) să genereze pseudonime și să le stocheze local și în formă criptată în portofelul european pentru identitatea digitală;

(c) să autentifice în condiții de siguranță portofelul european pentru identitatea digitală al unei alte persoane și să primească și partajeze date de identificare personală și atestate electronice ale atributelor într-un mod securizat între cele două portofele europene pentru identitatea digitală;

(d) să acceseze o evidență a tuturor tranzacțiilor efectuate cu ajutorul portofelului european pentru identitatea digitală prin intermediul unui tablou de bord comun care să permită utilizatorului:

(i) să vizualizeze o listă actualizată a beneficiarilor cu care utilizatorul a stabilit o conexiune și, după caz, a tuturor datelor partajate;

(ii) să solicite cu ușurință unui beneficiar să șteargă datele cu caracter personal în temeiul articolului 17 din Regulamentul (UE) 2016/679;

(iii) să semnaleze cu ușurință un beneficiar autorității naționale competente pentru protecția datelor, atunci când se primește o cerere de date presupus ilegală sau suspectă;

(e) să semneze prin intermediul semnăturilor electronice calificate sau să sigileze prin intermediul sigiliilor electronice calificate;

(f) să descarce, în măsura în care acest lucru este fezabil din punct de vedere tehnic, datele, atestatul electronic al atributelor și configurațiile utilizatorului;

(g) să exercite dreptul utilizatorului la portabilitatea datelor.

(5) În special, portofelele europene pentru identitatea digitală:

(a) permit utilizarea unor protocoale și interfețe comune:

(i) pentru emiterea datelor de identificare personală, a atestatelor electronice calificate și necalificate ale atributelor sau a certificatelor calificate și necalificate către portofelul european pentru identitatea digitală;

(ii) pentru ca beneficiarii să solicite și să valideze date de identificare personală și atestate electronice ale atributelor;

(iii) pentru partajarea și prezentarea către beneficiari a datelor de identificare personală, a atestatului electronic al atributelor sau a datelor conexe divulgate selectiv online și, după caz, în mod offline;

(iv) pentru ca utilizatorul să permită interacțiunea cu portofelul european pentru identitatea digitală și să afișeze o marcă de încredere a portofelului UE pentru identitatea digitală;

(v) pentru a realiza integrarea în condiții de siguranță a utilizatorului prin utilizarea unui mijloc de identificare electronică în conformitate cu articolul 5a alineatul (24);

(vi) pentru interacțiunea între portofelele europene pentru identitatea digitală a două persoane în scopul de a primi, a valida și a partaja date de identificare personală și atestate electronice ale atributelor într-un mod securizat;

(vii) pentru autentificarea și identificarea beneficiarilor prin punerea în aplicare a mecanismelor de autentificare în conformitate cu articolul 5b;

(viii) pentru ca beneficiarii să verifice autenticitatea și valabilitatea portofelelor europene pentru identitatea digitală;

(ix) pentru a solicita unui beneficiar să șteargă datele cu caracter personal în temeiul articolului 17 din Regulamentul (UE) 2016/679;

(x) pentru a semnala un beneficiar autorității naționale pentru protecția datelor competente în cazul în care se primește o cerere de date presupus ilegală sau suspectă;

(xi) pentru crearea de semnături sau sigilii electronice calificate prin intermediul dispozitivelor de creare a semnăturilor electronice sau a sigiliilor electronice calificate;

(b) nu oferă prestatorilor de servicii de încredere care furnizează atestate electronice ale atributelor nicio informație cu privire la utilizarea respectivelor atestate electronice;

(c) asigură faptul că beneficiarii pot fi autentificați și identificați prin punerea în aplicare a unor mecanisme de autentificare în conformitate cu articolul 5b;

(d) îndeplinesc cerințele prevăzute la articolul 8 în ceea ce privește nivelul de asigurare ridicat, în special în ceea ce privește cerințele privind dovedirea și verificarea identității, precum și gestionarea și autentificarea mijloacelor de identificare electronică;

(e) în cazul atestatelor electronice ale atributelor cu politici de divulgare încorporate, pune în aplicare mecanismul adecvat pentru a informa utilizatorul că beneficiarul sau utilizatorul portofelului european pentru identitatea digitală care solicită atestatul electronic al atributelor în cauză are permisiunea de a accesa astfel de atestate;

(f) asigură faptul că datele de identificare personală, care sunt disponibile din sistemul de identificare electronică în cadrul căruia este furnizat portofelul european pentru identitatea digitală, reprezintă în mod unic persoana fizică, persoana juridică sau persoana fizică ce reprezintă persoana fizică sau juridică și sunt asociate cu respectivul portofel european pentru identitatea digitală;

(g) oferă tuturor persoanelor fizice posibilitatea de a semna prin intermediul semnăturilor electronice calificate în mod implicit și gratuit.

Prin excepție de la dispozițiile de la primul paragraf litera (g), statele membre pot să prevadă măsuri proporționale pentru a asigura faptul că utilizarea gratuită a semnăturilor electronice calificate de către persoanele fizice este limitată la scopuri neprofesionale.

(6) Statele Membre informează utilizatorii, fără întârziere, despre orice încălcare a securității care le-ar fi putut compromite total sau parțial portofelul european pentru identitatea digitală sau conținutul lui, în special dacă portofelul european pentru identitatea digitală al utilizatorilor a fost suspendat sau revocat în conformitate cu articolul 5e.

(7) Fără a aduce atingere articolul 5f, statele membre pot să prevadă, în conformitate cu dreptul intern, funcționalități suplimentare ale portofelelor europene pentru identitatea digitală, inclusiv interoperabilitatea cu mijloacele naționale de identificare electronică existente. Aceste funcționalități suplimentare trebuie să fie conforme cu prezentul articol.

(8) Statele membre pun la dispoziție cu titlu gratuit mecanisme de validare pentru:

(a) a asigura faptul că autenticitatea și valabilitatea portofelelor europene pentru identitatea digitală pot fi verificate;

(b) a permite utilizatorilor să verifice autenticitatea și valabilitatea identității beneficiarilor înregistrați în conformitate cu articolul 5b.

(9) Statele membre se asigură că valabilitatea portofelului european pentru identitatea digitală poate fi revocată în următoarele circumstanțe:

(a) la cererea explicită a utilizatorului;

(b) în cazul în care a fost compromisă securitatea portofelului european pentru identitatea digitală;

(c) în caz de deces al utilizatorului sau de încetare a activității persoanei juridice.

(10) Furnizorii de portofele europene pentru identitatea digitală se asigură că utilizatorii pot solicita cu ușurință asistență tehnică și pot raporta problemele tehnice sau orice alte incidente care au impact negativ asupra utilizării portofelului european pentru identitatea digitală.

(11) Portofelele europene pentru identitatea digitală sunt furnizate în cadrul unui sistem de identificare electronică având nivelul de asigurare ridicat.

(12) Portofelele europene pentru identitatea digitală garantează securitatea de la stadiul conceperii.

(13) Portofelele europene pentru identitatea digitală se emit, se utilizează și sunt revocate în mod gratuit pentru toate persoanele fizice.

(14) Utilizatorii au controlul deplin asupra utilizării portofelului lor european pentru identitatea digitală și asupra datelor din acesta. Furnizorul portofelului european pentru identitatea digitală nu colectează informații cu privire la utilizarea portofelului european pentru identitatea digitală care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul european pentru identitatea digitală și nici nu combină date de identificare personală sau orice alte date cu caracter personal stocate sau legate de utilizarea portofelului european pentru identitatea digitală cu date cu caracter personal provenind de la orice alte servicii oferite de respectivul furnizor sau de la servicii furnizate de terți care nu sunt necesare pentru furnizarea serviciilor oferite de portofelul european pentru identitatea digitală, cu excepția cazului în care utilizatorul a solicitat în mod expres contrariul. Datele cu caracter personal legate de punerea la dispoziție de portofele europene pentru identitatea digitală sunt păstrate separate logic de orice alte date deținute de furnizorul de portofele europene pentru identitatea digitală. În cazul în care portofelul european pentru identitatea digitală este furnizat de părți private în conformitate cu alineatul (2) literele (b) și (c) de la prezentul articol, dispozițiile articolului 45h alineatul (3) se aplică *mutatis mutandis*.

(15) Utilizarea portofelelor europene pentru identitatea digitală este voluntară. Accesul la serviciile publice și private, accesul la piața muncii și libertatea de a desfășura o activitate comercială nu sunt în niciun fel restricționate sau permise în condiții mai dezavantajoase pentru persoanele fizice sau juridice care nu utilizează portofelele europene pentru identitatea digitală. Accesul la serviciile publice și private rămâne posibil prin alte mijloace de identificare și autentificare existente.

(16) Cadrul tehnic al portofelului european pentru identitatea digitală:

(a) nu permite furnizorilor de atestate electronice ale atributelor sau oricărei alte părți, după emiterea atestatelor atributelor, să obțină date care permit urmărirea, conectarea sau corelarea tranzacțiilor sau a comportamentul utilizatorului sau obținerea în alt mod de cunoștințe privind tranzacțiile sau comportamentul utilizatorului, cu excepția cazului în care utilizatorul autorizează în mod explicit acest lucru;

(b) permite aplicarea unor tehnici de protecție a vieții private care asigură imposibilitatea stabilirii unei legături, în cazul în care atestarea atributelor nu necesită identificarea utilizatorului.

(17) Orice prelucrare a datelor cu caracter personal efectuată de statele membre sau, în numele acestora, de organisme sau părți responsabile de furnizarea portofelelor europene pentru identitatea digitală drept mijloace de identificare electronică se efectuează în conformitate cu măsuri adecvate și eficace de protecție a datelor. Trebuie să se demonstreze conformitatea unei astfel de prelucrări cu Regulamentul (UE) 2016/679. Statele membre pot adopta dispoziții de drept intern pentru a preciza mai în detaliu aplicarea acestor măsuri.

(18) Statele membre transmit Comisiei, fără întârzieri nejustificate, informații cu privire la:

(a) organismul responsabil cu întocmirea și menținerea listei beneficiarilor înregistrați care recurg la portofelele europene pentru identitatea digitală în conformitate cu articolul 5b alineatul (5) și localizarea acestei liste;

(b) organismele responsabile de furnizarea portofelelor europene pentru identitatea digitală în conformitate cu articolul 5a alineatul (1);

(c) organismele responsabile de asigurarea faptului că datele de identificare personală sunt asociate cu portofelul european pentru identitatea digitală în conformitate cu articolul 5a alineatul (5) litera (f);

(d) mecanismul care permite validarea datelor de identificare personală menționate la articolul 5a alineatul (5) litera (f) și a identității beneficiarilor;

(e) mecanismul de validare a autenticității și valabilității portofelelor europene pentru identitatea digitală.

Comisia pune informațiile transmise în temeiul primului paragraf la dispoziția publicului prin intermediul unui canal sigur, într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.

(19) Fără a aduce atingere alineatului (22) de la prezentul articol, articolul 11 se aplică *mutatis mutandis* portofelului european pentru identitatea digitală.

(20) Articolul 24 alineatul (2) litera (b) și literele (d)-(h) se aplică *mutatis mutandis* furnizorilor de portofelele europene pentru identitatea digitală.

(21) Se asigură accesibilitatea portofelelor europene pentru identitatea digitală pentru ca persoanele cu dizabilități să le poată utiliza în aceleași condiții ca și ceilalți utilizatori, în conformitate cu Directiva (UE) 2019/882 a Parlamentului European și a Consiliului[*].

(22) În scopul furnizării portofelelor europene pentru identitatea digitală, portofelelor europene pentru identitatea digitală și sistemelor de identificare electronică în cadrul cărora sunt furnizate nu li se aplică cerințele prevăzute la articolele 7, 9, 10, 12 și 12a.

(23) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele menționate la alineatele (4), (5), (8) și (18) de la prezentul articol, privind implementarea portofelului european pentru identitatea digitală. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(24) Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații tehnice și proceduri pentru a facilita integrarea utilizatorilor în sistemul reprezentat de portofelul european pentru identitatea digitală fie prin mijloace de identificare electronică conforme cu nivelul de asigurare ridicat, fie prin mijloace de identificare electronică conforme cu nivelul de asigurare substanțial combinate cu proceduri suplimentare de integrare la distanță care, împreună, îndeplinesc cerințele nivelului de asigurare ridicat. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 5b

Beneficiarii portofelului european pentru identitatea digitală

(1) În cazul în care un beneficiar intenționează să recurgă la portofele europene pentru identitatea digitală pentru furnizarea de servicii publice sau private prin intermediul interacțiunii digitale, beneficiarul se înregistrează în statul membru în care este stabilit.

