Consiliul
Uniunii Europene

Bruxelles, 6 decembrie 2022
(OR. en)

15706/22

Dosar interinstituțional:
2021/0136(COD)

TELECOM 519
COMPET 1006
MI 919
DATAPROTECT 352
JAI 1634
CODEC 1941

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	6 decembrie 2022
Destinatar:	Delegațiile
Nr. doc. ant.:	14959/22 + ADD 1 + ADD 2
Nr. doc. Csie:	9471/21
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană - Abordare generală (6 decembrie 2022)

În anexă, se pune la dispoziția delegațiilor abordarea generală a Consiliului cu privire la propunerea sus-menționată, astfel cum a fost aprobată de Consiliu (Transporturi, Telecomunicații și Energie) în cadrul celei de a 3917-a reuniuni a sale, care a avut loc la 6 decembrie 2022.

Abordarea generală stabilește poziția provizorie a Consiliului cu privire la această propunere și constituie baza pregătirilor pentru negocierile cu Parlamentul European.

ANEXĂ

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană

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],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Comunicarea Comisiei din 19 februarie 2020 intitulată „Conturarea viitorului digital al Europei”[2] anunță o revizuire a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului cu scopul de a-i îmbunătăți eficacitatea, de a extinde beneficiile acestuia pentru sectorul privat și de a promova identitățile digitale de încredere pentru toți europenii.

[1] JO C , , p. .
[2] COM(2020) 67 final.

(2) În concluziile sale din 1-2 octombrie 2020[3], Consiliul European a invitat Comisia să propună elaborarea unui cadru la nivelul întregii UE pentru identificarea electronică publică securizată, inclusiv pentru semnăturile digitale interoperabile, cu scopul de a le oferi oamenilor controlul asupra identității și datelor lor online, precum și de a le permite accesul la servicii digitale publice, private și transfrontaliere.

(3) Comunicarea Comisiei din 9 martie 2021 intitulată „Busola pentru dimensiunea digitală 2030: modelul european pentru deceniul digital”[4] stabilește obiectivul unui cadru al Uniunii care, până în 2030, conduce la implementarea pe scară largă a unei identități de încredere, controlată de utilizator, care să permită fiecărui cetățean să aibă controlul asupra propriilor interacțiuni și asupra prezenței sale în mediul online.

(4) O abordare mai armonizată a identificării electronice ar trebui să reducă riscurile și costurile fragmentării actuale cauzate de utilizarea unor soluții naționale divergente și va consolida piața unică permițând cetățenilor, altor rezidenți, astfel cum sunt definiți în dreptul intern, și întreprinderilor să se identifice online într-un mod convenabil și uniform în întreaga Uniune. Portofelul european pentru identitatea digitală va oferi persoanelor fizice și juridice din întreaga Uniune un mijloc armonizat de identificare electronică care le va permite să se autentifice și să partajeze date legate de identitatea lor. Orice persoană ar trebui să poată avea acces în condiții de siguranță la serviciile publice și private, bazându-se pe un ecosistem îmbunătățit pentru serviciile de încredere și pe dovezi verificate ale identității și pe atestări ale atributelor, cum ar fi o diplomă universitară recunoscută în mod legal și acceptată oriunde în Uniune. Cadrul pentru o identitate digitală europeană vizează realizarea unei tranziții de la utilizarea în mod exclusiv a soluțiilor naționale de identitate digitală la furnizarea de atestări electronice ale atributelor valabile la nivel european. Furnizorii de atestări electronice ale atributelor ar trebui să beneficieze de un set de norme clar și uniform, iar administrațiile publice ar trebui să se poată baza pe documente electronice într-un anumit format.

---

[3] https://www.consilium.europa.eu/ro/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

[4] COM(2021) 118 final/2.

(4a) Mai multe state membre au dezvoltat și utilizează pe scară largă mijloace de identificare electronică care sunt acceptate în prezent de prestatorii de servicii din Uniune. În plus, au fost realizate investiții atât în soluții la nivel național, cât și în soluții transfrontaliere bazate pe actualul Regulament eIDAS, inclusiv în infrastructura tehnică de interoperabilitate a nodurilor eIDAS. Pentru a garanta 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 minimum impactul asupra prestatorilor de servicii existenți, se preconizează că portofelele europene pentru identitatea digitală vor beneficia de pe urma fructificării experienței dobândite cu mijloacele de identificare electronică existente și de pe urma utilizării infrastructurii eIDAS instalate la nivel european și național.

(5) Pentru a sprijini competitivitatea întreprinderilor europene, prestatorii de servicii online ar trebui să se poată baza pe soluții de identitate digitală recunoscute în întreaga Uniune, indiferent de statul membru în care au fost puse la dispoziție, beneficiind 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 aceeași valoare juridică conferită atestărilor electronice ale atributelor în întreaga Uniune.

(6) Regulamentul (UE) 2016/679[5] 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 care provin din alte servicii cu datele cu caracter personal referitoare la 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 să se păstreze separate logic de orice alte date deținute de emitent. Prezentul regulament nu îi împiedică pe emitenții portofelelor 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 punerea la dispoziție a portofelelor de orice alte date deținute de emitent.

---

[5] 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.

(7) Se impune stabilirea unor condiții armonizate pentru instituirea unui cadru corespunzător portofelelor europene pentru identitatea digitală care urmează a fi puse la dispoziție de statele membre, ceea ce ar trebui să permită tuturor cetățenilor Uniunii și altor rezidenți, astfel cum sunt definiți în dreptul intern, să partajeze în condiții de siguranță date privind identitatea lor, într-un mod ușor de utilizat și convenabil, exclusiv sub controlul utilizatorului. Tehnologiile utilizate pentru atingerea acestor obiective ar trebui dezvoltate cu scopul de a atinge cel mai înalt nivel de securitate, de confidențialitate, de confort pentru utilizatori și de utilizare pe scară largă. Statele membre ar trebui să asigure accesul egal la identificarea electronică pentru toți resortisanții și rezidenții lor.

(8) Pentru a se asigura că beneficiarii se pot baza cu încredere pe utilizarea portofelelor europene pentru identitatea digitală și pentru a proteja utilizatorul împotriva utilizării ilegale a datelor cu caracter sensibil, beneficiarii ar trebui să fie înregistrați, ca parte a unui proces de notificare. Cerințele de notificare impuse beneficiarilor ar trebui, în majoritatea cazurilor, să se bazeze pe furnizarea unui volum limitat de informații necesare pentru autentificarea beneficiarului în raport cu portofelul european pentru identitatea digitală. Cerințele ar trebui să permită, de asemenea, utilizarea de proceduri automatizate sau simple de autoraportare, inclusiv bazarea pe și utilizarea registrelor existente de către statele membre. În același timp, pentru categoriile de date cu caracter sensibil, pot exista regimuri specifice la nivel național sau la nivelul Uniunii, care pot impune beneficiarilor cerințe de înregistrare și de autorizare mai stricte pentru a preveni utilizarea ilegală a datelor de identitate în astfel de cazuri. În alte cazuri de utilizare, beneficiarii pot fi scutiți de obligația de a-și notifica intenția de a se baza pe portofelul digital european, de exemplu, atunci când dreptul de a verifica atribute specifice nu necesită sau nu permite autentificarea beneficiarului prin mijloace electronice. De regulă, în aceste scenarii care necesită prezență fizică, utilizatorul este în măsură să identifice beneficiarul datorită contextului, cum ar fi atunci când interacționează cu un angajat al unei firme de închirieri de mașini sau cu un farmacist. Se preconizează ca procesul de notificare să fie stabilit de legislația sectorială a Uniunii sau de legislația națională, deoarece acest lucru permite adaptarea la cazuri de utilizare variate, care pot fi diferite în ceea ce privește cerințele de înregistrare, modul de operare (online/offline) sau cerința de autentificare a dispozitivelor capabile să interacționeze cu portofelul european pentru identitatea digitală. La nivelul portofelului european pentru identitatea digitală nu ar trebui impusă executarea verificării utilizării portofelului european pentru identitatea digitală de către beneficiari.

(9) 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 resortisanților și rezidenților lor, portofelele pot răspunde și nevoilor instituționale ale administrațiilor publice, ale organizațiilor internaționale și ale instituțiilor, organelor, oficiilor și agențiilor Uniunii. Utilizarea offline ar avea un caracter important în numeroase sectoare, inclusiv în sectorul sănătății, unde serviciile sunt adesea furnizate prin interacțiune directă, iar prescripțiile electronice ar trebui să se poată baza pe coduri QR sau pe tehnologii similare pentru verificarea autenticității. Bazându-se pe nivelul de asigurare „ridicat”, portofelele europene pentru identitatea digitală ar trebui să beneficieze 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 UE. Pentru a obține beneficii în materie de simplificare și de reducere a costurilor pentru persoanele și întreprinderile din întreaga UE, inclusiv prin validarea competențelor de reprezentare și a mandatelor electronice, statele membre ar trebui să emită portofele europene pentru identitatea digitală care să se bazeze pe standarde comune pentru a asigura interoperabilitatea neîntreruptă și un nivel ridicat de securitate. Numai autoritățile competente ale statelor membre pot oferi un grad 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, este necesar ca portofelele europene pentru identitatea digitală să se bazeze pe identitatea juridică a cetățenilor, a altor rezidenți sau a entităților juridice. Încrederea în portofelele europene pentru identitatea digitală ar fi consolidată prin faptul că părților emitente li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate proporțional cu riscurile la adresa drepturilor și libertăților persoanelor fizice, în conformitate cu Regulamentul (UE) 2016/679. Emiterea, utilizarea pentru autentificare și revocarea portofelelor europene pentru identitatea digitală sunt gratuite pentru persoanele fizice. Serviciile care se bazează pe utilizarea portofelului pot genera costuri legate, de exemplu, de emiterea atestărilor electronice ale atributelor și înregistrarea lor în portofel.

(9a) 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, statele membre pot prevedea măsuri juridice și organizatorice pentru a spori flexibilitatea pentru emitenții de portofele europene pentru identitatea digitală și pentru a permite funcționalități suplimentare ale portofelelor europene pentru identitatea digitală dincolo de ceea ce este prevăzut în prezentul regulament, inclusiv printr-o interoperabilitate sporită cu mijloacele naționale de identificare electronică existente. Acest lucru nu ar trebui în niciun caz să fie în detrimentul asigurării funcțiilor de bază ale portofelelor europene pentru identitatea digitală, astfel cum se prevede în prezentul regulament, și nici să promoveze soluțiile naționale existente în detrimentul portofelelor europene pentru identitatea digitală. Întrucât depășesc limitele prezentului regulament, aceste funcționalități suplimentare nu intră sub incidența dispozițiilor privind utilizarea transfrontalieră a portofelelor europene pentru identitatea digitală prevăzute în prezentul regulament.

(10) Pentru a atinge un nivel ridicat de protecție a datelor, de securitate și de fiabilitate, prezentul regulament ar trebui să stabilească un cadru armonizat care să detalieze specificațiile și cerințele comune aplicabile portofelelor europene pentru identitatea 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. Certificarea ar trebui să se bazeze în special pe sistemele europene de certificare a securității cibernetice relevante sau pe părți ale acestora, instituite în temeiul Regulamentului (UE) 2019/881[6], în măsura în care acestea acoperă cerințele de securitate cibernetică aplicabile portofelelor europene pentru identitatea digitală. Recurgerea la sistemele europene de certificare a securității cibernetice ar trebui să asigure un nivel armonizat de încredere în securitatea portofelelor europene pentru identitatea digitală, indiferent de locul în care sunt emise în întreaga Uniune. Certificarea securității cibernetice a portofelelor europene pentru identitatea digitală ar trebui să se sprijine pe rolul autorităților naționale de certificare a securității cibernetice de a supraveghea și a monitoriza conformitatea certificatelor emise de organismele de evaluare a conformității din jurisdicția lor cu sistemele europene de certificare a securității cibernetice relevante. În mod similar, certificarea ar trebui să se bazeze, după caz, pe standarde și specificații tehnice, astfel cum se precizează în Regulamentul (UE) 2019/881. Astfel de specificații pot fi utilizate ca documente care reflectă stadiul actual al tehnologiei, astfel cum se specifică în cadrul sistemelor relevante de certificare a securității cibernetice în temeiul Regulamentului (UE) 2019/881. În cazul în care niciun sistem european de certificare a securității cibernetice relevant instituit în temeiul Regulamentului (UE) 2019/881 nu acoperă certificarea serviciilor sau proceselor relevante care contribuie la securitatea portofelului, ar trebui create sisteme adecvate în conformitate cu titlul III din Regulamentul (UE) 2019/881. Ar trebui instituit un sistem comun și armonizat de certificare a portofelelor europene pentru identitatea digitală în vederea evaluării conformității acestora cu specificațiile și cerințele comune prevăzute în prezentul regulament, altele decât cele legate de securitatea cibernetică și de protecția datelor, în special cu cele care vizează aspecte funcționale și operaționale. În ceea ce privește această certificare, pentru a asigura un nivel ridicat de încredere și transparență, ar trebui instituite mecanisme și proceduri menite să încurajeze învățarea reciprocă și cooperarea între statele membre în ceea ce privește monitorizarea și reevaluarea organismelor de certificare, precum și a certificatelor și a rapoartelor de certificare pe care acestea le eliberează. Un astfel de mecanism de învățare reciprocă nu ar trebui să aducă atingere Regulamentului (CE) 2016/679 și Regulamentului (UE) 2019/881. Certificarea portofelului în temeiul Regulamentului (CE) 2016/679 este un instrument opțional printre altele, care poate fi utilizat pentru a demonstra conformitatea cu cerințele prevăzute în Regulamentul (CE) 2016/679, astfel cum se aplică acestea portofelelor europene pentru identitatea digitală și punerii acestora la dispoziția cetățenilor europeni.