(2) Procesul de înregistrare este eficient din punctul de vedere al costurilor și proporțional cu riscurile. Beneficiarul furnizează cel puțin:

(a) informațiile necesare pentru autentificarea în portofelele europene pentru identitatea digitală, informații care includ cel puțin:

(i) statul membru în care este stabilit beneficiarul; și

(ii) numele beneficiarului și, după caz, numărul său de înregistrare, astfel cum figurează într-un registru oficial, împreună cu datele de identificare ale respectivului registru oficial;

(b) datele de contact ale beneficiarului;

(c) utilizarea preconizată a portofelelor europene pentru identitatea digitală, inclusiv menționarea datelor pe care beneficiarul urmează să le solicite utilizatorilor.

(3) Beneficiarii nu solicită utilizatorilor să furnizeze alte date decât cele menționate în temeiul alineatului (2) litera (c).

(4) Alineatele (1) și (2) nu aduc atingere dreptului Uniunii sau dreptului intern care se aplică prestării de servicii specifice.

(5) Statele membre pun la dispoziția publicului online informațiile menționate la alineatul (2), într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată.

(6) Beneficiarii înregistrați în conformitate cu prezentul articol informează fără întârziere statele membre cu privire la orice modificare a informațiilor furnizate în înregistrarea efectuată în temeiul alineatului (2).

(7) Statele membre stabilesc un mecanism comun care să permită identificarea și autentificarea beneficiarilor, astfel cum se menționează la articolul 5a alineatul (5) litera (c).

(8) Atunci când intenționează să recurgă la portofele europene pentru identitatea digitală, beneficiarii se identifică față de utilizator.

(9) Beneficiarii sunt responsabili de îndeplinirea procedurii de autentificare și validare a datelor de identificare personală și de atestare electronică a atributelor solicitate în cadrul portofelelor europene pentru identitatea digitală. Beneficiarii nu refuză utilizarea pseudonimelor, în cazul în care dreptul Uniunii sau de dreptul intern nu impun identificarea utilizatorului.

(10) Intermediarii care acționează în numele beneficiarilor sunt considerați beneficiari și nu stochează date cu privire la conținutul tranzacției.

(11) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește specificațiile tehnice și procedurile privind cerințele prevăzute la alineatele (2), (5) și (6)-(9) de la prezentul articol prin intermediul unor acte de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se menționează la articolul 5a alineatul (23). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 5c

Certificarea portofelelor europene pentru identitatea digitală

(1) Conformitatea portofelelor europene pentru identitatea digitală și a sistemului de identificare electronică în cadrul căruia sunt furnizate cu cerințele prevăzute la articolul 5a alineatele (4), (5) și (8), cu cerința privind separarea logică prevăzută la articolul 5a alineatul (14) și, după caz, cu standardele și specificațiile tehnice menționate la articolul 5a alineatul (24) este certificată de organisme de evaluare a conformității desemnate de statele membre.

(2) Certificarea conformității portofelelor europene pentru identitatea digitală cu cerințele menționate la alineatul (1) de la prezentul articol care sunt relevante în materie de securitate cibernetică sau cu părți ale acestora se efectuează în conformitate cu sistemele europene de certificare a securității cibernetice adoptate în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului[**] și indicate în actele de punere în aplicare menționate la alineatul (6) de la prezentul articol.

(3) Pentru cerințele menționate la alineatul (1) de la prezentul articol care nu sunt relevante în materie de securitate cibernetică și pentru cerințele menționate la alineatul (1) de la prezentul articol care sunt relevante în materie de securitate cibernetică, în măsura în care sistemele de certificare a securității cibernetice menționate la alineatul (2) de la prezentul articol nu acoperă sau acoperă doar parțial cerințele de securitate cibernetică respective, statele membre instituie, și pentru respectivele cerințe, sisteme de certificare naționale în conformitate cu cerințele stabilite în actele de punere în aplicare menționate la alineatul (6) de la prezentul articol. Statele membre transmit proiectele lor de sisteme de certificare naționale Grupului european de cooperare privind identitatea digitală constituit în temeiul articolului 46e alineatul (1) (denumit în continuare «grupul de cooperare») Grupul de cooperare poate emite avize și recomandări.

(4) Certificarea realizată în temeiul la alineatului (1) este valabilă pentru o perioadă de maximum cinci ani, cu condiția efectuării unei evaluări a vulnerabilității la fiecare doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în timp util, certificarea este anulată.

(5) Respectarea cerințelor stabilite la articolul 5a din prezentul regulament referitoare la operațiunile de prelucrare a datelor cu caracter personal poate să fie certificată în temeiul Regulamentului (UE) 2016/679.

(6) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificarea portofelelor europene pentru identitatea digitală menționată la alineatele (1), (2) și (3) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(7) Statele membre comunică Comisiei denumirile și adresele organismelor de evaluare a conformității menționate la alineatul (1). Comisia pune informațiile respective la dispoziția tuturor statelor membre.

(8) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47 prin care se stabilesc criteriile specifice care urmează să fie îndeplinite de organismele de evaluare a conformității desemnate menționate la alineatul (1) de la prezentul articol.

Articolul 5d

Publicarea unei liste a portofelelor europene pentru identitatea digitală certificate

(1) Statele membre informează, fără întârzieri nejustificate, Comisia și grupul de cooperare constituit în temeiul articolului 46e alineatul (1) cu privire la portofelele europene pentru identitatea digitală care au fost furnizate în temeiul articolului 5a și au fost certificate de organismele de evaluare a conformității menționate la articolul 5c alineatul (1). Statele membre informează, fără întârzieri nejustificate, Comisia și grupul de cooperare constituit în temeiul articolului 46e alineatul (1) în cazul în care o certificare este anulată și indică motivele anulării.

(2) Fără a aduce atingere articolului 5a alineatul (18), informațiile menționate la alineatul (1) de la prezentul articol, furnizate de statele membre, includ cel puțin:

(a) certificatul și raportul de evaluare a certificării portofelului european pentru identitatea digitală certificat;

(b) o descriere a sistemului de identificare electronică în cadrul căruia este furnizat portofelul european pentru identitatea digitală;

(c) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la partea care furnizează portofelul european pentru identitatea digitală;

(d) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică;

(e) dispozițiile pentru suspendarea sau revocarea sistemului de identificare electronică, a autentificării sau a părților compromise în cauză.

(3) Pe baza informațiilor primite în temeiul alineatului (1), Comisia stabilește, publică în *Jurnalul Oficial al Uniunii Europene* și menține într-o formă care poate fi citită automat o listă a portofelelor europene pentru identitatea digitală certificate.

(4) Un stat membru poate transmite Comisiei o cerere de eliminare de pe lista menționată la alineatul (3) a unui portofel european pentru identitatea digitală și a sistemului de identificare electronică în cadrul căruia este furnizat acesta.

(5) În cazul în care informațiile transmise în temeiul alineatului (1) se modifică, statul membru furnizează Comisiei informațiile actualizate.

(6) Comisia actualizează lista menționată la alineatul (3) prin publicarea în *Jurnalul Oficial al Uniunii Europene* a modificărilor corespunzătoare aduse listei în termen de o lună de la primirea unei cereri în temeiul alineatului (4) sau a informațiilor actualizate în temeiul alineatului (5).

(7) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește formatele și procedurile aplicabile în vederea îndeplinirii cerințelor prevăzute la alineatele (1), (4) și (5) de la prezentul articol prin intermediul unor acte de punere în aplicare cu privire la implementarea portofelelor europene pentru identitatea digitală, astfel cum se menționează la articolul 5a alineatul (23). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 5e

Încălcarea securității portofelelor europene pentru identitatea digitală

(1) În cazul în care portofelele europene pentru identitatea digitală furnizate în temeiul articolului 5a, mecanismele de validare menționate la articolul 5a alineatul (8) sau sistemul de identificare electronică în cadrul căruia sunt furnizate portofelele europene pentru identitatea digitală fac obiectul unei încălcări a securității sau sunt compromise parțial într-un mod care afectează fiabilitatea lor sau a altor portofele europene pentru identitatea digitală, statele membre care au furnizat portofelele europene pentru identitatea digitală suspendă fără întârziere nejustificată furnizarea și utilizarea portofelelor europene pentru identitatea digitală.

În cazul în care acest lucru este justificat de gravitatea încălcării securității sau a compromiterii menționate la primul paragraf, statul membru retrage fără întârzieri nejustificate portofelele europene pentru identitatea digitală.

Statul membru informează în mod corespunzător utilizatorii afectați, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1), beneficiarii și Comisia.

(2) În cazul în care încălcarea securității sau compromiterea menționată la alineatul (1) primul paragraf de la prezentul articol nu este remediată în termen de trei luni de la suspendare, statul membru care a furnizat portofelele europene pentru identitatea digitală retrage portofelele europene pentru identitatea digitală și le revocă valabilitatea. Statul membru informează în mod corespunzător utilizatorii afectați, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1), beneficiarii și Comisia cu privire la retragere.

(3) În cazul în care încălcarea securității sau compromiterea menționată la alineatul (1) primul paragraf de la prezentul articol este remediată, statul membru furnizor reia furnizarea și utilizarea portofelelor europene pentru identitatea digitală și informează fără întârzieri nejustificate utilizatorii și beneficiarii afectați, punctele unice de contact desemnate în temeiul articolului 46c alineatul (1) și Comisia.

(4) Comisia publică în *Jurnalul Oficial al Uniunii Europene*, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la articolul 5d.

(5) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru măsurile menționate la alineatele (1), (2) și (3) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 5f

Utilizarea transfrontalieră a portofelelor europene pentru identitatea digitală

(1) În cazul în care statele membre solicită identificarea și autentificarea electronică pentru a accesa un serviciu online furnizat de un organism din sectorul public, acestea acceptă și portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu prezentul regulament.

(2) În cazul în care beneficiarii privați care furnizează servicii, cu excepția microîntreprinderilor și a întreprinderilor mici, astfel cum sunt definite la articolul 2 din anexa la Recomandarea 2003/361/CE a Comisiei[***], au obligația în temeiul dreptului Uniunii sau al dreptului intern să utilizeze autentificarea strictă a utilizatorului pentru identificarea online sau în cazul în care autentificarea strictă a utilizatorului pentru identificarea online este obligatorie în temeiul unei obligații contractuale, inclusiv în domeniile transporturilor, energiei, serviciilor bancare și financiare, securității sociale, sănătății, apei potabile, serviciilor poștale, infrastructurii digitale, educației sau telecomunicațiilor, respectivii beneficiari privați, în termen de 36 de luni de la data intrării în vigoare a actelor de punere în aplicare menționate la articolul 5a alineatul (23) și la articolul 5c alineatul (6) și, numai la cererea voluntară a utilizatorului, acceptă și utilizarea portofelelor europene pentru identitatea digitală care sunt furnizate în conformitate cu prezentul regulament.

(3) În cazul în care furnizorii de platforme online foarte mari menționate la articolul 33 din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului[****] impun autentificarea utilizatorului pentru accesul la servicii online, aceștia acceptă și facilitează și utilizarea portofelelor europene pentru identitatea digitală care sunt furnizate în conformitate cu prezentul regulament pentru autentificarea utilizatorului, numai la cererea voluntară a acestuia și în ceea ce privește datele minime necesare pentru serviciul online specific pentru care se solicită autentificarea.

(4) În cooperare cu statele membre, Comisia facilitează elaborarea unor coduri de conduită în strânsă colaborare cu toate părțile interesate relevante, inclusiv cu societatea civilă, pentru a contribui la disponibilitatea și utilizarea pe scară largă a portofelelor europene pentru identitatea digitală care se încadrează în domeniul de aplicare al prezentului regulament și pentru a încuraja prestatorii de servicii să finalizeze elaborarea codurilor de conduită.

(5) În termen de 24 de luni de la implementarea portofelelor europene pentru identitatea digitală, Comisia evaluează cererea, disponibilitatea și posibilitatea de utilizare a portofelelor europene pentru identitatea digitală, ținând seama de criterii precum adoptarea de către utilizatori, prezența transfrontalieră a prestatorilor de servicii, evoluțiile tehnologice, evoluția modelelor de utilizare și cererea consumatorilor.