---

[6] 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.

(10a) Integrarea cetățenilor și a rezidenților în sistemul reprezentat de portofelul european pentru identitatea digitală ar trebui 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 cazurile în care specificații tehnice și operaționale 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 sau măsuri suplimentare ar trebui să fie fiabile și ușor de utilizat de către utilizatori și s-ar putea baza pe posibilitatea de a utiliza proceduri de integrare de la distanță, certificate calificate susținute de semnături calificate, atestarea electronică calificată a atributelor sau o combinație a acestora. Pentru a asigura adoptarea într-o măsură suficientă a portofelelor europene pentru identitatea digitală, ar trebui stabilite, prin acte de punere în aplicare, specificații tehnice și operaționale armonizate pentru integrarea utilizatorilor prin utilizarea mijloacelor de identificare electronică, inclusiv a celor emise cu un nivel de asigurare „substanțial”.

(10b) 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 se pot baza pe elemente de securitate certificate externe pentru protecția materialului criptografic și a altor date cu caracter sensibil sau pe soluții naționale notificate cu un nivel de asigurare „ridicat” pentru a demonstra conformitatea cu cerințele relevante ale regulamentului în ceea ce privește nivelul de asigurare al portofelului. Utilizarea măsurii tranzitorii menționate anterior ar trebui să se limiteze la cazurile de utilizare care necesită un nivel de asigurare „ridicat”, cum ar fi integrarea utilizatorului în sistemul reprezentat de portofel și autentificarea pentru servicii care necesită un nivel de asigurare „ridicat”. Atunci când efectuează un proces de autentificare pentru servicii care necesită un nivel de asigurare „substanțial”, portofelele europene pentru identitatea digitală nu ar trebui să necesite utilizarea măsurii tranzitorii menționate mai sus. Prezentul regulament nu ar trebui să aducă atingere condițiilor naționale pentru emiterea și utilizarea elementului de securitate certificat extern în cazul în care această măsură tranzitorie se bazează pe acesta.

(11) Portofelele europene pentru identitatea digitală ar trebui să asigure cel mai înalt nivel de protecție și de securitate pentru datele cu caracter personal utilizate în scopul autentificării, indiferent dacă aceste date sunt stocate la nivel local sau prin soluții de tip cloud, luând în considerare diferitele niveluri de risc. Prelucrarea datelor biometrice ca factor de autentificare specific unei autentificări stricte a utilizatorului este una dintre metodele de identificare ce conferă un nivel ridicat de încredere, în special atunci când este utilizată în combinație cu alte elemente de autentificare. Întrucât datele biometrice reprezintă o caracteristică unică a unei persoane, prelucrarea datelor biometrice este permisă numai în temeiul excepțiilor de la articolul 9 alineatul (2) din Regulamentul (UE) 2016/679 și necesită garanții adecvate, proporționale cu riscul pe care o astfel de prelucrare îl poate implica pentru drepturile și libertățile persoanelor fizice.

(11a) Funcționarea portofelelor europene pentru identitatea digitală ar trebui să fie transparentă și să permită prelucrarea verificabilă a datelor cu caracter personal. Pentru a realiza acest lucru, statele membre sunt încurajate să divulge codul sursă al componentelor software ale portofelelor europene pentru identitatea digitală care au legătură cu prelucrarea datelor cu caracter personal și a datelor persoanelor juridice. Divulgarea unui astfel de cod sursă permite societății, inclusiv utilizatorilor și dezvoltatorilor, să înțeleagă funcționarea acestuia. Acest lucru are, de asemenea, potențialul de a spori încrederea utilizatorilor în ecosistemul portofelelor și de a contribui la securitatea portofelelor, permițând oricărei persoane să raporteze vulnerabilități și erori identificate în cod. Acest lucru îi motivează pe furnizori să livreze și să întrețină un produs foarte sigur. În plus și după caz, statele membre sunt, de asemenea, încurajate să pună la dispoziție codul sursă în baza unei licențe cu sursă deschisă. O licență cu sursă deschisă permite societății, inclusiv utilizatorilor și dezvoltatorilor, să modifice și să reutilizeze codul sursă.

(12) Pentru a se asigura faptul că, în ceea ce privește cadrul european al identității digitale, acesta este deschis inovării, dezvoltării tehnologice și este adaptat exigențelor viitorului, statele membre ar trebui încurajate să creeze 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. Acest mediu ar trebui să încurajeze includerea întreprinderilor mici și mijlocii, a întreprinderilor nou-înființate, a inovatorilor și a cercetătorilor individuali la nivel european.

(13) Regulamentul (UE) 2019/1157[7] prevede consolidarea securității cărților de identitate cu elemente de securitate sporită până în august 2021. Statele membre ar trebui să aibă în vedere fezabilitatea notificării acestora în cadrul sistemelor de identificare electronică în scopul extinderii disponibilității transfrontaliere a mijloacelor de identificare electronică.

(14) Procesul de notificare a sistemelor de identificare electronică ar trebui simplificat și accelerat pentru a promova accesul la soluții de autentificare și identificare convenabile, 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.

(15) 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, ar trebui să încurajeze cooperarea dintre statele membre în ceea ce privește securitatea și interoperabilitatea sistemelor de identificare electronică notificate ale acestora.

(16) 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. 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 cadrul sistemelor de certificare ce urmează a fi instituite la nivelul Uniunii în temeiul Regulamentului (UE) 2019/881, pentru a le susține cererile privind alinierea sistemelor sau a unor părți ale acestora la cerințele Regulamentului privind interoperabilitatea și securitatea sistemelor de identificare electronică notificate.

---

[7] 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.

(17a) Utilizarea identificatorilor unici și permanenți emiși de statele membre sau generați de portofelul european pentru identitatea digitală, împreună cu utilizarea datelor de identificare personală sunt esențiale pentru a se asigura că identitatea utilizatorului poate fi verificată, în special în sectorul public și atunci când acest lucru este impus de dreptul intern sau de dreptul Uniunii. Prezentul regulament ar trebui să asigure faptul că portofelul european pentru identitatea digitală poate oferi un mecanism care să permită corelarea înregistrărilor, inclusiv prin utilizarea atestărilor electronice calificate ale atributelor, precum și includerea unor identificatori unici și permanenți în setul de date de identificare a persoanelor. Un identificator unic și permanent poate consta fie în date de identificare unice, fie în date de identificare multiple care pot fi specifice sectorului, atât timp cât servesc la identificarea unică a utilizatorului în întreaga Uniune. Portofelul european pentru identitatea digitală ar trebui, de asemenea, să ofere un mecanism care să permită utilizarea unor identificatori specifici beneficiarilor în cazurile în care dreptul național sau dreptul Uniunii impune utilizarea unui identificator unic și permanent. În toate cazurile, mecanismul pus la dispoziție pentru a facilita corelarea înregistrărilor și utilizarea unor identificatori unici și permanenți ar trebui să asigure faptul că utilizatorul este protejat împotriva utilizării abuzive a datelor cu caracter personal în conformitate cu prezentul regulament și cu dreptul aplicabil al Uniunii, în special cu Regulamentul (UE) 2016/679, inclusiv împotriva riscului de creare de profiluri și de urmărire legate de utilizarea portofelului european pentru identitatea digitală.

(17aa) Este esențial să se țină seama de nevoile utilizatorilor, stimulând astfel cererea de portofele europene pentru identitatea digitală. Ar trebui să existe 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 se întreprindă 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, dezvoltare și implementare a serviciilor online care se bazează pe portofelele europene pentru identitatea digitală au potențialul de a deveni un instrument util pentru atingerea acestui obiectiv. Astfel de orientări ar trebui elaborate ținând seama în mod corespunzător de cadrul de interoperabilitate al Uniunii. Statele membre ar trebui să aibă un rol principal în adoptarea acestora.

(18) În conformitate cu Directiva (UE) 2019/882[8], persoanele cu handicap ar trebui să aibă posibilitatea de a 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.

(19) 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 intern sau al Uniunii. Mai mult, prezentul regulament nu ar trebui să afecteze cerințele naționale cu privire la formă aferente registrelor publice, în special registrelor comerțului și cadastrelor.

(20) Prestarea și utilizarea serviciilor de încredere capătă o importanță sporită pentru comerțul și cooperarea la nivel internațional. Partenerii internaționali ai UE instituie cadre de încredere inspirate din Regulamentul (UE) nr. 910/2014. Prin urmare, pentru a facilita recunoașterea acestor servicii și a prestatorilor acestora, legislația de punere în aplicare poate 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, ca o completare la posibilitatea recunoașterii reciproce a serviciilor de încredere și a prestatorilor acestora stabiliți în Uniune și în țări terțe, în conformitate cu articolul 218 din tratat. Atunci când se stabilesc 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, ar trebui să se asigure, de asemenea, respectarea dispozițiilor relevante din Directiva XXXX/XXXX (Directiva NIS 2) și din Regulamentul (UE) 2016/679, precum și utilizarea listelor sigure ca elemente esențiale pentru consolidarea încrederii.

[8] 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).

(21) Prezentul regulament ar trebui să se bazeze pe actele Uniunii care asigură piețe contestabile și echitabile în sectorul digital. În special, acesta se bazează pe Regulamentul (UE) 2022/1925, care introduce norme pentru furnizorii de servicii de platformă esențiale desemnați drept controlori de acces și, printre altele, interzice controlorilor de acces să le impună utilizatorilor comerciali să utilizeze, să ofere sau să interopereze cu un serviciu de identificare al controlorului de acces în contextul serviciilor oferite de utilizatorii comerciali care utilizează serviciile de platformă esențiale ale controlorului de acces respectiv. Articolul 6 alineatul (7) din Regulamentul 2022/1925 impune controlorilor de acces să permită utilizatorilor comerciali și furnizorilor de servicii auxiliare accesul la aceleași elemente ale sistemului de operare, elemente de hardware sau de software, precum și interoperabilitatea cu acestea, care sunt disponibile sau utilizate la furnizarea de către controlorul de acces a oricăror servicii auxiliare. În conformitate cu articolul 2 punctul 15 din Actul legislativ privind piețele digitale, serviciile de identificare constituie un tip de servicii auxiliare. Prin urmare, utilizatorii comerciali și furnizorii de servicii auxiliare ar trebui să aibă posibilitatea de a accesa astfel de elemente de hardware sau de software, cum ar fi elementele de securitate ale telefoanelor inteligente, și de a interopera cu acestea prin intermediul portofelelor europene pentru identitatea digitală sau al mijloacelor de identificare electronică notificate ale statelor membre.

(22) 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 XXXX/XXXX (Directiva NIS 2), serviciile de încredere trebuie să ia măsuri tehnice și organizatorice adecvate în temeiul Directivei XXXX/XXXX (Directiva NIS 2), 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 XXXX/XXXX (Directiva NIS 2). 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 survenite în contextul identificării persoanelor. Cerințele de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare în temeiul Directivei XXXXXX [NIS 2] ar trebui considerate complementare cerințelor impuse prestatorilor de servicii de încredere în temeiul prezentului regulament. După caz, autoritățile competente desemnate în temeiul Directivei XXXX/XXXX (Directiva NIS 2) ar trebui să aplice în continuare practicile sau orientările naționale stabilite 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. Nicio cerință în temeiul prezentului regulament nu afectează obligația de notificare a încălcărilor securității datelor cu caracter personal în temeiul Regulamentului (UE) 2016/679.

(23) Trebuie acordată o atenție deosebită asigurării unei cooperări eficace între autoritățile NIS și e-IDAS. În cazurile în care organismul de supraveghere prevăzut în prezentul regulament este altul decât autoritățile competente desemnate în temeiul Directivei XXXX/XXXX [NIS 2], autoritățile respective 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 prezentul regulament și în Directiva XXXX/XXXX [NIS 2]. În special, organismele de supraveghere prevăzute în prezentul regulament ar trebui să aibă dreptul de a solicita autorității competente în temeiul Directivei XXXXX/XXXX [NIS 2] 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 NIS 2 sau de a le solicita să remedieze situațiile de nerespectare.

(24) 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 paneuropene de distribuție electronică înregistrată. 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.

(25) În majoritatea cazurilor, cetățenii și alți rezidenți nu pot face, la nivel transfrontalier, schimb digital de informații referitoare la identitatea lor, cum ar fi adrese, vârstă și calificări profesionale, permise de conducere și alte date privind plăți și permise, în condiții de siguranță și cu un nivel ridicat de protecție a datelor.

(26) Ar trebui să fie posibilă eliberarea și gestionarea atributelor digitale de încredere și contribuția la reducerea sarcinii administrative, oferind cetățenilor și altor rezidenți posibilitatea de a le utiliza în tranzacțiile lor private și publice. Cetățenii și alți rezidenți 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, care poate fi verificat și invocat de autoritățile relevante din alte state membre, să se bazeze pe credențialelor lor în materie de securitate socială sau pe viitoarele documente de călătorie digitale în context transfrontalier.

(27) Orice entitate care colectează, creează și eliberează atribute atestate, cum ar fi diplome, licențe, certificate de naștere, ar trebui să poată deveni furnizor de atestări electronice ale atributelor. Beneficiarii ar trebui să utilizeze atestările electronice ale atributelor ca fiind echivalente cu atestările în format tipărit. Prin urmare, unei atestări electronice a atributelor nu ar trebui să i se refuze efectul juridic din motiv că aceasta este în format electronic sau că nu îndeplinește cerințele pentru atestarea electronică calificată a atributelor. În acest scop, ar trebui stabilite cerințe generale pentru a se asigura că o atestare electronică calificată a atributelor are efectul juridic echivalent cu cel al atestărilor eliberate 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 definește cerințe sectoriale suplimentare în ceea ce privește forma cu efecte juridice subiacente și, în special, recunoașterea transfrontalieră a atestării electronice calificate a atributelor, după caz.

(28) Disponibilitatea și utilizarea pe scară largă a portofelelor europene pentru identitatea digitală necesită acceptarea acestora de către prestatorii privați de servicii. Beneficiarii privați care prestează servicii în domeniile transporturilor, energiei, serviciilor bancare și financiare, securității sociale, sănătății, apei potabile, serviciilor poștale, infrastructurii digitale, educației sau telecomunicațiilor ar trebui să accepte utilizarea portofelelor europene pentru identitatea digitală pentru prestarea serviciilor în cazul cărora dreptul național, dreptul Uniunii sau o obligație contractuală impune autentificarea strictă a utilizatorilor. Pentru a facilita utilizarea și acceptarea portofelului european pentru identitatea digitală, ar trebui să se țină seama de standardele și specificațiile din industrie acceptate pe scară largă. În cazul în care platformele online foarte mari, astfel cum sunt definite la articolul 25 alineatul (1) din Regulament [trimitere la Regulamentul DSA], impun utilizatorilor să se autentifice pentru a accesa servicii online, aceste platforme ar trebui să fie mandatate să accepte utilizarea portofelelor europene pentru identitatea digitală la cererea voluntară a utilizatorului. Utilizatorii nu ar trebui să aibă obligația de a utiliza portofelul pentru a accesa servicii private, dar, în cazul în care doresc acest lucru, platformele online mari ar trebui să accepte în acest scop portofelul european pentru identitatea digitală, respectând în același timp principiul reducerii la minimum a datelor. Având în vedere importanța platformelor online foarte mari, datorită impactului lor, în special în ceea ce privește numărul de destinatari ai serviciului și tranzacțiile economice, acest lucru este necesar pentru a spori protecția utilizatorilor împotriva fraudei și pentru a asigura un nivel ridicat de protecție a datelor. Ar trebui elaborate coduri de conduită de autoreglementare la nivelul Uniunii („coduri de conduită”) 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. Acestea ar trebui elaborate în termen de 12 luni de la adoptarea prezentului regulament. Comisia ar trebui să evalueze eficacitatea acestor dispoziții în ceea ce privește disponibilitatea și posibilitatea de utilizare pentru utilizatorul portofelelor europene pentru identitatea digitală după 24 de luni de la implementarea lor.

(29) 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 informațiile care sunt necesare, de exemplu, pentru ca un utilizator să divulge unui beneficiar numai datele 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. Astfel de atribute divulgate selectiv, inclusiv atunci când inițial fac parte din mai multe atestări electronice distincte, pot fi combinate ulterior și prezentate beneficiarilor. Această caracteristică ar trebui să devină un element de proiectare de bază, consolidând astfel confortul și protecția datelor cu caracter personal, inclusiv reducerea la minimum a datelor.

(30) Atributele furnizate de prestatorii de servicii de încredere calificați ca parte a atestării calificate a atributelor ar trebui verificate în raport cu sursele autentice, fie direct de către prestatorul de servicii de încredere calificat, fie prin intermediari desemnați, recunoscuți la nivel național în conformitate cu dreptul național sau cu dreptul Uniunii, în scopul schimbului securizat de atribute atestate între prestatorii de servicii de identitate 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 atestări electronice calificate ale atributelor sunt în măsură, pe baza consimțământului persoanei căreia i se emite atestarea, să verifice autenticitatea atributelor care se bazează pe surse autentice. Mecanismele adecvate pot include recurgerea la intermediari specifici sau la soluții tehnice în conformitate cu legislația națională care permite accesul la surse autentice. Asigurarea disponibilității unui mecanism care să permită verificarea atributelor prin compararea lor cu surse autentice ar trebui să faciliteze respectarea de către prestatorii de servicii de încredere calificați care emit atestări electronice calificate ale atributelor a obligațiilor care le revin în temeiul prezentului regulament. Anexa VI conține o listă a categoriilor de atribute pentru care statele membre ar trebui să se asigure că se iau măsuri pentru a permite prestatorilor calificați care emit atestări electronice ale atributelor să verifice prin mijloace electronice, la cererea utilizatorului, autenticitatea acestora prin comparare cu sursa autentică relevantă. Statele membre ar trebui să convină asupra atributelor specifice care se încadrează în aceste categorii.

(31) Identificarea electronică securizată și furnizarea atestării 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 Regulamentului privind combaterea spălării banilor, [a se adăuga trimiterea după adoptarea propunerii], cu 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.

(31a) Pentru a asigura consecvența practicilor de certificare în întreaga UE, Comisia ar trebui să emită orientări privind certificarea și recertificarea dispozitivelor de creare a semnăturilor electronice calificate și a dispozitivelor de creare a sigiliilor electronice calificate, inclusiv privind valabilitatea și limitările în timp ale acestora. Prezentul regulament nu împiedică statele membre să permită organismelor publice sau private care dețin dispozitive certificate de creare a semnăturilor electronice calificate să prelungească temporar valabilitatea certificării atunci când o recertificare a aceluiași dispozitiv nu a putut fi efectuată în termenul definit de lege din alt motiv decât o încălcare a securității sau un incident de securitate și fără a aduce atingere practicii de certificare aplicabile.

(32) Serviciile de autentificare a site-urilor internet oferă utilizatorilor o garanție solidă că în spatele site-ului internet se află o entitate autentică și legitimă, indiferent ce platformă este folosită pentru afișarea acestuia. Aceste servicii contribuie la construirea încrederii în desfășurarea de activități comerciale online și la reducerea numărului de cazuri de fraudă online. Utilizarea serviciilor de autentificare a unui site internet de către site-uri internet ar trebui să fie voluntară. Cu toate acestea, pentru ca autentificarea unui site internet să devină un mijloc de a spori încrederea, de a oferi utilizatorului o experiență mai bună și de a stimula creșterea economică pe piața internă, prezentul regulament ar trebui să prevadă obligații minime în materie de securitate și răspundere pentru prestatorii serviciilor de autentificare a site-urilor internet și serviciile oferite de aceștia. În acest scop, furnizorii de browsere internet ar trebui să asigure asistență și interoperabilitate cu certificatele calificate pentru autentificarea unui site internet, în temeiul Regulamentului (UE) nr. 910/2014. Aceștia ar trebui să recunoască certificatele calificate pentru autentificarea unui site internet și să permită afișarea datelor de identitate certificate utilizatorului final în mediul browserului, pe baza specificațiilor stabilite în conformitate cu prezentul regulament. Recunoașterea unui certificat calificat pentru autentificarea unui site internet drept un certificat calificat emis de un prestator de servicii de încredere calificat ar trebui să asigure faptul că datele de identitate incluse în certificat pot fi autentificate și verificate în conformitate cu prezentul regulament. Acest lucru nu ar trebui să afecteze posibilitatea ca furnizorii de browsere internet să abordeze neconformitățile majore legate de încălcarea securității și de pierderea integrității certificatelor individuale, contribuind astfel la securitatea online a utilizatorilor finali. Pentru a proteja suplimentar cetățenii și pentru a promova utilizarea acestora, autoritățile publice din statele membre ar trebui să ia în considerare includerea certificatelor calificate pentru autentificarea unui site internet în site-urile lor internet.

(33) Numeroase state membre au introdus cerințe naționale pentru serviciile care oferă arhivare digitală sigură și fiabilă, pentru a permite conservarea pe termen lung a datelor electronice și a serviciilor de încredere conexe. Pentru a asigura securitatea juridică, încrederea și armonizarea între statele membre, ar trebui instituit un cadru juridic pentru serviciile de arhivare electronică calificate, inspirat de cadrul aferent celorlalte servicii de încredere prevăzute în prezentul regulament. Acest cadru 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 de arhivare electronică calificat. Aceste dispoziții ar trebui să se aplice documentelor emise pe cale electronică, precum și documentelor pe suport de hârtie care au fost scanate și digitalizate. Atunci când este necesar, aceste dispoziții ar trebui să permită ca datele electronice păstrate să fie portate pe diferite suporturi sau în diferite formate în scopul prelungirii durabilității și lizibilității acestora dincolo de perioada de valabilitate tehnologică, reducând în același timp la minimum pierderile și modificările în cea mai mare măsură posibilă. Atunci când datele 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 credibilitatea pe perioada de păstrare a acestor date, eventual bazându-se pe utilizarea altor servicii electronice de încredere calificate instituite prin prezentul regulament. Pentru crearea de dovezi ale conservării datelor în cazul în care se utilizează semnături electronice, sigilii electronice sau mărci temporale electronice, ar trebui utilizate servicii electronice de încredere calificate. Pentru situațiile în care serviciile de arhivare electronică nu sunt armonizate prin prezentul regulament, statele membre pot menține sau introduce dispoziții naționale, în conformitate cu dreptul Uniunii, referitoare la aceste servicii, cum ar fi dispoziții specifice care permit unele derogări pentru serviciile integrate într-o organizație și utilizate strict pentru „arhivele interne” ale acestei organizații. Prezentul regulament nu ar trebui să facă distincție între documentele emise pe cale electronică și documentele fizice care au fost digitalizate.

(33a) Arhivele naționale și instituțiile dedicate conservării trecutului, în calitatea lor de organizații dedicate conservării patrimoniului documentar în interes public, sunt, de obicei, mandatate să își desfășoare activitățile în temeiul dreptului intern și nu furnizează neapărat servicii de încredere în sensul prezentului regulament. Atât timp cât aceste instituții nu furnizează astfel de servicii, prezentul regulament nu aduce atingere funcționării lor.