---

* Directiva (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor (JO L 151, 7.6.2019, p. 70).

** 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).

*** 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).

**** 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).”

6. Se introduce următorul titlu înainte de articolul 6:

„SECȚIUNEA 2
SISTEME DE IDENTIFICARE ELECTRONICĂ”.

7. La articolul 7, litera (g) se înlocuiește cu următorul text:

„(g) cu cel puțin șase luni înaintea notificării efectuate în temeiul articolului 9 alineatul (1), statul membru care notifică furnizează celorlalte state membre, în scopul aplicării articolului 12 alineatul (5), o descriere a sistemului respectiv în conformitate cu modalitățile procedurale prevăzute în actele de punere în aplicare adoptate în temeiul articolului 12 alineatul (6);”.

8. La articolul 8 alineatul (3), primul paragraf se înlocuiește cu următorul text:

„(3) Până la 18 septembrie 2015, ținând cont de standardele internaționale relevante și sub rezerva alineatului (2), Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice, standardele și procedurile minime, în raport cu care sunt determinate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică.”

9. La articolul 9, alineatele (2) și (3) se înlocuiesc cu următorul text:

„(2) Comisia publică în *Jurnalul Oficial al Uniunii Europene*, fără întârzieri nejustificate, o listă a sistemelor de identificare electronică ce au fost notificate în temeiul alineatului (1), împreună cu informațiile de bază cu privire la aceste sisteme.

(3) Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările la lista menționată la alineatul (2) în termen de o lună de la data primirii respectivei notificări.”

10. La articolul 10, titlul se înlocuiește cu următorul text:

„Încălcarea securității sistemelor de identificare electronică”.

11. Se introduce următorul articol:

„*Articolul 11a*
Corelarea transfrontalieră a identităților

(1) Atunci când acționează în calitate de beneficiari ai unor servicii transfrontaliere, statele membre asigură corelarea fără echivoc a identităților pentru persoanele fizice care utilizează mijloace de identificare electronică notificate sau portofele europene pentru identitatea digitală.

(2) Statele membre prevăd măsuri tehnice și organizatorice pentru a asigura un nivel ridicat de protecție a datelor cu caracter personal utilizate pentru corelarea identităților și pentru a preveni crearea de profiluri ale utilizatorilor.

(3) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele menționate la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

12. Articolul 12 se modifică după cum urmează:

(a) titlul se înlocuiește cu următorul text:

„Interoperabilitate”;

(b) alineatul (3) se modifică după cum urmează:

(i) litera (c) se înlocuiește cu următorul text:

„(c) facilitează protecția, începând cu momentul conceperii, a vieții private și a securității («privacy and security by design»);”;

(ii) litera (d) se elimină;

(c) la alineatul (4), litera (d) se înlocuiește cu următorul text:

„(d) o trimitere la un set minim de date de identificare personală necesare pentru a reprezenta în mod unic o persoană fizică sau juridică sau o persoană fizică ce reprezintă o altă persoană fizică sau o persoană juridică, care sunt disponibile din sistemele de identificare electronică;”;

(d) alineatele (5) și (6) se înlocuiesc cu următorul text:

„(5) Statele membre efectuează evaluări *inter pares* ale sistemelor de identificare electronică care intră în domeniul de aplicare al prezentului regulament și care trebuie să fie notificate în conformitate cu articolul 9 alineatul (1) litera (a).

(6) Până la 18 martie 2025, Comisia stabilește, prin intermediul unor acte de punere în aplicare, modalitățile procedurale necesare pentru efectuarea evaluărilor *inter pares* menționate la alineatul (5) de la prezentul articol, în vederea stimulării unui nivel ridicat de încredere și securitate corespunzător gradului de risc. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”;

(e) alineatul (7) se elimină;

(f) alineatul (8) se înlocuiește cu următorul text:

„(8) Până la 18 septembrie 2025, în vederea stabilirii unor condiții uniforme pentru punerea în aplicare a cerinței menționate la alineatul (1) de la prezentul articol, sub rezerva criteriilor stabilite la alineatul (3) de la prezentul articol și luând în considerare rezultatele cooperării dintre statele membre, Comisia adoptă acte de punere în aplicare privind cadrul de interoperabilitate, astfel cum este prevăzut la alineatul (4) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

13. În capitolul II se introduc următoarele articole:

„*Articolul 12a*

Certificarea sistemelor de identificare electronică

(1) Conformitatea sistemelor de identificare electronică ce trebuie notificate cu cerințele privind securitatea cibernetică prevăzute în prezentul regulament, inclusiv conformitatea cu cerințele relevante în materie de securitate cibernetică prevăzute la articolul 8 alineatul (2) în ceea ce privește nivelurile de asigurare ale sistemelor de identificare electronică, este certificată de organismele de evaluare a conformității desemnate de statele membre.

(2) Certificarea efectuată în temeiul alineatului (1) de la prezentul articol se efectuează în cadrul unui sistem de certificare a securității cibernetice relevant în conformitate cu Regulamentul (UE) 2019/881 sau al unor părți ale acestuia, în măsura în care certificatul de securitate cibernetică sau unele părți ale acestuia acoperă respectivele cerințe privind securitatea cibernetică.

(3) Certificarea efectuată în temeiul alineatului (1) este valabilă pentru o perioadă de maximum cinci ani, cu condiția să se efectueze o evaluare a vulnerabilității o dată la doi ani. În cazul în care este identificată o vulnerabilitate și aceasta nu este remediată în termen de trei luni de la identificarea sa, certificarea este anulată.

(4) În pofida alineatului (2), statele membre pot, în conformitate cu alineatul respectiv, să solicite de la un stat membru care notifică informații suplimentare cu privire la sistemele de identificare electronică sau la părți certificate ale acestora.

(5) Evaluarea *inter pares* privind sistemele de identificare electronică menționată la articolul 12 alineatul (5) nu se aplică sistemelor de identificare electronică sau unor părți ale acestor sisteme certificate în conformitate cu alineatul (1) de la prezentul articol. Statele membre pot utiliza un certificat sau o declarație de conformitate, emis(ă) în conformitate cu un sistem de certificare relevant sau cu părți ale unor astfel de sisteme, cu cerințele care nu țin de securitatea cibernetică prevăzute la articolul 8 alineatul (2) în ceea ce privește nivelul de asigurare ale sistemelor de identificare electronică.

(6) Statele membre transmite Comisiei denumirile și adresele organismelor de evaluare a conformității menționate la alineatul (1). Comisia pune informațiile respective la dispoziția tuturor statelor membre.

Articolul 12b

Accesul la componentele de hardware și de software

Atunci când furnizorii de portofele europene pentru identitatea digitală și emitenții de mijloace de identificare electronică notificate, care acționează cu titlu comercial sau profesional și utilizează servicii de platformă esențiale în sensul definiției de la articolul 2 punctul 2 din Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului* în scopul sau în cursul furnizării de servicii specifice portofelelor europene pentru identitatea digitală și de mijloace de identificare electronică utilizatorilor finali, sunt utilizatori comerciali în sensul definiției de la articolul 2 punctul 21 din regulamentul menționat, controlorii de acces le permit, în special, să beneficieze în mod efectiv de interoperabilitatea cu aceleași componente ale sistemului de operare, ale hardware-ului sau ale software-ului, precum și să aibă acces la respectivele componente în vederea asigurării interoperabilității. Interoperabilitatea efectivă și accesul menționate anterior sunt permise cu titlu gratuit și indiferent dacă componentele de hardware sau de software fac parte din sistemul de operare, în aceleași condiții în care respectivele componente îi sunt disponibile respectivului controlor de acces sau sunt folosite de acesta atunci când furnizează astfel de servicii, în sensul articolului 6 alineatul (7) din Regulamentul (UE) 2022/1925. Prezentul articol nu aduce atingere articolului 5a alineatul (14) din prezentul regulament.

---

* Regulamentul (UE) 2022/1925 al Parlamentului European și al Consiliului din 14 septembrie 2022 privind piețe contestabile și echitabile în sectorul digital și de modificare a Directivelor (UE) 2019/1937 și (UE) 2020/1828 (Regulamentul privind piețele digitale) (JO L 265, 12.10.2022, p. 1).”

14. La articolul 13, alineatul (1) se înlocuiește cu următorul text:

„(1) În pofida alineatului (2) de la prezentul articol și fără a aduce atingere Regulamentului (UE) 2016/679, prestatorii de servicii de încredere sunt răspunzători pentru prejudiciile cauzate în mod intenționat sau din neglijență oricărei persoane fizice sau juridice ca urmare a nerespectării obligațiilor prevăzute în prezentul regulament. Orice persoană fizică sau juridică ce a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament de către un prestator de servicii de încredere are dreptul de a solicita despăgubiri în conformitate cu dreptul Uniunii și cu dreptul intern.

Sarcina de a proba intenția sau neglijența unui prestator de servicii de încredere necalificat revine persoanei fizice sau juridice care introduce o acțiune în despăgubiri pentru prejudiciul menționat la primul paragraf.

Intenția sau neglijența din partea unui prestator de servicii de încredere calificat este prezumată, cu excepția cazului în care respectivul prestator de servicii de încredere calificat dovedește că prejudiciul menționat la primul paragraf nu a intervenit din intenția sau din neglijența sa.”

15. Articolele 14, 15 și 16 se înlocuiesc cu următorul text:

„*Articolul 14*
Aspecte internaționale

(1) Serviciile de încredere prestate de prestatori de servicii de încredere stabiliți într-o țară terță sau de o organizație internațională sunt recunoscute ca fiind echivalente din punct de vedere juridic cu serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune dacă serviciile de încredere care provin din țara terță sau de la organizația internațională sunt recunoscute prin intermediul unor acte de punere în aplicare sau al unui acord încheiat între Uniune și țara terță sau organizația internațională în cauză în conformitate cu articolul 218 din TFUE.

Actele de punere în aplicare menționate la primul paragraf se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(2) Actele de punere în aplicare și acordul menționate la alineatul (1) garantează că cerințele aplicabile prestatorilor de servicii de încredere calificați stabiliți în Uniune și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de prestatorii de servicii de încredere din țara terță în cauză sau de organizațiile internaționale, precum și de serviciile de încredere pe care aceștia le prestează. În special, țările terțe și organizațiile internaționale elaborează, mențin și publică o listă sigură a prestatorilor de servicii de încredere recunoscuți.

(3) Acordurile menționate la alineatul (1) garantează că serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune sunt recunoscute ca echivalente din punct de vedere juridic cu serviciile de încredere prestate de prestatorii de servicii de încredere din țara terță sau de organizația internațională cu care a fost încheiat acordul.

Articolul 15
Accesibilitatea pentru persoanele cu dizabilități și cu nevoi speciale

Mijloacele de identificare electronică, prestarea serviciilor de încredere și furnizarea produselor destinate utilizatorului final care sunt utilizate pentru prestarea serviciilor respective sunt furnizate într-un limbaj clar și inteligibil și în conformitate cu Convenția Națiunilor Unite privind drepturile persoanelor cu handicap și cu cerințele de accesibilitate prevăzute în Directiva (UE) 2019/882, fiind astfel accesibile și persoanelor care se confruntă cu limitări funcționale, cum ar fi persoanele în vârstă, și persoanelor cu acces limitat la tehnologiile digitale.

Articolul 16
Sancțiuni

(1) Fără a aduce atingere articolului 31 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[*], statele membre stabilesc normele referitoare la sancțiunile aplicabile în cazul încălcării prezentului regulament. Sancțiunile respective trebuie să fie eficace, proporționale și cu efect de descurajare.

(2) Statele membre se asigură că încălcările prezentului regulament de către prestatorii de servicii de încredere calificați și necalificați fac obiectul unor amenzi administrative în valoare de cel puțin:

(a) 5 000 000 EUR, în cazul în care prestatorul de servicii de încredere este o persoană fizică; sau

(b) în cazul în care prestatorul de servicii de încredere este o persoană juridică, 5 000 000 EUR sau 1 % din cifra de afaceri anuală totală la nivel mondial a întreprinderii căreia i-a aparținut prestatorul de servicii de încredere în exercițiul financiar anterior anului în care a avut loc încălcarea, luându-se în considerare valoarea cea mai mare.

(3) În funcție de sistemul juridic al statelor membre, normele privind amenzile administrative pot fi aplicate astfel încât amenda să fie inițiată de organismul de supraveghere competent și aplicată de instanțele naționale competente. Aplicarea acestor norme în statele membre respective garantează faptul că respectivele măsuri juridice sunt eficiente și au un efect echivalent cu cel al amenzilor administrative aplicate direct de autoritățile de supraveghere.