(34) Registrele electronice reprezintă o secvență de înregistrări electronice de date care asigură integritatea acestora și acuratețea ordonării lor cronologice. Scopul registrelor electronice este de a stabili o secvență cronologică de înregistrări de date pentru a împiedica copierea și vânzarea activelor digitale către mai mulți destinatari. Registrele electronice pot fi utilizate, de exemplu, pentru înregistrări digitale ale dreptului de proprietate în comerțul mondial, în finanțarea lanțului de aprovizionare, în digitalizarea drepturilor de proprietate intelectuală sau a mărfurilor, cum ar fi energia electrică. Împreună cu alte tehnologii, acestea pot contribui la găsirea de soluții pentru servicii publice mai eficiente și mai transformatoare, cum ar fi votul electronic, cooperarea transfrontalieră a autorităților vamale, cooperarea transfrontalieră a institutelor academice sau înregistrarea dreptului de proprietate asupra bunurilor imobiliare în registre funciare descentralizate. Registrele electronice calificate creează o prezumție legală pentru ordonarea cronologică secvențială unică și exactă și pentru integritatea înregistrărilor de date din registre. Atributele specifice ale registrelor electronice, și anume ordonarea cronologică secvențială a înregistrărilor de date, diferențiază registrele electronice de alte servicii de încredere, cum ar fi mărcile temporale electronice și serviciile de distribuție electronică înregistrată. Mai precis, nici marcarea temporală a documentelor digitale, nici transferul acestora prin intermediul serviciilor de distribuție electronică înregistrată nu ar putea împiedica în mod suficient, în absența altor măsuri tehnice sau organizatorice, 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 (centralizat sau distribuit).

(35) Pentru a preveni fragmentarea pieței interne, ar trebui instituit un cadru juridic paneuropean care să permită recunoașterea transfrontalieră a serviciilor de încredere pentru înregistrarea datelor în registrele electronice calificate. Prestatorii de servicii de încredere pentru registrele electronice ar trebui să fie mandatați să verifice înregistrarea secvențială a datelor în registru. Prezentul regulament nu aduce atingere obligațiilor juridice pe care utilizatorii registrelor electronice ar putea fi nevoiți să le respecte în temeiul dreptului Uniunii și al dreptului intern. De exemplu, cazurile de utilizare care implică prelucrarea datelor cu caracter personal ar trebui să respecte Regulamentul (UE) 2016/679. Cazurile de utilizare care implică criptoactive ar trebui să fie compatibile cu toate normele financiare aplicabile, inclusiv, de exemplu, Directiva privind piețele instrumentelor financiare[9], Directiva privind serviciile de plată[10], Directiva privind moneda electronică[11], precum și cu posibila legislație viitoare privind piețele criptoactivelor și cu normele privind combaterea spălării banilor care ar putea fi incluse în Regulamentul privind transferurile de fonduri[12] și ar putea impune furnizorilor de servicii de criptoactive să verifice identitatea utilizatorilor registrelor electronice pentru a respecta standardele internaționale de combatere a spălării banilor.

---

9 Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE, JO L 173, 12.6.2014, p. 349-496.

10 Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE, JO L 337, 23.12.2015, p. 35-127.

11 Directiva 2009/110/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 privind accesul la activitate, desfășurarea și supravegherea prudențială a activității instituțiilor emitente de monedă electronică, de modificare a Directivelor 2005/60/CE și 2006/48/CE și de abrogare a Directivei 2000/46/CE (JO L 267, 10.10.2009, p. 7-17).

12 A se vedea propunerea Comisiei din 20.7.2021 de reformare a Regulamentului (UE) 2015/847 al Parlamentului European și alConsiliului din 20 mai 2015 privind informațiile care însoțesc transferurile de fonduri, COM/2021/422 final.

(36) Pentru a evita fragmentarea și barierele, din cauza standardelor divergente și a restricțiilor tehnice, precum și pentru a asigura un proces coordonat în scopul de a evita periclitarea punerii în aplicare a viitorului cadru european al identității digitale, este necesar să existe un proces de cooperare strânsă și structurată între Comisie, statele membre și sectorul privat. Pentru a atinge acest obiectiv, statele membre ar trebui să coopereze în temeiul cadrului stabilit în Recomandarea XXX/XXXX a Comisiei [Setul de instrumente pentru o abordare coordonată în direcția unui cadru pentru identitatea digitală europeană][13] în vederea identificării unui set de instrumente vizând un cadru european al identității digitale. Setul de instrumente ar trebui să includă o arhitectură tehnică cuprinzătoare și un cadru de referință, un set de standarde comune și de referințe tehnice, precum și un set de orientări și descrieri ale celor mai bune practici care să acopere cel puțin toate aspectele legate de funcționalitățile și interoperabilitatea portofelelor europene pentru identitatea digitală, inclusiv semnăturile electronice, și serviciul de încredere calificat pentru atestarea 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 întreprinderile mici și mijlocii în context transfrontalier. Conținutul setului de instrumente ar trebui să evolueze în paralel cu rezultatul discuțiilor și al procesului de adoptare a cadrului european al identității digitale și să reflecte rezultatele acestora.

(36a) Statele membre ar trebui să stabilească norme privind sancțiunile aplicate pentru încălcări precum practicile directe sau indirecte care creează confuzie între serviciile de încredere necalificate și cele calificate sau conduc la utilizarea abuzivă a mărcii de încredere a UE de către prestatorii de servicii de încredere necalificați. Marca de încredere a UE nu ar trebui utilizată în condiții care, în mod direct sau indirect, dau impresia că orice servicii de încredere necalificate oferite de un astfel de prestator ar fi calificate.

---

13 [a se introduce trimiterea după adoptarea recomandării].

(36b) Prezentul regulament ar trebui să asigure 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 calificate ar trebui să fie autorizat să își externalizeze operațiunile legate de prestarea unui serviciu de încredere calificat în afara Uniunii, cu condiția să ofere garanții care asigură că activitățile de supraveghere și auditurile pot fi puse în aplicare ca și cum aceste operațiuni ar fi efectuate în Uniune. Atunci când respectarea regulamentului 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.

(36c) Pentru a asigura securitatea juridică cu privire la valabilitatea semnăturilor electronice avansate bazate pe certificate calificate, este esențial să se specifice în detaliu componentele unei semnături electronice avansate bazate pe certificate calificate, care ar trebui să fie evaluate de către beneficiarul care efectuează validarea semnăturii respective.

(36d) Prestatorii de servicii de încredere ar trebui să utilizeze algoritmi criptografici care să reflecte bunele practici actuale și să implementeze acești algoritmi într-un mod demn de încredere pentru a asigura securitatea și fiabilitatea serviciilor lor de încredere.

(36e) Prezentul regulament ar trebui să prevadă obligația prestatorilor de servicii de încredere calificați de a verifica identitatea unei persoane fizice sau juridice căreia i se emite certificatul calificat pe baza mai multor metode armonizate în întreaga UE. Astfel de metode pot include bazarea pe mijloace de identificare electronică care îndeplinesc cerințele privind un nivel de asigurare „substanțial” în combinație cu proceduri suplimentare armonizate la distanță care asigură identificarea persoanei cu un nivel de asigurare „ridicat”.

(36f) Emitenții de portofele europene pentru identitatea digitală și emitenții de mijloace de identificare electronică notificate care acționează în capacitate comercială sau profesională și utilizează servicii de platformă esențiale oferite de controlori de acces în scopul sau în cursul furnizării de bunuri și servicii utilizatorilor finali ar trebui să fie considerați utilizatori comerciali în conformitate cu articolul 2 punctul 21 din Regulamentul (UE) 2022/1925. Prin urmare, controlorii de acces ar trebui să fie obligați să asigure, în mod gratuit, atât interoperabilitatea efectivă cu aceleași componente ale sistemului de operare, ale hardware-ului sau ale software-ului care sunt disponibile sau sunt utilizate pentru furnizarea propriilor lor servicii complementare sau de sprijin sau a propriului lor hardware, cât și accesul la aceste componente în scopul interoperabilității. Acest lucru ar trebui să le permită emitenților de portofele europene pentru identitatea digitală și emitenților de mijloace de identificare electronică notificate să se interconecteze cu ajutorul interfețelor sau prin soluții similare la componentele respective în mod la fel de eficace ca serviciile sau hardware-ul controlorului de acces.

(36g) Pentru a menține prezentul regulament aliniat la evoluțiile actuale și pentru a respecta practicile de pe piața internă, actele delegate și actele de punere în aplicare adoptate de Comisie ar trebui revizuite și, dacă este necesar, actualizate periodic. Evaluarea necesității acestor actualizări ar trebui să țină seama de noile tehnologii, practici, standarde sau specificații tehnice apărute pe piața internă.

(37) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[14].

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

---

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

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

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

1. Articolul 1 se înlocuiește cu următorul text:

„Prezentul regulament urmărește să asigure buna funcționare a pieței interne și să furnizeze un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere. În acest scop, prezentul regulament:

(aa) stabilește condițiile în care statele membre asigură și 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;

(ab) stabilește condițiile în care statele membre 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, validarea electronică a semnăturilor electronice, a sigiliilor electronice și a certificatelor acestora, validarea electronică a certificatelor pentru autentificarea unui site internet, păstrarea electronică a semnăturilor electronice, a sigiliilor electronice și a certificatelor acestora, arhivarea electronică, atestarea electronică a atributelor, gestionarea dispozitivelor calificate de creare a semnăturilor și a sigiliilor electronice la distanță, 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 au fost notificate de către un stat membru, portofelelor europene pentru identitatea digitală puse la dispoziție de statele membre 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 intern sau al Uniunii privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma ori cerințelor sectoriale privind forma.”

3. Articolul 3 se modifică după cum urmează:

(X) punctul 1 se înlocuiește cu următorul text:

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

(a) punctul 2 se înlocuiește cu următorul text:

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

(aa) punctul 3 se înlocuiește cu următorul text:

„3. «date de identificare personală» înseamnă un set de date emise în conformitate cu dreptul Uniunii sau cu dreptul intern care permit stabilirea identității unei persoane fizice sau juridice ori a unei persoane fizice ce reprezintă o persoană fizică sau juridică;”;

(b) punctul 4 se înlocuiește cu următorul text:

„4. «sistem de identificare electronică» înseamnă un sistem pentru identificarea electronică prin care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice ori pentru persoane fizice ce reprezintă persoane fizice sau juridice;”;

(ba) punctul 5 se înlocuiește cu următorul text:

„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;”;

(bb) se introduce punctul 5a cu următorul text:

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

(c) punctul 14 se înlocuiește cu următorul text:

„14. «certificat pentru semnătura electronică» înseamnă o atestare electronică care face legătura între datele de validare a semnăturii electronice și o persoană fizică și care confirmă cel puțin numele sau pseudonimul persoanei respective;”;

(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:

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

(aa) 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;

(b) crearea semnăturilor electronice sau a sigiliilor electronice;

(c) validarea semnăturilor electronice sau a sigiliilor electronice;

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

(e) gestionarea dispozitivelor calificate de creare a semnăturilor electronice la distanță sau a dispozitivelor calificate de creare a sigiliilor electronice la distanță;

(f) emiterea de atestări electronice ale atributelor;

(fa) validarea atestării electronice a atributelor;

(g) crearea de mărci temporale electronice;

(ga) validarea mărcilor temporale electronice;

(gb) prestarea de servicii de distribuție electronică înregistrate;

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

(h) arhivarea electronică a datelor electronice; sau

(i) înregistrarea datelor electronice într-un registru electronic;”;

(da) punctul 18 se înlocuiește cu următorul text:

„18. «organism de evaluare a conformității» înseamnă un organism definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care este acreditat în conformitate cu regulamentul în cauză 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 să efectueze certificarea portofelelor europene pentru identitatea digitală sau a mijloacelor de identificare electronică;”;

(e) punctul 21 se înlocuiește cu următorul text:

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

(f) se introduc următoarele puncte 23a și 23b:

„23a. «dispozitiv calificat de creare a semnăturii electronice la distanță» înseamnă un dispozitiv calificat de creare a semnăturii electronice 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 gestionat de un prestator de servicii de încredere calificat în conformitate cu articolul 39a în numele unui creator de sigilii;”;

(g) punctul 29 se înlocuiește cu următorul text:

„29. «certificat pentru sigiliul electronic» înseamnă o atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă numele persoanei respective;”;

(h) 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 cerințele prezentului regulament;”;

(i) se adaugă punctele 42-55b având următorul text:

„42. «portofel european pentru identitatea digitală» înseamnă un mijloc de identificare electronică care îi permite utilizatorului să stocheze și să recupereze date de identitate, inclusiv date de identificare personală, și atestări electronice ale atributelor legate de identitatea sa, să le furnizeze beneficiarilor la cerere și să le utilizeze în scopul autentificării, online și, după caz, offline, pentru un serviciu în conformitate cu articolul 6a; și care face posibilă semnarea prin intermediul semnăturilor electronice calificate și sigilarea 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. «atestare electronică a atributelor» înseamnă o atestare în format electronic care permite autentificarea atributelor;

45. «atestare electronică calificată a atributelor» înseamnă o atestare electronică a atributelor, care este emisă de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa V;

45a. «atestare electronică a atributelor» eliberată de un organism din sectorul public responsabil de o sursă autentică sau în numele acestuia înseamnă o atestare electronică a atributelor emisă de un organism din sectorul public responsabil de o sursă autentică ori de un organism din sectorul public desemnat de statul membru să emită astfel de atestări ale atributelor în numele organismelor din sectorul public responsabile de sursele autentice în conformitate cu articolul 45da și care îndeplinește cerințele prevăzute în anexa VII;

46. «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 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;

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

48. «serviciu calificat de arhivare electronică» înseamnă un serviciu de arhivare electronică ce îndeplinește cerințele prevăzute la articolul 45ga;

49. «marca de încredere a portofelului UE pentru identitatea digitală» înseamnă o indicație verificabilă simplă, ușor de recunoscut și clară a faptului că un portofel pentru identitatea digitală a fost pus la dispoziție în conformitate cu prezentul regulament;

50. «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;

53. «registru electronic» înseamnă o secvență de înregistrări electronice de date care asigură integritatea acestora și acuratețea ordonării lor cronologice;

53a «registru electronic calificat» înseamnă o un registru electronic care îndeplinește cerințele prevăzute la articolul 45i;

54. «date cu caracter personal» înseamnă orice informație astfel cum este definită la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

55. «corelarea înregistrărilor» înseamnă un proces prin care datele de identificare personală, mijloacele de identificare personală, atestarea electronică calificată a atributelor sau atestările atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele acestuia sunt corelate cu sau legate de un cont existent care aparține aceleiași persoane;

55a. «identificator unic și permanent» înseamnă un identificator care poate consta fie în date de identificare unice, fie în date de identificare multiple specifice sectorului sau naționale, care este asociat cu un singur utilizator în cadrul unui sistem anume și care este persistent în timp;

55b. «înregistrare de date» înseamnă date electronice înregistrate împreună cu metadatele (sau atributele) aferente care susțin prelucrarea datelor;

55c. «utilizarea offline a portofelelor europene pentru identitatea digitală» înseamnă o interacțiune între un utilizator și un beneficiar într-un loc fizic, caz în care portofelul nu este necesar pentru accesarea unor sisteme la distanță prin intermediul rețelelor de comunicații electronice în scopul interacțiunii respective.”

„*Articolul 5*

Pseudonime în tranzacțiile electronice

Fără a aduce atingere efectului juridic aferent pseudonimelor în temeiul dreptului intern, utilizarea pseudonimelor în cadrul tranzacțiilor electronice nu este interzisă.”

5. La capitolul II se introduce următorul titlu înainte de articolul 6a:

„SECȚIUNEA I

Portofelele europene pentru identitatea digitală”

7. Se introduc următoarele articole 6a, 6b, 6c și 6d:

„*Articolul 6a*

Portofelele europene pentru identitatea digitală

(1) În scopul garantării faptului că toate persoanele fizice și juridice din Uniune au acces transfrontalier securizat, fiabil și neîntrerupt la servicii publice și private, fiecare stat membru se asigură că se pune la dispoziție un portofel european pentru identitatea digitală în termen de 24 de luni de la intrarea în vigoare a actelor de punere în aplicare menționate la alineatul (11) și la articolul 6c alineatul (4).

(2) Portofelele europene pentru identitatea digitală sunt puse la dispoziție:

(a) de către un stat membru;

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

(c) în mod independent de orice stat membru, dar cu recunoașterea de către un stat membru.

(3) Portofelele europene pentru identitatea digitală sunt mijloace de identificare electronică ce permit utilizatorului, într-un mod transparent și ușor de urmărit de către acesta:

(a) să solicite, să selecteze, să combine, să stocheze, să șteargă și să prezinte beneficiarilor în condiții de siguranță atestarea electronică a atributelor și datele de identificare personală, inclusiv să se autentifice online și, după caz, offline, pentru a utiliza servicii publice și private, asigurând, în același timp, că este posibilă divulgarea selectivă a datelor;

(b) să semneze prin intermediul semnăturilor electronice calificate și să sigileze prin intermediul sigiliilor electronice calificate.

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

(a) furnizează un set comun de interfețe:

1. pentru eliberarea datelor de identificare personală, a atestărilor electronice calificate și necalificate ale atributelor sau a certificatelor calificate și necalificate către portofelul european pentru identitatea digitală;

2. pentru ca beneficiarii să solicite date de identificare personală și atestări electronice ale atributelor;

3. pentru prezentarea către beneficiari a datelor de identificare personală sau a atestării electronice a atributelor online și, după caz, și offline;

4. 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”;

(b) nu oferă prestatorilor de servicii de încredere care pun la dispoziție atestări electronice ale atributelor nicio informație cu privire la utilizarea acestor atribute după emiterea lor;

(ba) asigură faptul că identitatea beneficiarilor poate fi validată prin punerea în aplicare a unor mecanisme de autentificare în conformitate cu articolul 6b;

(c) îndeplinesc cerințele prevăzute la articolul 8 în ceea ce privește nivelul de asigurare „ridicat” aplicabil *mutatis mutandis* gestionării și utilizării datelor de identificare personală prin intermediul portofelului, inclusiv identificării și autentificării electronice;

(e) asigură faptul că datele de identificare personală menționate la articolul 12 alineatul (4) litera (d) corespund în mod unic și permanent persoanei fizice sau persoanei juridice asociate cu portofelul ori persoanei fizice care reprezintă persoana fizică sau juridică asociată cu portofelul;

(4a) Statele membre prevăd proceduri care să permită utilizatorului să raporteze eventuala pierdere sau utilizare abuzivă a portofelului său și să solicite revocarea acestuia.

(5) Statele membre pun la dispoziție mecanisme de validare pentru portofelele europene pentru identitatea digitală:

(a) pentru a se asigura că autenticitatea și valabilitatea acestora pot fi verificate;

(d) pentru a permite utilizatorului să autentifice beneficiarii în conformitate cu articolul 6b.

(6) Portofelele europene pentru identitatea digitală sunt eliberate în cadrul unui sistem de identificare electronică notificat, având un nivel de asigurare „ridicat”.

(6a) Punerea la dispoziție, utilizarea pentru autentificare și revocarea portofelelor europene pentru identitatea digitală sunt gratuite pentru persoanele fizice.

(6b) Fără a aduce atingere articolul 6db, statele membre pot prevedea, în conformitate cu dreptul intern, funcționalități suplimentare ale portofelelor europene pentru identitatea digitală, inclusiv interoperabilitatea cu mijloacele naționale de identificare electronică existente.

(7) Utilizatorii dețin controlul deplin asupra utilizării portofelului european pentru identitatea digitală și asupra datelor din portofelul lor european pentru identitatea digitală. Emitentul portofelului european pentru identitatea digitală nu colectează informații cu privire la utilizarea portofelului care nu sunt necesare pentru furnizarea serviciilor oferite de portofel și nici nu combină date de identificare personală și 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 emitentul în cauză sau de la servicii furnizate de terți care nu sunt necesare pentru furnizarea serviciilor oferite de portofel, cu excepția cazului în care utilizatorul a solicitat în mod expres acest lucru. 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 emitentul de portofele europene pentru identitatea digitală. În cazul în care portofelul european pentru identitatea digitală este pus la dispoziție de părți private în conformitate cu alineatul (2) literele (b) și (c), dispozițiile articolului 45f alineatul (4) se aplică *mutatis mutandis*.

(7a) Statele membre notifică Comisiei, fără întârzieri nejustificate, informații cu privire la:

(a) organismul responsabil cu întocmirea și menținerea listei beneficiarilor notificați care recurg la portofelele europene pentru identitatea digitală în conformitate cu articolul 6b alineatul (2);

(b) organismele responsabile cu punerea la dispoziție a portofelelor europene pentru identitatea digitală în conformitate cu articolul 6a alineatul (1);

(c) organismele responsabile cu asigurarea faptului că datele de identificare personală sunt asociate cu portofelul în conformitate cu articolul 6a alineatul (4) litera (e);

Notificarea furnizează, de asemenea, informații cu privire la mecanismul care permite validarea datelor de identificare personală menționate la articolul 12 alineatul (4) și a identității beneficiarilor.

Comisia pune la dispoziția publicului, printr-un canal sigur, informațiile menționate la prezentul alineat într-o formă purtând o semnătură electronică sau un sigiliu electronic, adecvată pentru prelucrarea automată.

(8) Articolul 11 se aplică *mutatis mutandis* portofelului european pentru identitatea digitală.

(9) Articolul 24 alineatul (2) literele (b), (e), (g) și (h) se aplică *mutatis mutandis* emitentului portofelelor europene pentru identitatea digitală.

(10) Portofelul european pentru identitatea digitală este accesibil persoanelor cu handicap în conformitate cu cerințele de accesibilitate prevăzute în Directiva 2019/882.

(11) În termen de șase luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește specificații tehnice și operaționale și standarde de referință pentru cerințele menționate la alineatele (3), (4), (5) și (7a) prin intermediul unui act de punere în aplicare privind implementarea portofelului european pentru identitatea digitală. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(11a) Comisia stabilește specificații tehnice și operaționale, precum și standarde de referință pentru a facilita integrarea utilizatorilor în sistemul reprezentat de portofelul european pentru identitatea digitală, utilizându-se fie mijloace de identificare electronică conforme cu nivelul de asigurare „ridicat”, fie mijloace de identificare electronică conforme cu nivelul de asigurare „substanțial” în combinație cu proceduri suplimentare de integrare la distanță, care împreună îndeplinesc cerințele nivelului de asigurare „ridicat”. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 6b

Beneficiarii portofelelor europene pentru identitatea digitală

(1) În cazul în care un beneficiar care furnizează servicii private sau publice intenționează să recurgă la portofelele europene pentru identitatea digitală puse la dispoziție în conformitate cu prezentul regulament, beneficiarul respectiv notifică acest lucru statului membru în care este stabilit.

(1a) Procedura de notificare este eficientă din punctul de vedere al costurilor și proporțională cu riscurile și asigură faptul că beneficiarii furnizează cel puțin informațiile necesare pentru autentificarea în portofelele europene pentru identitatea digitală. Aceasta ar trebui să includă cel puțin statul membru în care sunt stabiliți și numele beneficiarului și, după caz, numărul său de înregistrare, astfel cum figurează în registrele oficiale.

(1b) Cerința de notificare nu aduce atingere altor cerințe de notificare și de înregistrare în conformitate cu dreptul Uniunii sau cu dreptul intern, cum ar fi cele aplicabile categoriilor speciale de date cu caracter personal, care pot impune cerințe suplimentare de autorizare.

(1c) Statele membre pot scuti beneficiarii de obligația de notificare în cazul în care dreptul Uniunii sau dreptul intern nu prevede cerințe specifice de notificare sau de înregistrare în vederea accesării informațiilor furnizate prin intermediul portofelului european pentru identitatea digitală. Beneficiarii scutiți ar putea să nu fie nevoiți să se autentifice în portofelul european pentru identitatea digitală.

(1d) Beneficiarii notificați în conformitate cu prezentul articol informează fără întârziere statul membru cu privire la orice modificare ulterioară a informațiilor furnizate inițial.

(2) Beneficiarii asigură punerea în aplicare a mecanismelor de autentificare menționate la articolul 6a alineatul (4) litera (ba).

(3) Beneficiarii sunt responsabili de îndeplinirea procedurii de autentificare a persoanelor și de validare a atestărilor electronice a atributelor care provin din portofelele europene pentru identitatea digitală, obținute prin intermediul interfeței comune în conformitate cu articolul 6a alineatul (4) litera (a) punctul 2.

(4) În termen de 6 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește specificații tehnice și operaționale pentru cerințele prevăzute la alineatele (1), (1a) și (1d) prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11). Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 6c

Certificarea portofelelor europene pentru identitatea digitală

(1) Conformitatea portofelelor europene pentru identitatea digitală cu cerințele prevăzute la articolul 6a alineatele (3), (4) și (5), cu cerința de separare logică prevăzută la articolul 6a alineatul (7) și, după caz, cu cerințele prevăzute la articolul 6a alineatul (11a) este certificată de organisme de evaluare a conformității desemnate de statele membre și acreditate în conformitate cu articolul 60 din Regulamentul privind securitatea cibernetică și cu sistemele, specificațiile, standardele și procedurile la care se face trimitere la alineatul (4) literele (a), (aa) și (aaa). Certificarea se acordă pentru o perioadă care nu depășește cinci ani, cu condiția efectuării periodice o dată la doi ani a unei evaluări a vulnerabilității. În cazul în care sunt identificate vulnerabilități și acestea nu sunt remediate în termen de trei luni, certificarea este anulată.