---

* 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).”

16. În capitolul III secțiunea 2, titlul se înlocuiește cu următorul text:

„Servicii de încredere necalificate”.

17. Articolele 17 și 18 se elimină.

18. În capitolul III secțiunea 2 se introduce următorul articol:

„*Articolul 19a*
Cerințe pentru prestatorii de servicii de încredere necalificați

(1) Un prestator de servicii de încredere necalificat care prestează servicii de încredere necalificate:

(a) dispune de politici adecvate și ia măsurile corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau indirecte legate de prestarea serviciului de încredere necalificat, care, în pofida articolului 21 din Directiva (UE) 2022/2555, includ cel puțin măsuri referitoare la:

(i) procedurile de înregistrare și de integrare legate de un serviciu de încredere;

(ii) controalele procedurale sau administrative necesare pentru prestarea de servicii de încredere;

(iii) gestionarea și implementarea serviciilor de încredere;

(b) notificarea organismului de supraveghere, persoanelor afectate care pot fi identificate, publicului – dacă chestiunea este de interes public –, și, după caz, altor autorități competente relevante, cu privire la orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la litera (a) punctul (i), (ii) sau (iii) care are impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, nu mai târziu de 24 de ore din momentul în care a luat cunoștință de orice încălcare a securității sau perturbare.

(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri în scopul alineatului (1) litera (a) de la prezentul articol. În cazul în care standardele, specificațiile și procedurile respective sunt respectate, se prezumă că sunt respectate cerințele prevăzute la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

19. Articolul 20 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin la fiecare 24 de luni, de către un organism de evaluare a conformității. Auditul confirmă că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament și la articolul 21 din Directiva (UE) 2022/2555. Prestatorii de servicii de încredere calificați transmit raportul de evaluare a conformității care a rezultat organismului de supraveghere în termen de trei zile lucrătoare de la primirea lui.”;

(b) se introduc următoarele alineate:

„(1a) Prestatorii de servicii de încredere calificați informează organismul de supraveghere cu cel puțin o lună înainte de un audit planificat și, la cerere, îi permit organismului de supraveghere să participe în calitate de observator.

(1b) Statele membre notifică Comisiei, fără întârzieri nejustificate, denumirile, adresele și detaliile de acreditare ale organismelor de evaluare a conformității menționate la alineatul (1), precum și orice modificări ulterioare ale acestora. Comisia pune informațiile respective la dispoziția tuturor statelor membre.”;

(c) alineatele (2), (3) și (4) se înlocuiesc cu următorul text:

„(2) Fără a aduce atingere alineatului (1), organismul de supraveghere poate, în orice moment, să efectueze un audit sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității privind prestatorii de servicii de încredere calificați, pe cheltuiala prestatorilor de servicii de încredere respectivi, pentru a confirma că aceștia și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament. În cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, organismul de supraveghere informează, fără întârzieri nejustificate, autoritățile de supraveghere competente înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679.

(3) În cazul în care prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în prezentul regulament, organismul de supraveghere îi solicită să remedieze situația într-un termen stabilit, dacă este cazul.

În cazul în care prestatorul respectiv nu remediază situația, dacă este cazul în termenul stabilit de organismul de supraveghere, acesta din urmă, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei neîndepliniri, retrage statutul de calificat al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.

(3a) În cazul în care autoritățile competente desemnate sau înființate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555 informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute la articolul 21 din respectiva directivă, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei neîndepliniri, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.

(3b) În cazul în care autoritățile de supraveghere înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679 informează organismul de supraveghere că prestatorul de servicii de încredere calificat nu îndeplinește oricare dintre cerințele prevăzute în regulamentul menționat, organismul de supraveghere, atunci când acest lucru este justificat în special de amploarea, durata și consecințele respectivei neîndepliniri, retrage statutul de calificat al prestatorului respectiv sau al serviciului afectat pe care îl prestează acesta.

(3c) Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire la retragerea statutului de calificat, al său sau al serviciului în cauză. Organismul de supraveghere informează organismul notificat în temeiul articolului 22 alineatul (3) din prezentul regulament în scopul actualizării listelor sigure menționate la alineatul (1) de la articolul respectiv, precum și autoritatea competentă desemnată sau înființată în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555.

(4) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru:

(a) acreditarea organismelor de evaluare a conformității și pentru raportul de evaluare a conformității menționat la alineatul (1);

(b) cerințele de audit pe baza cărora organismele de evaluare a conformității își desfășoară evaluarea conformității, inclusiv evaluarea compozită, a prestatorilor de servicii de încredere calificați, astfel cum se menționează la alineatul (1);

(c) sistemele de evaluare a conformității utilizate de organismele de evaluare a conformității pentru efectuarea evaluării conformității prestatorilor de servicii de încredere calificați și pentru furnizarea raportului menționat la alineatul (1).

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

20. Articolul 21 se modifică după cum urmează:

(a) alineatele (1) și (2) se înlocuiesc cu următorul text:

„(1) În cazul în care prestatorii de servicii de încredere intenționează să înceapă prestarea unui serviciu de încredere calificat, aceștia informează organismul de supraveghere cu privire la intenția lor, însoțită de un raport de evaluare a conformității emis de un organism de evaluare a conformității, care confirmă îndeplinirea cerințelor prevăzute în prezentul regulament și la articolul 21 din Directiva (UE) 2022/2555.

(2) Organismul de supraveghere verifică dacă prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezentul regulament și, în special, cerințele pentru prestatorii de servicii de încredere calificați și pentru serviciile de încredere calificate prestate de aceștia.

Pentru a verifica respectarea de către prestatorul de servicii de încredere a cerințelor prevăzute la articolul 21 din Directiva (UE) 2022/2555, organismul de supraveghere solicită autorităților competente desemnate sau înființate în temeiul articolului 8 alineatul (1) din respectiva directivă să desfășoare acțiuni de supraveghere în această privință și să furnizeze informații cu privire la rezultat fără întârzieri nejustificate și, în orice caz, în termen de două luni de la primirea cererii respective. În cazul în care verificarea nu este încheiată în termen de două luni de la notificare, autoritățile competente respective informează organismul de supraveghere, specificând motivele întârzierii și termenul în care urmează să se încheie verificarea.

În cazul în care organismul de supraveghere ajunge la concluzia că prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezentul regulament, organismul de supraveghere acordă statutul de calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de acesta și informează în consecință organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1), în termen de trei luni de la notificare, în conformitate cu alineatul (1) de la prezentul articol.

În cazul în care verificarea nu este încheiată în termen de trei luni de la notificare, organismul de supraveghere informează prestatorul de servicii de încredere, specificând motivele întârzierii și termenul în care urmează să se încheie verificarea.”;

(b) alineatul (4) se înlocuiește cu următorul text:

„(4) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, formatele și procedurile de notificare și verificare în vederea aplicării alineatelor (1) și (2) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

21. Articolul 24 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) Atunci când emite un certificat calificat sau un atestat electronic calificat al atributelor, un prestator de servicii de încredere calificat verifică identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia urmează să i se emită certificatul calificat sau atestatul electronic calificat al atributelor.

(1a) Verificarea identității menționată la alineatul (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora atunci când este necesar, în conformitate cu actele de punere în aplicare menționate la alineatul (1c):

(a) prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la articolul 8 în ceea ce privește nivelul de asigurare ridicat;

(b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu litera (a), (c) sau (d);

(c) prin utilizarea altor metode de identificare care asigură identificarea persoanei cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității;

(d) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu dreptul intern.

(1b) Verificarea atributelor menționată la alineatul (1) se realizează, prin mijloace adecvate, de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unui terț, pe baza uneia dintre următoarele metode sau a unei combinații a acestora, atunci când este necesar, în conformitate cu actele de punere în aplicare menționate la alineatul (1c):

(a) prin intermediul portofelului european pentru identitatea digitală sau al unui mijloc de identificare electronică notificat care îndeplinește cerințele stabilite la articolul 8 în ceea ce privește nivelul de asigurare ridicat;

(b) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu alineatul (1a) litera (a), (c) sau (d);

(c) prin intermediul unui atestat electronic calificat al atributelor;

(d) prin utilizarea altor metode, care asigură verificarea atributelor cu un nivel ridicat de încredere, a căror conformitate este confirmată de un organism de evaluare a conformității;

(e) prin prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin utilizarea unor mijloace de probă și proceduri adecvate, în conformitate cu dreptul intern.

(1c) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru verificarea identității și a atributelor în conformitate cu alineatele (1), (1a) și (1b) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2). ”;

(b) alineatul (2) se modifică după cum urmează:

(i) litera (a) se înlocuiește cu următorul text:

„(a) informează organismul de supraveghere cu cel puțin o lună înainte de punerea în aplicare a oricărei modificări în prestarea serviciilor sale de încredere calificate sau cu cel puțin trei luni înainte în cazul în care intenționează să înceteze activitățile respective;”;

(ii) literele (d) și (e) se înlocuiesc cu următorul text:

„(d) înainte de stabilirea unei relații contractuale, informează, în mod clar, cuprinzător și ușor accesibil, într-un spațiu accesibil publicului și în mod individual, orice persoană care dorește să utilizeze un serviciu de încredere calificat în ceea ce privește clauzele și condițiile exacte privind utilizarea acelui serviciu, inclusiv orice restricție privind utilizarea acestuia;

(e) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și asigură siguranța tehnică și fiabilitatea proceselor susținute de acestea, inclusiv prin folosirea unor tehnici criptografice adecvate;”;

(iii) se introduc următoarele litere:

„(fa) în pofida articolului 21 din Directiva (UE) 2022/2555, dispune de politici adecvate și ia măsuri corespunzătoare pentru a gestiona riscurile juridice, comerciale, operaționale și alte riscuri directe sau indirecte legate de prestarea serviciului de încredere calificat, inclusiv cel puțin măsuri referitoare la următoarele aspecte:

(i) procedurile de înregistrare și de integrare legate de un serviciu;

(ii) controalele procedurale sau administrative;

(iii) gestionarea și implementarea serviciilor;

(fb) notifică organismului de supraveghere, persoanelor afectate care pot fi identificate, altor organisme competente relevante, după caz, și, la cererea organismului de supraveghere, publicului, dacă chestiunea este de interes public, orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la litera (fa) punctul (i), (ii) sau (iii) care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate în cadrul acestuia, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la producerea incidentului;”;

(iv) literele (g), (h) și (i) se înlocuiesc cu următorul text:

„(g) ia măsuri adecvate împotriva falsificării, furtului sau însușirii ilegale de date ori împotriva ștergerii sau modificării neautorizate a datelor sau a acțiunii neautorizate de a le face inaccesibile;

(h) înregistrează și menține accesibile atât timp cât este necesar, după încetarea activității prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către acesta, în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic;

(i) are un plan actualizat pentru a asigura, în cazul încetării serviciului, continuitatea serviciului conform dispozițiilor verificate de organismul de supraveghere în conformitate cu articolul 46b alineatul (4) litera (i);”;

(v) litera (j) se elimină;

(vi) se adaugă următorul paragraf:

„Organismul de supraveghere poate solicita informații în plus față de informațiile notificate în temeiul primului paragraf litera (a) sau rezultatul unei evaluări a conformității și poate stabili anumite condiții pentru acordarea permisiunii de a pune în aplicare modificările preconizate ale serviciilor de încredere calificate. În cazul în care verificarea nu este încheiată în termen de trei luni de la notificare, organismul de supraveghere informează prestatorul de servicii de încredere, specificând motivele întârzierii și termenul în care urmează să se încheie verificarea.”;

(c) alineatul (5) se înlocuiește cu următorul text:

„(4a) Alineatele (3) și (4) se aplică în mod corespunzător revocării atestatelor electronice calificate ale atributelor.

(4b) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47, pentru a stabili măsurile suplimentare menționate la alineatul (2) litera (fa) de la prezentul articol.

(5) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele menționate la alineatul (2) de la prezentul articol. În cazul în care standardele, specificațiile și procedurile respective sunt respectate, se prezumă că sunt respectate cerințele prevăzute la prezentul alineat. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

22. În capitolul III secțiunea 3 se introduce următorul articol:

„*Articolul 24a*

Recunoașterea serviciilor de încredere calificate

(1) Semnăturile electronice calificate bazate pe un certificat calificat emis într-un stat membru și sigiliile electronice calificate bazate pe un certificat calificat emis într-un stat membru sunt recunoscute drept semnături electronice calificate și, respectiv, drept sigilii electronice calificate în toate celelalte state membre.

(2) Dispozitivele de creare a semnăturilor electronice calificate și dispozitivele de creare a sigiliilor electronice calificate certificate într-un stat membru sunt recunoscute drept dispozitive de creare a semnăturilor electronice calificate și, respectiv, drept dispozitive de creare a sigiliilor electronic calificate în toate celelalte state membre.

(3) Un certificat calificat pentru semnăturile electronice, un certificat calificat pentru sigilii electronice, un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță și un serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță furnizat într-un stat membru este recunoscut drept certificat calificat pentru semnăturile electronice, drept certificat calificat pentru sigilii electronice, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță și, respectiv, drept serviciu de încredere calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță în toate celelalte state membre.

(4) Un serviciu de validare calificat pentru semnături electronice calificate și un serviciu de validare calificat pentru sigilii electronice calificate furnizat într-un stat membru este recunoscut drept serviciu de validare calificat pentru semnături electronice calificate și, respectiv, drept serviciu de validare calificat pentru sigilii electronice calificate în toate celelalte state membre.

(5) Un serviciu calificat de păstrare a semnăturilor electronice calificate și un serviciu calificat de păstrare a sigiliilor electronice calificate furnizat într-un stat membru este recunoscut drept serviciu calificat de păstrare a semnăturilor electronice calificate și, respectiv, drept serviciu calificat de păstrare a sigiliilor electronice calificate în toate celelalte state membre.

(6) O marcă temporală electronică calificată furnizată într-un stat membru este recunoscută drept marcă temporală electronică calificată în toate celelalte state membre.

(7) Un certificat calificat pentru autentificarea unui site internet emis într-un stat membru este recunoscut drept certificat calificat pentru autentificarea unui site internet în toate celelalte state membre.

(8) Un serviciu de distribuție electronică înregistrată calificat furnizat într-un stat membru este recunoscut drept serviciu de distribuție electronică înregistrată calificat în toate celelalte state membre.

(9) Un atestat electronic calificat al atributelor emis într-un stat membru este recunoscut drept atestat electronic calificat al atributelor în toate celelalte state membre.

(10) Un serviciu calificat de arhivare electronică furnizat într-un stat membru este recunoscut drept serviciu calificat de arhivare electronică în toate celelalte state membre.

(11) Un registru electronic calificat furnizat într-un stat membru este recunoscut drept registru electronic calificat în toate celelalte state membre.”

23. La articolul 25, alineatul (3) se elimină.

24. Articolul 26 se modifică după cum urmează:

(a) unicul paragraf devine alineatul (1);

(b) se adaugă următorul alineat:

(2) Până la … [24 de luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia evaluează dacă este necesar să adopte acte de punere în aplicare prin care să stabilească o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru semnăturile electronice avansate. Pe baza rezultatului evaluării respective, Comisia poate adopta astfel de acte de punere în aplicare. În cazul în care o semnătură electronică avansată îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele referitoare la semnăturile electronice avansate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

25. La articolul 27, alineatul (4) se elimină.

26. La articolul 28, alineatul (6) se înlocuiește cu următorul text:

„(6) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificatele calificate pentru semnăturile electronice. În cazul în care un certificat calificat pentru semnătura electronică îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele prevăzute în anexa I. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

27. La articolul 29 se introduce următorul alineat:

„(1a) Generarea sau gestionarea datelor de creare a semnăturii electronice sau duplicarea unor astfel de date de creare a semnăturii în scopul creării unei copii de rezervă se realizează numai în numele semnatarului și la cererea acestuia și de către un prestator de servicii de încredere calificat care prestează un serviciu de încredere calificat pentru gestionarea unui dispozitiv calificat de creare a semnăturii electronice la distanță.”

28. Se introduce următorul articol:

„*Articolul 29a*
Cerințe privind un serviciu calificat pentru gestionarea
dispozitivelor calificate de creare a semnăturii electronice la distanță

(1) Gestionarea dispozitivelor calificate de creare a semnăturii electronice la distanță în calitate de serviciu calificat se efectuează numai de către un prestator de servicii de încredere calificat care:

(a) generează sau gestionează datele de creare a semnăturilor electronice în numele semnatarului;

(b) în pofida punctului 1 litera (d) din anexa II, duplică datele de creare a semnăturilor electronice numai în scopul creării unei copii de rezervă, cu condiția să fie îndeplinite următoarele cerințe:

(i) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale;

(ii) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului;

(c) respectă toate cerințele identificate în raportul de certificare a dispozitivului calificat specific de creare a semnăturii electronice la distanță, emis în temeiul articolului 30.

(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri în scopul aplicării alineatului (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

29. La articolul 30 se introduce următorul alineat:

„(3a) Perioada de valabilitate a certificării menționate la alineatul (1) nu depășește cinci ani, cu condiția efectuării unei evaluări a vulnerabilităților la fiecare doi ani. În cazul în care sunt identificate vulnerabilități și acestea nu sunt remediate, certificarea este anulată.”

30. La articolul 31, alineatul (3) se înlocuiește cu următorul text:

„(3) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, formatele și procedurile aplicabile în vederea îndeplinirii cerințelor prevăzute la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

31. Articolul 32 se modifică după cum urmează:

(a) la alineatul (1), se adaugă următorul paragraf:

„În cazul în care validarea semnăturilor electronice calificate respectă standardele, specificațiile și procedurile menționate la alineatul (3), se prezumă că sunt respectate cerințele prevăzute la primul paragraf de la prezentul alineat.”;

(b) alineatul (3) se înlocuiește cu următorul text:

„(3) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru validarea semnăturilor electronice calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

32. Se introduce următorul articol:

„*Articolul 32a*
Cerințe pentru validarea semnăturilor electronice avansate bazate pe certificate calificate

(1) Prin procesul de validare a unei semnături electronice avansate bazate pe un certificat calificat se confirmă validitatea semnăturii electronice avansate bazate pe un certificat calificat în următoarele condiții:

(a) certificatul care stă la baza semnăturii să fi fost, la momentul semnării, un certificat calificat pentru semnătura electronică conform cu anexa I;

(b) certificatul calificat să fi fost emis de un prestator de servicii de încredere calificat și să fi fost valabil la momentul semnării;

(c) datele de validare a semnăturii să corespundă datelor furnizate de beneficiar;

(d) setul unic de date care reprezintă semnatarul în certificat să fie furnizat corect beneficiarului;

(e) în cazul în care la momentul semnării s-a folosit un pseudonim, utilizarea acestuia să fie indicată clar beneficiarului;

(f) integritatea datelor semnate să nu fi fost compromisă;

(g) cerințele prevăzute la articolul 26 să fi fost îndeplinite la momentul semnării.

(2) Sistemul utilizat pentru validarea semnăturii electronice avansate bazate pe un certificat calificat furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.

(3) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru validarea semnăturilor electronice avansate bazate pe certificate calificate. În cazul în care validarea semnăturii electronice avansate bazate pe certificate calificate îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele prevăzute la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

33. La articolul 33, alineatul (2) se înlocuiește cu următorul text:

„(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru serviciul calificat de validare menționat la alineatul (1) de la prezentul articol. În cazul în care serviciul calificat de validare pentru semnături electronice calificate îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele de la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

34. Articolul 34 se modifică după cum urmează:

(a) se introduce următorul alineat:

„(1a) În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele, specificațiile și procedurile menționate la alineatul (2), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).”;

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru serviciul calificat de păstrare a semnăturilor electronice calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

35. La articolul 35, alineatul (3) se elimină.

36. Articolul 36 se modifică după cum urmează:

(a) unicul paragraf devine alineatul (1);

(b) se adaugă următorul alineat:

„(2) Până la … [24 de luni de la intrarea în vigoare a prezentului regulament de modificare], Comisia evaluează dacă este necesar să adopte acte de punere în aplicare prin care să stabilească o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru sigiliile electronice avansate. Pe baza rezultatului evaluării respective, Comisia poate adopta astfel de acte de punere în aplicare. În cazul în care un sigiliu electronic avansat îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele privind sigiliile electronice avansate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

37. La articolul 37, alineatul (4) se elimină.

38. La articolul 38, alineatul (6) se înlocuiește cu următorul text:

„(6) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificatele calificate pentru sigiliul electronic. În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele prevăzute în anexa III. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

39. Se introduce următorul articol:

„*Articolul 39a*
Cerințe privind un serviciu calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță

Articolul 29a se aplică *mutatis mutandis* unui serviciu calificat pentru gestionarea dispozitivelor calificate de creare a sigiliului electronic la distanță.”

40. În capitolul III secțiunea 5 se introduce următorul articol:

„*Articolul 40a*
Cerințe pentru validarea sigiliilor electronice avansate bazate pe certificate calificate

Articolul 32a se aplică *mutatis mutandis* validării sigiliilor electronice avansate bazate pe certificate calificate.”

41. La articolul 41, alineatul (3) se elimină.

42. Articolul 42 se modifică după cum urmează:

(a) se introduce următorul alineat:

„(1a) În cazul în care legătura dintre dată și oră și date și exactitatea sursei orei indicate îndeplinesc standardele, specificațiile și procedurile menționate la alineatul (2), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).”;

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru legătura dintre dată și oră și date și pentru stabilirea exactității surselor orei indicate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

43. Articolul 44 se modifică după cum urmează:

(a) se introduce următorul alineat:

„(1a) În cazul în care procesul de trimitere și primire de date îndeplinește standardele, specificațiile și procedurile menționate la alineatul (2), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).”;

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru procesele de trimitere și primire de date. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”;

(c) se introduc următoarele alineate:

„(2a) Prestatorii de servicii de distribuție electronică înregistrată calificate pot conveni asupra interoperabilității dintre serviciile de distribuție electronică înregistrată calificate pe care le prestează. Un astfel de cadru de interoperabilitate respectă cerințele prevăzute la alineatul (1), iar respectarea acestor cerințe este confirmată de un organism de evaluare a conformității.

(2b) Comisia poate stabili, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru cadrul de interoperabilitate menționat la alineatul (2a) de la prezentul articol. Specificațiile tehnice și conținutul standardelor sunt eficiente din punctul de vedere al costurilor și proporționale. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

44. Articolul 45 se înlocuiește cu următorul text:

„*Articolul 45*

Cerințe pentru certificatele calificate pentru autentificarea unui site internet

(1) Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute în anexa IV. Evaluarea conformității cu aceste cerințe se efectuează în conformitate cu standardele, specificațiile și procedurile menționate la alineatul (2) de la prezentul articol.

(1a) Certificatele calificate pentru autentificarea unui site internet emise în conformitate cu alineatul (1) de la prezentul articol sunt recunoscute de furnizorii de browsere web. Furnizorii de browsere web asigură faptul că datele de identitate atestate în certificat și atributele suplimentare atestate sunt afișate într-un mod ușor de recunoscut de către utilizator. Furnizorii de browsere web asigură suport și interoperabilitate cu certificatele calificate pentru autentificarea unui site internet menționate la alineatul (1) de la prezentul articol, cu excepția microîntreprinderilor sau a întreprinderilor mici, astfel cum sunt definite la articolul 2 din anexa la Recomandarea 2003/361/CE, în primii cinci ani de funcționare ca prestatori de servicii de navigare pe internet.

(1b) Certificatele calificate pentru autentificarea unui site internet nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute la alineatul (1).

(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru certificatele calificate pentru autentificarea unui site internet 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 48 alineatul (2).”

45. Se introduce următorul articol:

„*Articolul 45a*
Măsuri de precauție în materie de securitate cibernetică

(1) Furnizorii de browsere web nu iau nicio măsură contrară obligațiilor lor prevăzute la articolul 45, în special cerințelor de recunoaștere a certificatelor calificate pentru autentificarea unui site internet și de afișare a datelor de identitate furnizate într-un mod ușor de recunoscut de către utilizator.

(2) Prin derogare de la alineatul (1) și numai în cazul unor suspiciuni motivate legate de încălcări ale securității sau de pierderea integrității unui certificat identificat sau a unui set de certificate identificate, furnizorii de browsere web pot lua măsuri de precauție în legătură cu respectivul certificat sau set de certificate.