(2) În ceea ce privește conformitatea cu cerințele privind protecția datelor prevăzute la articolul 6a alineatul (7), certificarea prevăzută la alineatul (1) poate fi completată de o certificare în temeiul articolului 42 din Regulamentul (UE) 2016/679.

(3) Conformitatea portofelelor europene pentru identitatea digitală sau a unor părți ale acestora cu cerințele relevante în materie de securitate cibernetică prevăzute la articolul 6a alineatele (3), (4), (5) și (7) și, după caz, (11a), este certificată de organismele de evaluare a conformității menționate la alineatul (1) în cadrul sistemelor relevante de certificare a securității cibernetic în temeiul Regulamentului (UE) 2019/881, la care se face trimitere la alineatul (4) literele (a) și (aa).

(3a) Portofelele europene pentru identitatea digitală certificate nu fac obiectul cerințelor menționate la articolele 7 și 9.

(4) În termen de șase luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare:

(a) o listă a sistemelor de certificare a securității cibernetice în temeiul Regulamentului (UE) 2019/881, necesare pentru certificarea portofelelor europene pentru identitatea digitală, astfel cum se menționează la alineatul (3);

(aa) specificații, proceduri și standarde de referință care să fie utilizate în cadrul sistemelor relevante de certificare a securității cibernetice incluse pe listă în conformitate cu litera (a);

(aaa) o listă de specificații, proceduri și standarde de referință care stabilesc cerințe comune de certificare care nu sunt acoperite de sistemele relevante de certificare a securității cibernetice în temeiul Regulamentului (UE) 2019/881, în scopul certificării menționate la alineatul (1), și care urmăresc să demonstreze că un portofel european pentru identitatea digitală îndeplinește cerințele menționate la alineatul (1);

(b) specificații tehnice, procedurale, organizatorice și operaționale pentru desemnarea organismelor de evaluare a conformității menționate la alineatul (1) și, în ceea ce privește cerințele de certificare stabilite în temeiul literei (aaa), pentru monitorizarea și revizuirea sistemelor de certificare și a metodelor de evaluare conexe pe care le utilizează aceste organisme, precum și a certificatelor și rapoartelor de certificare pe care le eliberează;

(5) Statele membre comunică Comisiei denumirile și adresele organismelor publice sau private menționate la alineatul (1). Comisia pune informațiile respective la dispoziția statelor membre.

(6) Actele de punere în aplicare menționate la alineatul (4) se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 6d

Publicarea unei liste a portofelelor europene pentru identitatea digitală certificate

(1) Statele membre informează Comisia, fără întârzieri nejustificate, cu privire la portofelele europene pentru identitatea digitală care au fost puse la dispoziție în temeiul articolului 6a și certificate de organismele menționate la articolul 6c alineatul (1). De asemenea, statele membre informează Comisia, fără întârzieri nejustificate, în cazul în care certificarea este anulată.

(2) Pe baza informațiilor primite, Comisia stabilește, publică și actualizează o listă, într-un format prelucrabil automat, a portofelelor europene pentru identitatea digitală certificate.

(3) În termen de șase luni de la intrarea în vigoare a prezentului regulament, Comisia definește formatele și procedurile aplicabile în sensul alineatelor (1) și (2) prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11). Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 6da

Încălcarea securității portofelelor europene pentru identitatea digitală

(1) În cazul în care portofelele europene pentru identitatea digitală puse la dispoziție în temeiul articolului 6a sau mecanismele de validare menționate la articolul 6a alineatul (5) litera (a), (d) sau (e) 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, emitentul portofelelor în cauză suspendă fără întârziere punerea la dispoziție și utilizarea acestora. Statul membru în care au fost puse la dispoziție portofelele în cauză informează statele membre și Comisia fără întârzieri nejustificate. Emitentul portofelelor în cauză sau statul membru informează beneficiarii și utilizatorii în mod corespunzător.

(2) În cazul în care încălcarea securității sau compromiterea menționată la alineatul (1) este remediată, emitentul portofelului european pentru identitatea digitală reinstituie punerea la dispoziție și utilizarea acestuia. Statul membru în care au fost puse la dispoziție portofelele în cauză informează statele membre și Comisia fără întârzieri nejustificate. Emitentul portofelelor în cauză sau statul membru informează beneficiarii și utilizatorii fără întârzieri nejustificate.

(3) În cazul în care încălcarea securității sau compromiterea menționată la alineatul (1) nu este remediată în termen de trei luni de la suspendare, statul membru în cauză retrage portofelul european pentru identitatea digitală în cauză și informează celelalte state membre și Comisia în mod corespunzător. Portofelul european pentru identitatea digitală în cauză este retras fără întârzieri nejustificate în cazul în care gravitatea încălcării securității justifică această măsură.

(4) Comisia publică în *Jurnalul Oficial al Uniunii Europene*, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la articolul 6d.

(5) În termen de șase luni de la intrarea în vigoare a prezentului regulament, Comisia aduce precizări suplimentare cu privire la măsurile menționate la alineatele (1), (2) și (3) prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11). Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 6db

Utilizarea transfrontalieră a portofelelor europene pentru identitatea digitală

(1) În cazul în care statele membre solicită o identificare electronică utilizând un mijloc de identificare electronică și o autentificare pentru a accesa un serviciu online furnizat de un organism din sectorul public, acestea acceptă pentru autentificarea utilizatorului și portofele europene pentru identitatea digitală puse la dispoziție în conformitate cu prezentul regulament în scopul autentificării utilizatorului.

(2) În cazul în care beneficiarii privați care furnizează servicii, cu excepția microîntreprinderilor și a întreprinderilor mici, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei, sunt obligați în temeiul dreptului intern sau al dreptului Uniunii să utilizeze autentificarea strictă a utilizatorului pentru identificarea online sau în cazul în care autentificarea strictă a utilizatorului este impusă în baza unei obligații contractuale, inclusiv în domeniile transporturilor, energiei, serviciilor bancare și financiare, securității sociale, sănătății, apei potabile, serviciilor poștale, infrastructurii digitale, educației sau telecomunicațiilor, beneficiarii privați acceptă, de asemenea, în termen de 12 luni de la data punerii la dispoziție a portofelelor europene pentru identitatea digitală în temeiul articolului 6a alineatul (1) și strict la cererea voluntară a utilizatorului, utilizarea portofelelor europene pentru identitatea digitală puse la dispoziție în conformitate cu prezentul regulament în ceea ce privește datele minime necesare pentru serviciul online specific pentru care se solicită autentificarea utilizatorului.

(3) În cazul în care platformele online foarte mari, astfel cum sunt definite la articolul 25 punctul 1 din Regulamentul [trimitere la Regulamentul privind serviciile digitale], impun utilizatorilor să se autentifice pentru a accesa servicii online, acestea acceptă pentru autentificarea utilizatorului și utilizarea portofelelor europene pentru identitatea digitală puse la dispoziție în conformitate cu prezentul regulament, numai la cererea voluntară a utilizatorului și în ceea ce privește datele minime necesare pentru serviciul online pentru care se solicită autentificarea.

(4) În cooperare cu statele membre, Comisia încurajează și facilitează elaborarea unor coduri de conduită, pentru a contribui la disponibilitatea și utilizarea pe scară largă a portofelelor europene pentru identitatea digitală în cadrul domeniului de aplicare al prezentului regulament. Aceste coduri de conduită facilitează acceptarea mijloacelor de identificare electronică, inclusiv a portofelelor europene pentru identitatea digitală, în cadrul domeniului de aplicare al prezentului regulament, în special de către prestatorii de servicii care utilizează servicii de identificare electronică furnizate de terți pentru autentificarea utilizatorilor. Comisia va facilita elaborarea unor astfel de coduri de conduită în strânsă cooperare cu toate părțile interesate relevante și va încuraja prestatorii de servicii să finalizeze elaborarea codurilor de conduită în termen de 12 luni de la adoptarea prezentului regulament și să le pună efectiv în aplicare în termen de 18 luni de la adoptarea regulamentului.

(5) În termen de 24 luni de la implementarea portofelelor europene pentru identitatea digitală, Comisia efectuează o evaluare pentru a stabili, pe baza unor dovezi privind cererea, disponibilitatea și posibilitatea de utilizare a portofelului european pentru identitatea digitală, dacă este oportun ca și alți prestatori privați de servicii online să fie mandatați să accepte utilizarea portofelelor europene pentru identitatea digitală, numai la cererea voluntară a utilizatorului. Criteriile de evaluare includ mărimea bazei de utilizatori, prezența transfrontalieră a prestatorilor de servicii, dezvoltarea tehnologică, evoluția modelelor de utilizare și cererea consumatorilor.”

8. Se introduce următorul titlu înainte de articolul 7:

„SECȚIUNEA II

SISTEME DE IDENTIFICARE ELECTRONICĂ”.

9. Teza introductivă de la articolul 7 se înlocuiește cu următorul text:

„În temeiul articolului 9 alineatul (1), statele membre care nu au făcut încă acest lucru notifică, în termen de 24 de luni de la intrarea în vigoare a actelor de punere în aplicare menționate la articolul 6a alineatul (11) și la articolul 6c alineatul (4), cel puțin un sistem de identificare electronică care include cel puțin un mijloc de identificare cu nivel de asigurare «ridicat»”. Un sistem de identificare electronică este eligibil pentru notificare în temeiul articolului 9 alineatul (1) în cazul în care sunt îndeplinite toate condițiile de mai jos:”.

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

„(2) Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a sistemelor de identificare electronică care au fost notificate în temeiul alineatului (1) de la prezentul articol și informațiile de bază cu privire la acestea.

(3) Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările aduse listei menționate la alineatul (2) în termen de o lună de la data primirii notificării respective.”

12. Se introduce următorul articol 11a:

„*Articolul 11a*

Corelarea înregistrărilor

(1) Atunci când se utilizează pentru autentificare mijloace de identificare electronică notificate și portofele europene pentru identitatea digitală, statele membre, atunci când acționează în calitate de beneficiari, asigură corelarea înregistrărilor.

(2) În scopul punerii la dispoziție de portofele europene pentru identitatea digitală, statele membre includ în setul minim de date de identificare personală menționat la articolul 12 alineatul (4) litera (d) cel puțin un identificator unic și permanent în conformitate cu dreptul Uniunii și cu dreptul intern, pentru a identifica utilizatorul, la cererea acestuia, în cazurile în care identificarea utilizatorului este impusă prin lege.

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

(2aa) Statele membre pot prevedea, în conformitate cu dreptul intern, că utilizatorul portofelului european pentru identitatea digitală poate solicita ca un identificator unic și permanent inclus în setul minim de date de identificare personală și asociat portofelului în conformitate cu articolul 6a alineatul (4) litera (e) să fie înlocuit cu un alt identificator unic și permanent emis de statul membru.

(3) În termen de șase luni de la intrarea în vigoare a prezentului regulament, Comisia aduce precizări suplimentare cu privire la măsurile menționate la alineatul (1) prin intermediul unui act de punere în aplicare. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(3a) În termen de șase luni de la intrarea în vigoare a prezentului regulament, Comisia detaliază măsurile menționate la alineatele (2) și (2aa) prin intermediul unui act de punere în aplicare. Actul de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

13. Articolul 12 se modifică după cum urmează:

Cooperarea și interoperabilitatea

(a) la alineatul (3), litera (d) se elimină;

(b) 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 identifica în mod unic și permanent o persoană fizică, o persoană juridică sau o persoană fizică ce reprezintă persoane fizice sau juridice;”;

(ba) la alineatul (5) se introduce litera (c) cu următorul text:

„(c) o abordare similară în ceea ce privește acceptarea în cadrul serviciilor online a utilizării portofelelor europene pentru identitatea digitală puse la dispoziție în conformitate cu prezentul regulament;”;

(c) la alineatul (6), litera (a) se înlocuiește cu următorul text:

„(a) schimbul de informații, de experiență și de bune practici privind sistemele de identificare electronică și, în special, cerințele tehnice referitoare la interoperabilitate, la corelarea înregistrărilor și la nivelurile de asigurare;”;

(ca) la alineatul (6) se introduce litera (e) cu următorul text:

„(e) schimbul de informații, de experiență și de bune practici și emiterea de orientări cu privire la modul în care serviciile online pot fi concepute, dezvoltate și puse în aplicare astfel încât să se bazeze pe portofelele europene pentru identitatea digitală.”