(3) În cazul în care un furnizor de browsere web ia măsuri de precauție conform alineatului (2), furnizorul de browsere web își notifică suspiciunile în scris, fără întârzieri nejustificate, împreună cu o descriere a măsurilor luate pentru a remedia aceste suspiciuni, Comisiei, organismului de supraveghere competent, entității căreia i-a fost emis certificatul și prestatorului de servicii de încredere calificat care a emis certificatul sau setul de certificate. La primirea unei astfel de notificări, organismul de supraveghere competent emite furnizorului de browsere web în cauză o confirmare de primire.

(4) Organismul de supraveghere competent investighează, în conformitate cu articolul 46b alineatul (4) litera (k), aspectele prezentate în notificare. În cazul în care rezultatul investigației respective nu are ca rezultat retragerea statutului de calificat al certificatului, organismul de supraveghere informează furnizorul de browsere web în consecință și îi solicită acestuia să pună capăt măsurilor de precauție menționate la alineatul (2) de la prezentul articol.”

46. În capitolul III se introduc următoarele secțiuni:

„SECȚIUNEA 9
ATESTATUL ELECTRONIC AL ATRIBUTELOR

Articolul 45b
Efectele juridice ale atestatului electronic al atributelor

(1) Unui atestat electronic al atributelor nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele privind atestatele electronice calificate ale atributelor.

(2) Un atestat electronic calificat al atributelor și atestatele atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism au același efect juridic ca atestatele emise în mod legal în format tipărit.

(3) Un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică într-un stat membru sau în numele unui astfel de organism este recunoscut drept un atestat al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism în toate statele membre.

Articolul 45c

Atestatul electronic al atributelor în serviciile publice

Atunci când identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării este obligatorie în temeiul dreptului intern pentru a accesa un serviciu prestat online de un organism din sectorul public, datele de identificare personală din atestatul electronic al atributelor nu înlocuiesc identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării pentru identificarea electronică, cu excepția cazului în care acest lucru este permis în mod expres de statul membru. Într-un astfel de caz, se acceptă, de asemenea, atestatul electronic calificat al atributelor din alte state membre.

Articolul 45d

Cerințe privind atestatul electronic calificat al atributelor

(1) Atestatul electronic calificat al atributelor îndeplinește cerințele prevăzute în anexa V.

(2) Evaluarea conformității cu cerințele prevăzute în anexa V se efectuează în conformitate cu standardele, specificațiile și procedurile menționate la alineatul (5) de la prezentul articol.

(3) Atestatele electronice calificate ale atributelor nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa V.

(4) În cazul în care un atestat electronic calificat al atributelor este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se poate reveni în niciun caz la statutul său anterior.

(5) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind atestatele electronice calificate ale atributelor. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală. Acestea se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 45e

Verificarea atributelor în raport cu surse autentice

(1) În termen de 24 de luni de la data intrării în vigoare a actelor de punere în aplicare menționate la articolul 5a alineatul (23) și la articolul 5c alineatul (6), statele membre se asigură că, cel puțin în cazul atributelor enumerate în anexa VI, ori de câte ori respectivele atribute se bazează pe surse autentice din sectorul public, se iau măsuri pentru a permite prestatorilor de servicii de încredere calificați care pun la dispoziție atestate electronice ale atributelor să verifice respectivele atribute prin mijloace electronice, la cererea utilizatorului, în conformitate cu dreptul Uniunii sau cu dreptul intern.

(2) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], ținând seama de standardele internaționale relevante, Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri pentru catalogul de atribute, precum și sisteme pentru atestarea atributelor și procedurile de verificare pentru atestatele electronice calificate ale atributelor în sensul alineatului (1) de la prezentul articol. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală și se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 45f

Cerințe privind atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism

(1) Un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism îndeplinește următoarele cerințe:

(a) cerințele prevăzute în anexa VII;

(b) cerința ca certificatul calificat care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat al organismului din sectorul public menționat la articolul 3 punctul 46, identificat drept emitentul menționat la litera (b) din anexa VII, să conțină un set specific de atribute certificate într-o formă adecvată pentru prelucrarea automată, care:

(i) indică faptul că organismul emitent este înființat în conformitate cu dreptul Uniunii sau cu dreptul intern ca fiind responsabil de sursa autentică pe baza căreia este emis atestatul electronic al atributelor sau ca organism desemnat să acționeze în numele acestuia;

(ii) furnizează un set de date care reprezintă fără ambiguitate sursa autentică menționată la punctul (i); și

(iii) identifică dreptul Uniunii sau dreptul intern menționat la punctul (i).

(2) Statul membru în care sunt stabilite organismele din sectorul public menționate la articolul 3 punctul 46 se asigură că organismele din sectorul public care emit atestate electronice ale atributelor au un nivel de fiabilitate și încredere echivalent cu cel al prestatorilor de servicii de încredere calificați, în conformitate cu articolul 24.

(3) Statele membre notifică Comisiei organismele din sectorul public menționate la articolul 3 punctul 46. Notificarea respectivă include un raport de evaluare a conformității emis de un organism de evaluare a conformității care confirmă că sunt îndeplinite cerințele prevăzute la alineatele (1), (2) și (6) de la prezentul articol. Comisia pune la dispoziția publicului, printr-un canal sigur, lista organismelor din sectorul public menționate la articolul 3 punctul 46, într-o formă purtând o semnătură electronică sau un sigiliu electronic, adecvată pentru prelucrarea automată.

(4) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este revocat după emiterea inițială, acesta își pierde valabilitatea din momentul revocării și nu se mai poate reveni la statutul anterior revocării.

(5) În cazul în care un atestat electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism îndeplinește standardele, specificațiile și procedurile menționate la alineatul (6), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).

(6) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind atestatul electronic al atributelor emis de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală. Acestea se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(7) Până la … [6 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri în sensul alineatului (3) de la prezentul articol. Actele de punere în aplicare respective sunt în concordanță cu actele de punere în aplicare menționate la articolul 5a alineatul (23) privind implementarea portofelului european pentru identitatea digitală. Acestea se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(8) Organismele din sectorul public menționate la articolul 3 punctul 46 care emit atestate electronice ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu articolul 5a.

Articolul 45g

Emiterea atestatului electronic al atributelor pentru portofelele europene pentru identitatea digitală

(1) Furnizorii de atestate electronice ale atributelor oferă utilizatorilor portofelului european pentru identitatea digitală posibilitatea de a solicita, de a obține, de a stoca și de a gestiona atestatul electronic al atributelor indiferent de statele membre în care este furnizat portofelul european pentru identitatea digitală.

(2) Furnizorii de atestate electronice calificate ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală care sunt furnizate în conformitate cu articolul 5a.

Articolul 45h

Norme suplimentare privind prestarea serviciilor de atestare electronică a atributelor

(1) Prestatorii serviciilor de atestare electronică calificată și necalificată a atributelor nu combină datele cu caracter personal referitoare la prestarea serviciilor respective cu datele cu caracter personal care provin din orice alte servicii oferite de ei sau de partenerii lor comerciali.

(2) Datele cu caracter personal referitoare la prestarea serviciilor de atestare electronică a atributelor sunt păstrate separate logic de alte date deținute de furnizorul atestatului electronic al atributelor.

(3) Prestatorii de servicii de atestare electronică calificată a atributelor pun în aplicare prestarea unor astfel de servicii de încredere calificate într-un mod care este separat din punct de vedere funcțional de alte servicii pe care le prestează.

SECȚIUNEA 10

SERIVICII DE ARHIVARE ELECTRONICĂ

Articolul 45i

Efectul juridic al serviciilor de arhivare electronică

(1) Datelor electronice și documentelor electronice păstrate prin utilizarea unui serviciu de arhivare electronică nu li se refuză efectul juridic sau posibilitatea de a fi acceptate ca probă în procedurile judiciare doar pentru motivul că acestea sunt în format electronic sau că nu sunt păstrate prin utilizarea unui serviciu calificat de arhivare electronică.

(2) Datele electronice și documentele electronice păstrate prin utilizarea unui serviciu calificat de arhivare electronică beneficiază de prezumția de integritate și de acuratețe a originii pe toată durata perioadei de păstrare de către prestatorul de servicii de încredere calificat.

Articolul 45j

Cerințe privind serviciile calificate de arhivare electronică

(1) Serviciile calificate de arhivare electronică îndeplinesc următoarele cerințe:

(a) sunt prestate de prestatori de servicii de încredere calificați;

(b) utilizează proceduri și tehnologii capabile să asigure durabilitatea și lizibilitatea datelor electronice și a documentelor electronice dincolo de perioada de valabilitate tehnologică și cel puțin pe toată perioada de păstrare legală sau contractuală, menținându-le totodată integritatea și acuratețea originii;

(c) garantează că respectivele date electronice și documente electronice sunt păstrate astfel încât să fie protejate împotriva pierderii și modificării, cu excepția modificărilor privind suportul lor sau formatul lor electronic;

(d) permit beneficiarilor autorizați să primească în mod automat un raport care confirmă faptul că datele electronice și documentele electronice extrase dintr-o arhivă electronică calificată beneficiază de prezumția de integritate a datelor de la începutul perioadei de păstrare până în momentul extragerii.

Raportul menționat la litera (d) de la primul paragraf este furnizat într-un mod fiabil și eficient și poartă semnătura electronică calificată sau sigiliul electronic calificat al prestatorului serviciului calificat de arhivare electronică.

(2) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind serviciile calificate de arhivare electronică. În cazul în care un serviciu calificat de arhivare electronică îndeplinește standardele, specificațiile și procedurile respective, se prezumă că sunt respectate cerințele privind serviciile calificate de arhivare electronică. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

SECȚIUNEA 11
REGISTRE ELECTRONICE

Articolul 45k
Efectele juridice ale registrelor electronice

(1) Unui registru electronic nu i se refuză efectul juridic sau posibilitatea de a fi acceptat ca mijloc de probă în procedurile judiciare doar pentru motivul că acesta este în format electronic sau că nu îndeplinește cerințele pentru registrele electronice calificate.

(2) Înregistrările de date cuprinse într-un registru electronic calificat beneficiază de prezumția ordonării lor cronologice secvențiale unice și exacte și de prezumția de integritate.

Articolul 45l
Cerințe privind registrele electronice calificate

(1) Registrele electronice calificate îndeplinesc următoarele cerințe:

(a) sunt create și gestionate de unul sau mai mulți prestatori de servicii de încredere calificați;

(b) stabilesc originea înregistrărilor de date din registru;

(c) asigură ordonarea cronologică secvențială unică a înregistrărilor de date din registru;

(d) înregistrează datele astfel încât orice modificare a lor ulterioară să poată fi detectată imediat, asigurând integritatea datelor în timp.

(2) În cazul în care registrul electronic îndeplinește standardele, specificațiile și procedurile menționate la alineatul (3), se prezumă că sunt respectate cerințele prevăzute la alineatul (1).

(3) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, o listă de standarde de referință și, dacă este necesar, specificații și proceduri privind cerințele prevăzute la alineatul (1) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

47. Se introduce următorul capitol:

„CAPITOLUL IVa
CADRUL DE GUVERNANȚĂ

Articolul 46a
Supravegherea cadrului pentru portofelul european pentru identitatea digitală

(1) Statele membre desemnează unul sau mai multe organisme de supraveghere stabilite pe teritoriul lor.

Organismelor de supraveghere desemnate în temeiul primului paragraf li se conferă competențele necesare și resursele adecvate pentru a-și îndeplini sarcinile în mod eficace, eficient și independent.

(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate în temeiul alineatului (1), precum și orice modificări ulterioare ale acestora. Comisia publică o listă a organismelor de supraveghere notificate.

(3) Rolul organismelor de supraveghere desemnate în temeiul alineatului (1) constă în:

(a) supravegherea furnizorilor de portofele europene pentru identitatea digitală stabiliți pe teritoriul statului membru care a desemnat organismele de supraveghere și asigurarea, prin intermediul unor activități de supraveghere *ex ante* și *ex post*, îndeplinirii de către respectivii furnizori și de către portofelele europene pentru identitatea digitală furnizate de aceștia a cerințelor stabilite în prezentul regulament;

(b) a lua măsuri, dacă este necesar, în ceea ce îi privește pe furnizorii de portofele europene pentru identitatea digitală stabiliți pe teritoriul statului membru care a desemnat organismele de supraveghere, prin intermediul unor activități de supraveghere *ex post*, atunci când sunt informate că furnizorii sau portofelele europene pentru identitatea digitală furnizate de aceștia încalcă prezentul regulament.

(4) Printre sarcinile organismelor de supraveghere desemnate în temeiul alineatului (1) se numără, în special, următoarele:

(a) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolele 46c și 46e;

(b) să solicite informațiile necesare pentru monitorizarea conformității cu prezentul regulament;

(c) să informeze autoritățile competente relevante ale statelor membre în cauză, desemnate sau înființate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, cu privire la orice încălcare semnificativă a securității sau pierdere a integrității de care iau cunoștință în îndeplinirea sarcinilor lor și, în cazul unei încălcări semnificative a securității sau al pierderii integrității care privește alte state membre, să informeze punctul unic de contact din statul membru în cauză, desemnat sau înființat în temeiul articolului 8 alineatul (3) din Directiva (UE) 2022/2555, și punctele unice de contact din celelalte state membre în cauză, desemnate în temeiul articolului 46c alineatul (1) din prezentul regulament, și să informeze publicul sau să solicite furnizorilor de portofele europene pentru identitatea digitală să facă acest lucru în cazul în care organismul de supraveghere consideră că divulgarea încălcării securității sau a pierderii integrității ar fi de interes public*;*

(d) să efectueze inspecții la fața locului și supraveghere *ex situ*;

(e) să solicite furnizorilor de portofele europene pentru identitatea digitală să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament;

(f) să suspende sau să anuleze înregistrarea și includerea beneficiarilor în mecanismul menționat la articolul 5b alineatul (7) în cazul utilizării ilegale sau frauduloase a portofelului european pentru identitatea digitală;

(g) să coopereze cu autoritățile de supraveghere competente înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679, în special prin informarea acestora, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal.

(5) În cazul în care organismul de supraveghere desemnat în temeiul alineatului (1) solicită furnizorului unui portofel european pentru identitatea digitală să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament în temeiul alineatului (4) litera (e), iar furnizorul respectiv nu acționează în consecință și, dacă este cazul, într-un termen stabilit de organismul de supraveghere, organismul de supraveghere desemnat în temeiul alineatului (1) poate, ținând seama, în special, de amploarea, durata și consecințele respectivei neîndepliniri, să dispună ca furnizorul să suspende sau să înceteze furnizarea portofelului european pentru identitatea digitală. Organismul de supraveghere informează fără întârzieri nejustificate organismele de supraveghere ale altor state membre, Comisia, beneficiarii și utilizatorii portofelului european pentru identitatea digitală cu privire la decizia de a solicita suspendarea sau încetarea furnizării portofelului european pentru identitatea digitală.

(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere desemnat în temeiul alineatului (1) prezintă Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior. Comisia pune la dispoziția Parlamentului European și a Consiliului rapoartele anuale respective.

(7) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, formatele și procedurile privind raportul menționat la alineatul (6) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 46b

Supravegherea serviciilor de încredere

(1) Statele membre desemnează un organism de supraveghere înființat pe teritoriul lor sau desemnează, de comun acord cu un alt stat membru, un organism de supraveghere înființat în acel alt stat membru. Organismul de supraveghere respectiv este responsabil de sarcinile de supraveghere în statul membru care l-a desemnat în ceea ce privește serviciile de încredere.

Organismelor de supraveghere desemnate în temeiul primului paragraf li se acordă competențele necesare și resursele adecvate pentru a-și îndeplini sarcinile.

(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate în temeiul alineatului (1), precum și orice modificări ulterioare ale acestora. Comisia publică o listă a organismelor de supraveghere notificate.

(3) Rolul organismelor de supraveghere desemnate în temeiul alineatului (1) constă în:

(a) supravegherea prestatorilor de servicii de încredere calificați stabiliți pe teritoriul statului membru care le-a desemnat și asigurarea, prin intermediul unor activități de supraveghere *ex ante* și *ex post*, îndeplinirii de către respectivii prestatori de servicii de încredere calificați și de către serviciile de încredere calificate prestate de aceștia a cerințelor stabilite în prezentul regulament;

(b) luarea de măsuri, după caz, în legătură cu prestatorii de servicii de încredere necalificați stabiliți pe teritoriul statului membru care le-a desemnat, prin intermediul activităților de supraveghere *ex post*, atunci când sunt informate că respectivii prestatori de servicii de încredere necalificați sau serviciile de încredere prestate de aceștia nu ar îndeplini cerințele stabilite în prezentul regulament.

(4) Printre sarcinile organismelor de supraveghere desemnate în temeiul alineatului (1) se numără, în special, următoarele:

(a) să informeze autoritățile competente relevante ale statelor membre în cauză, desemnate sau înființate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, cu privire la orice încălcare semnificativă a securității sau pierdere a integrității de care iau cunoștință în îndeplinirea sarcinilor lor și, în cazul unei încălcări semnificative a securității sau al pierderii integrității care privește alte state membre, să informeze punctul unic de contact din statul membru în cauză, desemnat sau înființat în temeiul articolului 8 alineatul (3) din Directiva (UE) 2022/2555, și punctele unice de contact din celelalte state membre în cauză, desemnate în temeiul articolului 46c alineatul (1) din prezentul regulament, și să informeze publicul sau să solicite prestatorului de servicii de încredere să facă acest lucru în cazul în care organismul de supraveghere consideră că divulgarea încălcării securității sau a pierderii integrității ar fi de interes public;

(b) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolele 46c și 46e;

(c) să analizeze rapoartele de evaluare a conformității menționate la articolul 20 alineatul (1) și la articolul 21 alineatul (1);

(d) să raporteze Comisiei cu privire la activitățile sale principale, în conformitate cu alineatul (6) de la prezentul articol;

(e) să realizeze audituri sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității prestatorilor de servicii de încredere calificați, în conformitate cu articolul 20 alineatul (2);

(f) să coopereze cu autoritățile de supraveghere competente înființate în temeiul articolului 51 din Regulamentul (UE) 2016/679, în special prin informarea acestora, fără întârzieri nejustificate, în cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, precum și cu privire la încălcările securității care par să constituie încălcări ale securității datelor cu caracter personal;

(g) să acorde statutul de calificat prestatorilor de servicii de încredere, precum și serviciilor pe care aceștia le prestează și să retragă statutul respectiv, în conformitate cu articolele 20 și 21;

(h) să informeze organismul responsabil cu lista sigură națională menționată la articolul 22 alineatul (3) cu privire la deciziile sale de acordare sau de retragere a statutului de calificat, cu excepția cazului în care respectivul organism este și organism de supraveghere desemnat în temeiul alineatului (1) de la prezentul articol;

(i) să verifice existența și aplicarea corectă a dispozițiilor privind planurile de încetare a serviciului atunci când prestatorul de servicii de încredere calificat își încetează activitățile, inclusiv modul în care informațiile sunt păstrate accesibile, în conformitate cu articolul 24 alineatul (2) litera (h);

(j) să solicite prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament;

(k) să investigheze cererile formulate de furnizorii de browsere web în temeiul articolului 45a și să ia măsuri, dacă este necesar.

(5) Statele membre pot să solicite organismului de supraveghere desemnat în temeiul alineatului (1) să stabilească, să mențină și să actualizeze o infrastructură de asigurare a încrederii în conformitate cu dreptul intern.

(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere desemnat în temeiul alineatului (1) prezintă Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior. Comisia pune la dispoziția Parlamentului European și a Consiliului rapoartele anuale respective.

(7) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia adoptă orientări privind îndeplinirea de către organismele de supraveghere desemnate în temeiul alineatului (1) de la prezentul articol a sarcinilor menționate la alineatul (4) de la prezentul articol și, prin intermediul unor acte de punere în aplicare, stabilește formatele și procedurile privind raportul menționat la alineatul (6) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 46c

Puncte unice de contact

(1) Fiecare stat membru desemnează un punct unic de contact pentru serviciile de încredere, portofelele europene pentru identitatea digitală și sistemele de identificare electronică notificate.

(2) Fiecare punct unic de contact exercită o funcție de legătură pentru a facilita cooperarea transfrontalieră între organismele de supraveghere pentru prestatorii de servicii de încredere și între organismele de supraveghere pentru furnizorii de portofele europene pentru identitatea digitală și, după caz, cu Comisia și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și cu alte autorități competente din statul său membru.

(3) Fiecare stat membru publică și, fără întârzieri nejustificate, notifică Comisiei denumirea și adresa punctului unic de contact desemnat în temeiul alineatului (1), precum și orice modificare ulterioară a acestora.

(4) Comisia publică o listă a punctelor unice de contact notificate în temeiul alineatului (3).

Articolul 46d

Asistență reciprocă

(1) Pentru a facilita supravegherea și executarea obligațiilor prevăzute de prezentul regulament, organismele de supraveghere desemnate în temeiul articolului 46a alineatul (1) sau al articolului 46b alineatul (1) pot solicita, inclusiv prin intermediul grupului de cooperare înființat în temeiul articolului 46e alineatul (1), asistență reciprocă din partea organismelor de supraveghere dintr-un alt stat membru în care este stabilit furnizorul portofelului european pentru identitatea digitală sau prestatorul de servicii de încredere sau în care se află rețeaua și sistemele sale informatice ori sunt prestate serviciile acestuia.

(2) Asistența reciprocă implică cel puțin faptul că:

(a) organismul de supraveghere care aplică măsuri de supraveghere și de executare într-un stat membru informează și consultă organismul de supraveghere din celălalt stat membru în cauză;

(b) un organism de supraveghere poate solicita organismului de supraveghere dintr-un alt stat membru în cauză să ia măsuri de supraveghere sau de executare, inclusiv, de exemplu, cereri de a efectua inspecții legate de rapoartele de evaluare a conformității menționate la articolele 20 și 21 în ceea ce privește prestarea de servicii de încredere;

(c) după caz, organismele de supraveghere pot efectua anchete comune cu organismele de supraveghere din alte state membre.

Mecanismele și procedurile pentru acțiunile comune menționate la primul paragraf sunt convenite și stabilite de către statele membre în cauză, în conformitate cu dreptul lor intern.

(3) Un organism de supraveghere căruia i se adresează o solicitare de asistență poate respinge respectiva solicitare pentru oricare dintre următoarele motive:

(a) asistența solicitată nu este proporțională cu activitățile de supraveghere ale organismului de supraveghere desfășurate în conformitate cu articolele 46a și 46b;

(b) organismul de supraveghere nu are competența de a acorda asistența solicitată;

(c) acordarea asistenței solicitate ar contraveni prezentului regulament.

(4) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare] și, ulterior, la fiecare doi ani, grupul de cooperare înființat în temeiul articolului 46e alineatul (1) emite orientări privind aspectele organizatorice și procedurile pentru asistența reciprocă menționată la alineatele (1) și (2) de la prezentul articol.

Articolul 46e

Grupul european de cooperare privind identitatea digitală

(1) Pentru a sprijini și a facilita cooperarea transfrontalieră și schimbul de informații dintre statele membre privind serviciile de încredere, portofelele europene pentru identitatea digitală și sistemele de identificare electronică notificate, Comisia înființează un Grup european de cooperare privind identitatea digitală (denumit în continuare «grupul de cooperare»).

(2) Grupul de cooperare este alcătuit din reprezentanți numiți de statele membre și de Comisie. Grupul de cooperare este prezidat de Comisie. Comisia asigură secretariatul grupului de cooperare.

(3) Reprezentanții părților interesate relevante pot fi invitați ad-hoc să participe la reuniunile grupului de cooperare și la lucrările acestuia în calitate de observatori.

(4) ENISA este invitată să participe în calitate de observator la lucrările grupului de cooperare atunci când are loc un schimb de opinii, de bune practici și de informații cu privire la aspecte relevante în materie de securitate cibernetică, cum ar fi notificarea încălcărilor securității, și atunci când se abordează utilizarea certificatelor sau a standardelor de securitate cibernetică.