14. Se introduc următoarele articole 12a și 12b:

„*Articolul 12a*

Certificarea sistemelor de identificare electronică

(1) Conformitatea sistemelor de identificare electronică ce trebuie notificate cu cerințele prevăzute în prezentul regulament este certificată pentru a demonstra conformitatea unor astfel de sisteme sau a unor părți ale acestora cu cerințele prevăzute la articolul 8 alineatul (2) în ceea ce privește nivelurile de asigurare ale sistemelor de identificare electronică din cadrul unui sistem relevant de certificare a securității cibernetice în temeiul Regulamentului (UE) 2019/881 sau al unor părți ale acestuia, în măsura în care certificatul de securitate cibernetică sau unele părți ale acestuia acoperă cerințele prevăzute la articolul 8 alineatul (2) în ceea ce privește nivelurile de asigurare ale sistemelor de identificare electronică. Certificarea se acordă pentru o perioadă care nu depășește cinci ani, cu condiția efectuării periodice o dată la doi ani a unei evaluări a vulnerabilității. În cazul în care sunt identificate vulnerabilități și acestea nu sunt remediate în termen de trei luni, certificarea este anulată.

Certificarea se efectuează de către organisme de evaluare a conformității publice sau private acreditate, desemnate de statele membre, și în conformitate cu Regulamentul (CE) nr. 765/2008.

(2) Evaluarea *inter pares* privind sistemele de identificare electronică menționată la articolul 12 alineatul (6) litera (c) nu se aplică sistemelor de identificare electronică sau unor părți ale acestor sisteme certificate în conformitate cu alineatul (1).

(2a) În pofida alineatului (2) de la prezentul articol, statele membre pot solicita unui stat membru notificator informații suplimentare cu privire la sistemele de identificare electronică sau la părți ale acestora certificate în conformitate cu alineatul (2) de la prezentul articol.

(3) Statele membre notifică Comisiei denumirile și adresele organismului public sau privat menționat la alineatul (1). Comisia pune informațiile respective la dispoziția statelor membre.

Articolul 12b

Accesul la elemente de hardware și software

Emitenții de portofele europene pentru identitatea digitală și emitenții de mijloace de identificare electronică notificate care acționează în capacitate comercială sau profesională și utilizează servicii de platformă esențiale, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2022/1925, 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 conformitate cu articolul 2 alineatul (21) din Regulamentul (UE) 2022/1925.”

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

„(1) În pofida alineatului (2) de la prezentul articol, 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.

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.

Prezumția de intenție sau de neglijență se aplică unui prestator de servicii de încredere calificat, cu excepția cazului în care acesta dovedește că prejudiciul menționat la primul paragraf nu a intervenit din intenția sau din neglijența sa.”

18. Articolul 14 se înlocuiește 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 o organizație internațională sunt recunoscute în temeiul unei decizii 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 tratat.

(2) Deciziile de punere în aplicare și acordurile menționate la alineatul (1) asigură faptul 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 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.

Acordurile menționate la alineatul (1) asigură faptul 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.

(3) Deciziile de punere în aplicare menționate la alineatul (1) se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

19. Articolul 15 se înlocuiește cu următorul text:

„*Articolul 15*

Accesibilitatea pentru persoanele cu handicap

Prestarea serviciilor de încredere și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu handicap în conformitate cu cerințele de accesibilitate prevăzute în Directiva 2019/882 privind cerințele de accesibilitate aplicabile produselor și serviciilor.”

20. Articolul 17 se modifică după cum urmează:

(a) alineatul (4) se modifică după cum urmează:

1. alineatul (4) litera (c) se înlocuiește cu următorul text:

„(c) să informeze autoritățile naționale competente relevante ale statelor membre în cauză, desemnate în temeiul Directivei (UE) XXXX/XXXX [NIS2], cu privire la orice încălcare gravă a securității sau pierdere a integrității de care ia cunoștință în îndeplinirea sarcinilor sale. În cazul în care încălcarea gravă a securității sau pierderea integrității vizează alte state membre, organismul de supraveghere informează punctul unic de contact al statului membru în cauză desemnat în temeiul Directivei (UE) XXXX/XXXX (NIS2) și organismele de supraveghere desemnate în temeiul articolului 17 din prezentul regulament din celelalte state membre în cauză. Organismul de supraveghere notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării securității sau pierderii integrității servește interesului public;”;

2. litera (f) se înlocuiește cu următorul text:

„(f) să coopereze cu autoritățile de supraveghere competente instituite în temeiul Regulamentului (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;”;

(b) alineatul (6) se înlocuiește cu următorul text:

„(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere înaintează Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior.”;

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

„(8) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia adoptă orientări privind îndeplinirea de către organismele de supraveghere a sarcinilor menționate la alineatul (4) și, prin intermediul unor acte de punere în aplicare adoptate în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2), definește formatele și procedurile pentru raportul menționat la alineatul (6).”

21. Articolul 18 se modifică după cum urmează:

(a) titlul articolului 18 se înlocuiește cu următorul text:

„Asistență reciprocă și cooperare”;

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

„(1) Organismele de supraveghere cooperează cu scopul de a face schimb de bune practici și de informații privind prestarea de servicii de încredere.”;

(c) se adaugă următoarele alineate (4) și (5):

„(4) Organismele de supraveghere și autoritățile naționale competente în temeiul Directivei (UE) XXXX/XXXX a Parlamentului European și a Consiliului [NIS2] cooperează și se asistă reciproc pentru a se asigura că prestatorii de servicii de încredere respectă cerințele prevăzute în prezentul regulament și în Directiva (UE) XXXX/XXXX [NIS2]. Organismele de supraveghere solicită autorităților naționale competente în temeiul Directivei XXXX/XXXX [NIS2] să desfășoare acțiuni de supraveghere pentru a verifica respectarea de către prestatorii de servicii de încredere a cerințelor prevăzute în Directiva XXXX/XXXX (NIS2), să solicite prestatorilor de servicii de încredere să remedieze orice nerespectare a cerințelor respective, să furnizeze în timp util rezultatele oricăror activități de supraveghere în legătură cu prestatorii de servicii de încredere și să informeze organismele de supraveghere cu privire la incidentele relevante notificate în conformitate cu Directiva XXXX/XXXX [NIS2].

(5) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, modalitățile procedurale necesare pentru a facilita cooperarea dintre autoritățile de supraveghere menționate la alineatul (1). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

21a. Se introduce următorul articol 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. În pofida dispozițiilor articolului 18 din Directiva (UE) XXXX/XXX [NIS2], măsurile respective includ cel puțin următoarele:

(i) măsuri referitoare la procedurile de înregistrare și de integrare în cadrul unui serviciu;

(ii) măsuri referitoare la controalele procedurale sau administrative;

(iii) măsuri referitoare la gestionarea și implementarea serviciilor.

(b) notifică organismului de supraveghere, persoanelor afectate care pot fi identificate, publicului, dacă chestiunea este de interes public, și, după caz, altor organisme competente relevante, orice încălcare a securității sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la litera (a) punctele (i), (ii) și (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, nu mai târziu de 24 de ore din momentul în care a luat cunoștință de respectiva încălcare a securității sau perturbare.

(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia precizează, prin intermediul unor acte de punere în aplicare, caracteristicile tehnice ale măsurilor menționate la alineatul (1) litera (a). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

22. 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 o dată la 24 de luni, de către un organism de evaluare a conformității. Auditul confirmă dacă prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care aceștia le prestează îndeplinesc cerințele prevăzute în prezentul regulament și la articolul 18 din Directiva (UE) XXXX/XXX [NIS2]. 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.”;

(aa) se introduce următorul alineat:

„(1a) Statele membre pot prevedea ca prestatorii de servicii de încredere calificați să informeze în prealabil organismul de supraveghere cu privire la auditurile planificate și să permită participarea organismului de supraveghere în calitate de observator, la cerere.”;

(b) la alineatul (2), ultima teză se înlocuiește cu următorul text:

„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 în temeiul Regulamentului (UE) 2016/679.”;

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

„(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, organismul de supraveghere, ținând seama în special de amploarea, durata și consecințele respectivei neîndepliniri a cerințelor, poate retrage statutul de „calificat” al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.

(3a) În cazul în care organismul de supraveghere este informat de autoritățile naționale competente în temeiul Directivei (UE) XXXX/XXXX [NIS2] că prestatorul de servicii de încredere calificat nu îndeplinește vreuna dintre cerințele prevăzute la articolul 18 din Directiva (UE) XXXX/XXXX [NIS2], organismul de supraveghere, ținând seama în special de amploarea, durata și consecințele acestei neîndepliniri a cerințelor, poate retrage statutul de „calificat” al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.

(3b) În cazul în care organismul de supraveghere este informat de autoritățile de supraveghere în temeiul Regulamentului (UE) 2016/679 că prestatorul de servicii de încredere calificat nu îndeplinește vreuna dintre cerințele prevăzute în Regulamentul (UE) 2016/679, organismul de supraveghere, ținând seama în special de amploarea, durata și consecințele acestei neîndepliniri a cerințelor, poate retrage statutul de „calificat” al prestatorului respectiv sau al serviciului prestat de acesta care este afectat.

(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 menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1), precum și autoritățile naționale competente menționate în Directiva (UE) XXXX/XXXX [NIS2].

(4) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor 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 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).

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

23. Articolul 21 se modifică după cum urmează:

„(1) În cazul în care prestatorii de servicii de încredere intenționează să înceapă prestarea unui serviciu de încredere calificat, aceștia transmit organismului de supraveghere o notificare 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 18 din Directiva (UE) XXXX/XXXX [NIS2].”;

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

„(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 18 din Directiva XXXX [NIS2], organismul de supraveghere solicită autorităților competente menționate în Directiva XXXX [NIS2] să desfășoare acțiuni de supraveghere în această privință și să furnizeze informații cu privire la rezultat, fără întârzieri nejustificate și în termen de două luni de la primirea solicitării. În cazul în care verificarea nu este încheiată în termen de două luni de la notificare, autoritățile competente menționate în Directiva XXXX [NIS2] 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) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia definește, prin intermediul unor acte de punere în aplicare, formatele și procedurile de notificare și verificare în sensul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

25. Articolul 24 se modifică după cum urmează:

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

„(1) Atunci când emite un certificat calificat sau o atestare electronică calificată a 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 atestarea electronică calificată a atributelor.

Informațiile menționate la primul paragraf sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe, în oricare dintre următoarele moduri:

(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 unor atestări electronice calificate ale atributelor sau al unui certificat al unei semnături electronice calificate sau al unui sigiliu electronic calificat eliberat în conformitate cu literele (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) în prezența persoanei fizice sau a unui reprezentant autorizat al persoanei juridice, prin proceduri adecvate și în conformitate cu legislația națională.”;

(b) se introduce următorul alineat (1a):

„(1a) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificații tehnice, standarde și proceduri minime cu privire la verificarea identității și a atributelor în conformitate cu alineatul (1) litera (c). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

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

0. litera (a) se modifică după cum urmează:

„(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. Organismul de supraveghere poate solicita informații suplimentare sau rezultatul unei evaluări a conformității înainte de a acorda permisiunea pentru punerea în aplicare a modificărilor preconizate la serviciile 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.”

1. 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 securitatea tehnică și fiabilitatea proceselor pe care le sprijină, inclusiv prin folosirea unor algoritmi criptografici, lungimi ale cheilor și funcții hash adecvate în cadrul sistemelor și produselor, precum și în cadrul proceselor sprijinite de acestea;”;

2. se introduc următoarele litere (fa) și (fb):

„(fa) 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. În pofida dispozițiilor articolului 18 din Directiva UE XXXX/XXXX [NIS2], măsurile respective includ cel puțin următoarele:

(i) măsuri referitoare la procedurile de înregistrare și de integrare în cadrul unui serviciu;

(ii) măsuri referitoare la controalele procedurale sau administrative;

(iii) măsuri referitoare la gestionarea și punerea în aplicare a 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 sau perturbare survenită în prestarea serviciului sau în punerea în aplicare a măsurilor menționate la litera (fa) punctele (i), (ii) și (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, nu mai târziu de 24 de ore după producerea incidentului.”;

3. literele (g) și (h) 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 prestatorul de servicii de încredere calificat, în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic;”;

4. litera (j) se elimină;

(d) se introduce următorul alineat (4a):

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

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

„(5) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice, procedurile și numerele de referință ale standardelor pentru cerințele menționate la alineatul (2). În cazul în care se respectă specificațiile tehnice, procedurile și standardele respective, se presupune că cerințele prevăzute la prezentul articol sunt respectate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”;

(f) se introduce următorul alineat (6):

„(6) Comisia este împuternicită să adopte acte de punere în aplicare care să precizeze caracteristicile tehnice ale măsurilor menționate la alineatul (2) litera (fa).”