(5) Grupului de cooperare îi revin următoarele sarcini:

(a) să facă schimb de opinii și să coopereze cu Comisia cu privire la inițiativele de politică emergente în domeniul portofelelor pentru identitatea digitală, al mijloacelor de identificare electronică și al serviciilor de încredere;

(b) să consilieze Comisia, după caz, în fazele inițiale de pregătire a proiectelor de acte de punere în aplicare și de acte delegate care urmează să fie adoptate în temeiul prezentului regulament;

(c) pentru a sprijini organismele de supraveghere la punerea în aplicare a dispozițiilor prezentului regulament:

(i) să facă schimb de bune practici și de informații privind punerea în aplicare a dispozițiilor prezentului regulament;

(ii) să evalueze evoluțiile pertinente din sectorul portofelului pentru identitatea digitală, al identificării electronice și al serviciilor de încredere;

(iii) să organizeze reuniuni comune cu părțile interesate relevante din întreaga Uniune pentru a discuta activitățile desfășurate de grupul de cooperare și pentru a colecta informații cu privire la dificultățile emergente în materie de politici;

(iv) cu sprijinul ENISA, să facă schimb de opinii, de bune practici și de informații cu privire la aspectele relevante în materie de securitate cibernetică în ceea ce privește portofelele europene pentru identitatea digitală, sistemele de identificare electronică și serviciile de încredere;

(v) să facă schimb de bune practici cu privire la elaborarea și punerea în aplicare a politicilor privind notificarea încălcărilor securității și măsurile comune menționate la articolele 5e și 10;

(vi) să organizeze reuniuni comune cu Grupul de cooperare NIS înființat în temeiul articolului 14 alineatul (1) din Directiva (UE) 2022/2555 pentru a face schimb de informații relevante în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, capacitățile în materie de standarde și specificații tehnice, precum și standardele și specificațiile tehnice în legătură cu serviciile de încredere și identificarea electronică;

(vii) să discute, la cererea unui organism de supraveghere, cererile specifice de asistență reciprocă menționate la articolul 46d;

(viii) să faciliteze schimbul de informații între organismele de supraveghere prin furnizarea de orientări cu privire la aspectele organizatorice și procedurile de asistență reciprocă menționate la articolul 46d;

(d) să organizeze evaluări *inter pares* ale sistemelor de identificare electronică ce trebuie notificate în temeiul prezentului regulament.

(6) Statele membre asigură cooperarea eficace și eficientă a reprezentanților lor desemnați în grupul de cooperare.

(7) Până la … [12 luni de la data intrării în vigoare a prezentului regulament de modificare], Comisia stabilește, prin intermediul unor acte de punere în aplicare, modalitățile procedurale necesare pentru facilitarea cooperării dintre statele membre menționate la alineatul (5) litera (d) de la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

48. Articolul 47 se modifică după cum urmează:

(a) alineatele (2) și (3) se înlocuiesc cu următorul text:

„(2) Competența de a adopta acte delegate menționată la articolul 5c alineatul (7), la articolul 24 alineatul (4b) și la articolul 30 alineatul (4) se conferă Comisiei pe o perioadă nedeterminată de la 17 septembrie 2014.

(3) Delegarea de competențe menționată la articolul 5c alineatul (7), la articolul 24 alineatul (4b) și la articolul 30 alineatul (4) 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.”;

(b) alineatul (5) se înlocuiește cu următorul text:

„(5) Un act delegat adoptat în temeiul articolului 5c alineatul (7), al articolului 24 alineatul (4b) sau al articolului 30 alineatul (4) 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.”

49. În capitolul VI se introduce următorul articol:

„*Articolul 48a*
Cerințe de raportare

(1) Statele membre asigură colectarea de date statistice în legătură cu funcționarea portofelelor europene pentru identitatea digitală și a serviciilor de încredere calificate furnizate pe teritoriile lor.

(2) Datele statistice colectate în conformitate cu alineatul (1) includ următoarele:

(a) numărul persoanelor fizice și juridice care dețin un portofel european pentru identitatea digitală valabil;

(b) tipul și numărul serviciilor care acceptă utilizarea portofelului european pentru identitatea digitală;

(c) numărul reclamațiilor din partea utilizatorilor și al incidentelor privind protecția consumatorilor sau protecția datelor în legătură cu beneficiarii și serviciile de încredere calificate;

(d) un raport de sinteză care include date privind incidentele care împiedică utilizarea portofelului european pentru identitatea digitală;

(e) un rezumat al incidentelor semnificative de securitate, al încălcărilor securității datelor și al utilizatorilor afectați ai portofelelor europene pentru identitatea digitală sau ai serviciilor de încredere calificate.

(3) Datele statistice menționate la alineatul (2) sunt puse la dispoziția publicului într-un format deschis, utilizat în mod obișnuit și prelucrabil automat.

(4) Până la data de 31 martie a fiecărui an, statele membre transmit Comisiei un raport privind datele statistice colectate în conformitate cu alineatul (2).”

50. Articolul 49 se înlocuiește cu următorul text:

„*Articolul 49*
Reexaminare

(1) Comisia reexaminează modul de aplicare a prezentului regulament și, până la …[24 de luni de la data intrării în vigoare a regulamentului de modificare], prezintă un raport în acest sens Parlamentului European și Consiliului. În respectivul raport, Comisia evaluează, în special, dacă este oportun să se modifice domeniul de aplicare al prezentului regulament sau dispozițiile sale specifice, inclusiv, în special, dispozițiile articolului 5c alineatul (5), ținând seama de experiența dobândită în aplicarea prezentului regulament, precum și de evoluțiile tehnologice, ale pieței și juridice. Dacă este necesar, raportul respectiv este însoțit de o propunere de modificare a prezentului regulament.

(2) Raportul menționat la alineatul (1) include o analiză a disponibilității, a securității și a posibilității de utilizare a mijloacelor de identificare electronică notificate și a portofelelor europene pentru identitatea digitală care intră în domeniul de aplicare al prezentului regulament și analizează dacă tuturor prestatorilor privați de servicii online care recurg la servicii de identificare electronică furnizate de terți pentru autentificarea utilizatorilor trebuie să le revină obligația să accepte utilizarea mijloacelor de identificare electronică notificate și a portofelului european pentru identitatea digitală.

(3) Până la … [șase ani de la data intrării în vigoare a prezentului regulament de modificare] și, ulterior, la fiecare patru ani, Comisia prezintă un raport Parlamentului European și Consiliului cu privire la progresele realizate în vederea atingerii obiectivelor prezentului regulament.”

51. Articolul 51 se înlocuiește cu următorul text:

„*Articolul 51*
Măsuri tranzitorii

(1) Dispozitivele sigure de creare a semnăturilor a căror conformitate a fost stabilită în conformitate cu articolul 3 alineatul (4) din Directiva 1999/93/CE sunt considerate în continuare dispozitive de creare a semnăturilor electronice calificate în temeiul prezentului regulament până la … [36 de luni de la data intrării în vigoare a prezentului regulament de modificare].

(2) Certificatele calificate emise persoanelor fizice în temeiul Directivei 1999/93/CE sunt considerate în continuare certificate calificate pentru semnături electronice în temeiul prezentului regulament până la … [24 de luni de la data intrării în vigoare a prezentului regulament de modificare].

(3) Până la … [24 de luni de la data intrării în vigoare a prezentului regulament de modificare], gestionarea dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice la distanță de către alți prestatori de servicii de încredere calificați decât cei care prestează servicii de încredere calificate pentru gestionarea dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice la distanță în conformitate cu articolele 29a și 39a, se poate desfășura fără să fie necesară obținerea statutului de calificat pentru prestarea acestor servicii de gestionare.

(4) Prestatorii de servicii de încredere calificați cărora li s-a acordat statutul de calificat în temeiul prezentului regulament înainte de … [data intrării în vigoare a prezentului regulament de modificare] prezintă organismului de supraveghere un raport de evaluare a conformității care dovedește conformitatea cu articolul 24 alineatele (1), (1a) și (1b) cât mai curând posibil și în orice caz până la … [24 de luni de la data intrării în vigoare a prezentului regulament de modificare].”

52. Anexele I-IV se modifică în conformitate cu anexele I-IV la prezentul regulament.

53. Se adaugă noile anexe V, VI și VII astfel cum figurează în anexele V, VI și VII la prezentul regulament.

Articolul 2

Intrarea 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,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

ANEXA I

În anexa I la Regulamentul (UE) nr. 910/2014, litera (i) se înlocuiește cu următorul text:

„(i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii;”.

ANEXA II

În anexa II la Regulamentul (UE) nr. 910/2014, se elimină punctele 3 și 4.

ANEXA III

În anexa III la Regulamentul (UE) nr. 910/2014, litera (i) se înlocuiește cu următorul text:

„(i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii;”.

ANEXA IV

Anexa IV la Regulamentul (UE) nr. 910/2014 se modifică după cum urmează:

1. Litera (c) se înlocuiește cu următorul text:

„(c) în cazul persoanelor fizice: cel puțin numele persoanei căreia i s-a emis certificatul sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

(ca) în cazul persoanelor juridice: un set unic de date care reprezintă fără echivoc persoana juridică căreia i se emite certificatul, incluzând cel puțin denumirea persoanei juridice căreia i se emite certificatul și, după caz, numărul de înregistrare astfel cum este menționat în registrele oficiale;”.

2. Litera (j) se înlocuiește cu următorul text:

„(j) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.”

ANEXA V

„ANEXA V

CERINȚE PRIVIND

ATESTATUL ELECTRONIC CALIFICAT AL ATRIBUTELOR

Atestatul electronic calificat al atributelor conține:

(a) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic calificat al atributelor;

(b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite atestatul electronic calificat al atributelor, incluzând cel puțin statul membru în care este stabilit prestatorul respectiv și:

(i) în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum figurează în registrele oficiale,

(ii) în cazul unei persoane fizice: numele persoanei;

(c) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

(d) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru a identifica domeniul de aplicare al atributelor respective;

(e) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului;

(f) codul de identificare al atestatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat și, în cazurile aplicabile, indicarea sistemului de atestare din care face parte atestatul atributelor;

(g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent;

(h) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la litera (g);

(i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.”

ANEXA VI

„ANEXA VI

LISTA MINIMĂ A ATRIBUTELOR

În temeiul articolului 45e, statele membre se asigură că sunt adoptate măsuri pentru a le permite prestatorilor de servicii de încredere calificați care pun la dispoziție atestate electronice ale atributelor să verifice prin mijloace electronice, la cererea utilizatorului, autenticitatea următoarelor atribute prin raportare la sursa autentică relevantă la nivel național sau prin intermediul unor intermediari desemnați recunoscuți la nivel național, în conformitate cu dreptul Uniunii sau cu dreptul intern și în cazurile în care aceste atribute se bazează pe surse autentice din cadrul sectorului public:

1. adresa;

2. vârsta;

3. genul;

4. starea civilă;

5. componența familiei;

6. naționalitatea sau cetățenia;

7. nivelul de studii, titluri și diplome;

8. calificări profesionale, titluri și licențe;

9. împuterniciri și mandate de reprezentare a persoanelor fizice sau juridice;

10. autorizații publice și licențe;

11. pentru persoanele juridice, datele financiare și datele privind societățile.”

ANEXA VII

„ANEXA VII

CERINȚE PRIVIND ATESTATUL ELECTRONIC AL ATRIBUTELOR
EMIS DE UN ORGANISM PUBLIC RESPONSABIL DE O SURSĂ AUTENTICĂ
SAU ÎN NUMELE UNUI ASTFEL DE ORGANISM

Un atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism conține:

(a) o indicație, cel puțin într-un format adecvat pentru prelucrarea automată, a faptului că atestatul a fost emis ca atestat electronic al atributelor emis de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism;

(b) un set de date care reprezintă fără echivoc organismul public care emite atestatul electronic al atributelor, incluzând cel puțin statul membru în care este stabilit organismul public respectiv și denumirea sa și, după caz, numărul său de înregistrare, astfel cum figurează în registrele oficiale;

(c) un set de date care reprezintă fără echivoc entitatea la care se referă atributele atestate; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

(d) atributul atestat sau atributele atestate, inclusiv, în cazurile aplicabile, informațiile necesare pentru a identifica domeniul de aplicare al atributelor respective;

(e) detalii privind începutul și sfârșitul perioadei de valabilitate a atestatului;

(f) codul de identificare al atestatului, care trebuie să fie unic pentru organismul public emitent și, în cazurile aplicabile, o indicare a sistemului de atestare din care face parte atestatul atributelor;

(g) semnătura electronică calificată sau sigiliul electronic calificat al organismului emitent;

(h) locul în care este disponibil gratuit certificatul care stă la baza semnăturii electronice calificate sau a sigiliului electronic calificat menționate la litera (g);

(i) informațiile privind serviciile care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat sau localizarea acestor servicii.”