25a. Articolul 26 se modifică după cum urmează:

„(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru semnăturile electronice avansate. În cazul în care o semnătură electronică avansată îndeplinește specificațiile și standardele respective, se presupune că cerințele privind semnăturile electronice avansate sunt respectate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

25b. Articolul 27 se modifică după cum urmează:

alineatul (4) se elimină.

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

„(6) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru certificatele calificate pentru semnăturile electronice. În cazul în care un certificat calificat pentru semnătura electronică îndeplinește specificațiile și standardele respective, se presupune că acesta respectă cerințele prevăzute în anexa I. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

27. La articolul 29, se adaugă un nou alineat (1a) cu următorul text:

„(1a) Generarea și gestionarea datelor de creare a semnăturilor electronice în numele semnatarului sau duplicarea unor astfel de date în scopul creării unei copii de rezervă se pot realiza numai 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 29a:

„*Articolul 29a*

Cerințe privind un serviciu calificat pentru gestionarea dispozitivelor calificate de creare a semnăturilor electronice la distanță

(1) Gestionarea dispozitivelor calificate de creare a semnăturilor electronice la distanță ca serviciu calificat poate fi efectuată 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, poate duplica 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 la distanță, emis în temeiul articolului 30.

(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor în sensul alineatului (1).”

29. La articolul 30 se introduce următorul alineat (3a):

„(3a) Perioada de valabilitate a certificării menționate la alineatul (1) nu depășește cinci ani, cu condiția efectuării periodice o dată la doi ani a unei evaluări a vulnerabilității. 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) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia definește, prin intermediul unor acte de punere în aplicare, formatele și procedurile aplicabile în sensul alineatului (1). Actele de punere în aplicare respective 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 îndeplinește specificațiile și standardele menționate la alineatul (3), se presupune că aceasta respectă cerințele prevăzute la primul paragraf.”;

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

„(3) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile și numerele de referință ale standardelor pentru validarea semnăturilor electronice calificate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

31a. Se introduce următorul articol 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 cu următoarele condiții:

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

(b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării;

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

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

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

(f) integritatea datelor semnate nu a fost compromisă;

(g) cerințele prevăzute la articolul 26 au fost îndeplinite la momentul semnării. În cazul în care validarea semnăturilor electronice avansate bazate pe certificate calificate îndeplinește specificațiile și standardele menționate la alineatul (3), se presupune că aceasta respectă cerințele prevăzute la primul paragraf.

(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) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile și numerele de referință ale standardelor pentru validarea semnăturilor electronice avansate bazate pe certificate calificate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

31b. Articolul 33 se modifică după cum urmează:

„(1) Un serviciu de validare calificat pentru semnături electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care:”;

„(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru serviciul de validare calificat menționat la alineatul (1). În cazul în care serviciul de validare a semnăturilor electronice calificate îndeplinește specificațiile și standardele respective, se presupune că acesta respectă cerințele prevăzute la alineatul (1). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

32. Articolul 34 se înlocuiește cu următorul text:

„*Articolul 34*

Serviciul calificat de păstrare a semnăturilor electronice calificate

(1) Un serviciu calificat de păstrare a semnăturilor electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care utilizează proceduri și tehnologii capabile să extindă fiabilitatea semnăturilor electronice calificate dincolo de perioada de validitate tehnologică.

(2) În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc specificațiile și standardele menționate la alineatul (3), se presupune că acestea respectă cerințele prevăzute la alineatul (1).

(3) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru serviciul calificat de păstrare a semnăturilor electronice calificate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

32a. La articolul 36 se adaugă un nou alineat (2):

„(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru sigiliile electronice avansate.

În cazul în care un sigiliu electronic avansat îndeplinește specificațiile și standardele respective, se presupune că cerințele privind sigiliile electronice avansate sunt respectate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

33. Articolul 37 se modifică după cum urmează:

alineatul (4) se elimină.

34. Articolul 38 se modifică după cum urmează:

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

„(1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute în anexa III. În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește specificațiile și standardele menționate la alineatul (6), se presupune că acesta respectă cerințele prevăzute în anexa III.”;

(b) alineatul (6) se înlocuiește cu următorul text:

„(6) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru certificatele calificate pentru sigiliile electronice. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

35. Se introduce următorul articol 39a:

„*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.”

35a. Se introduce următorul articol 40a:

„*Articolul 40a*

Cerințe pentru validarea sigiliilor electronice avansate bazate pe certificate calificate

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

36. Articolul 42 se modifică după cum urmează:

(a) se introduce un nou alineat (1a) cu următorul text:

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

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

„(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru legătura între dată și oră și date și pentru exactitatea sursei orei indicate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

36a. La articolul 43 se adaugă un nou alineat (3) cu următorul text:

„(2a) Un serviciu de distribuție electronică înregistrată calificat dintr-un stat membru este recunoscut drept serviciu de distribuție electronică înregistrată calificat în orice alt stat membru.”

37. Articolul 44 se modifică după cum urmează:

(a) se introduce următorul alineat (1a):

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

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

„(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru procesele de trimitere și primire de date. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”;

(c) se introduc următoarele alineate (3) și (4):

„(3) 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). Conformitatea este confirmată de un organism de evaluare a conformității.

(4) Comisia poate stabili, prin intermediul unui act de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru a facilita transferul de date între doi sau mai mulți prestatori de servicii de încredere calificați. Specificațiile tehnice și conținutul standardelor sunt eficiente din punctul de vedere al costurilor și proporționate. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

38. 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 cerințele prevăzute în anexa IV se efectuează în conformitate cu specificațiile și standardele menționate la alineatul (4).

(2) Certificatele calificate pentru autentificarea unui site internet menționate la alineatul (1) sunt recunoscute de browserele web. În acest scop, browserele web garantează că datele de identitate furnizate utilizând oricare dintre metode sunt afișate într-un mod ușor de utilizat. Browserele web asigură suport și interoperabilitate cu certificatele calificate pentru autentificarea unui site internet menționate la alineatul (1), cu excepția întreprinderilor considerate microîntreprinderi și întreprinderi mici în conformitate cu Recomandarea 2003/361/CE a Comisiei în primii 5 ani de funcționare ca prestatori de servicii de navigare pe internet.

(4) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile și numerele de referință ale standardelor pentru certificatele calificate pentru autentificarea unui site internet menționate la alineatul (1). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

39. După articolul 45, se introduc următoarele secțiuni 9, 10 și 11:

„SECȚIUNEA 9

ATESTAREA ELECTRONICĂ A ATRIBUTELOR

Articolul 45a

Efectele juridice ale atestării electronice a atributelor

(1) Unei atestări electronice a atributelor nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru atestările electronice calificate ale atributelor.

(2) O atestare electronică calificată a atributelor și atestările 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 atestările eliberate în mod legal în format tipărit.

(3) O atestare electronică calificată a atributelor emisă într-un stat membru este recunoscută drept atestare electronică calificată a atributelor în orice alt stat membru.

(4) O atestare a atributelor emisă de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este recunoscută ca o atestare a atributelor emisă de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism în toate statele membre.

Articolul 45b

Atestarea electronică a atributelor în serviciile publice

Atunci când identificarea electronică cu ajutorul unui mijloc de identificare electronică și al autentificării este necesară în temeiul dreptului intern pentru a accesa un serviciu prestat online de un organism din sectorul public, datele de identificare personală din atestarea electronică a 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, atestarea electronică calificată a atributelor din alte state membre.

Articolul 45c

Cerințe pentru atestarea electronică calificată a atributelor

(1) Atestarea electronică calificată a atributelor îndeplinește cerințele prevăzute în anexa V.

(1a) Evaluarea conformității cu cerințele prevăzute în anexa V se efectuează în conformitate cu specificațiile și standardele menționate la alineatul (4).

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

(3) În cazul în care o atestare electronică calificată a atributelor este revocată după emiterea inițială, aceasta își pierde valabilitatea din momentul revocării și nu se poate reveni în niciun caz la statutul său anterior.

(4) În termen de 6 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește specificațiile tehnice și numerele de referință ale standardelor pentru atestările electronice calificate ale atributelor, prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11).

Articolul 45d

Verificarea atributelor în raport cu surse autentice

(1) În termen de 24 de luni de la intrarea în vigoare a actelor de punere în aplicare menționate la articolul 6a alineatul (11) și la articolul 6c alineatul (4), statele membre se asigură că, cel puțin în cazul atributelor enumerate în anexa VI, ori de câte ori aceste atribute se bazează pe surse autentice din sectorul public, se iau măsuri pentru a permite prestatorilor calificați de atestări electronice ale atributelor să verifice aceste atribute prin mijloace electronice, la cererea utilizatorului și în conformitate cu dreptul intern sau cu dreptul Uniunii.

(2) În termen de 6 luni de la intrarea în vigoare a prezentului regulament, ținând cont de standardele internaționale relevante, Comisia stabilește specificații tehnice, standarde și proceduri minime în ceea ce privește catalogul de atribute și sisteme pentru atestarea atributelor și procedurile de verificare pentru atestările electronice calificate ale atributelor, prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11).

Articolul 45da

Cerințe privind atestarea electronică a atributelor emisă de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism

(1) O atestare electronică a atributelor emisă 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) certificatul calificat care sprijină semnătura electronică calificată sau sigiliul electronic calificat al organismului din sectorul public menționat la articolul 3 punctul 45a, identificat drept emitentul menționat la litera (b) din anexa VII conține un set specific de atribute certificate într-o formă adecvată pentru prelucrarea automată, care:

(i) indică faptul că organismul emitent este instituit în conformitate cu legislația națională sau cu dreptul Uniunii ca fiind responsabil de sursa autentică pe baza căreia este emisă atestarea electronică a atributelor sau ca organism desemnat să acționeze în numele acestuia;

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

(iii) precizează legislația națională sau dreptul Uniunii menționate la litera (i).

(2) Statul membru în care sunt stabilite organismele din sectorul public menționate la articolul 3 punctul 45a se asigură că organismele din sectorul public care emit atestări electronice ale atributelor au un nivel de fiabilitate echivalent cu cel al prestatorilor de servicii de încredere calificați, în conformitate cu articolul 24.

(2a) Statele membre notifică Comisiei organismele din sectorul public menționate la articolul 3 punctul 45a. Această notificare 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 45a într-o formă purtând o semnătură electronică sau un sigiliu electronic, adecvată pentru prelucrarea automată.

(3) În cazul în care o atestare electronică a atributelor emisă de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este revocată după emiterea inițială, aceasta își pierde valabilitatea din momentul revocării. După revocare, nu se poate reveni la statutul atestării electronice anterior revocării.

(4) O atestare electronică a atributelor emisă de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este considerată conformă cu cerințele prevăzute la alineatul (1) de la prezentul articol, în cazul în care îndeplinește standardele menționate la alineatul (5).

(5) În termen de 6 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește specificațiile tehnice și numerele de referință ale standardelor pentru atestările electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism, prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11).

(5a) În termen de 6 luni de la intrarea în vigoare a prezentului regulament, Comisia definește formatele, procedurile, specificațiile și standardele aplicabile în sensul alineatului (2a) prin intermediul unui act de punere în aplicare privind implementarea portofelelor europene pentru identitatea digitală, astfel cum se prevede la articolul 6a alineatul (11).

(6) Organismele din sectorul public menționate la articolul 3 punctul 45a care emit atestări electronice ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală furnizate în conformitate cu articolul 6a.

Articolul 45e

Emiterea atestării electronice a atributelor pentru portofelele europene pentru identitatea digitală

Prestatorii de atestări electronice calificate ale atributelor pun la dispoziție o interfață cu portofelele europene pentru identitatea digitală furnizate în conformitate cu articolul 6a.

Articolul 45f

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 atestării electronice a atributelor.

(4) Prestatorii de servicii de atestare electronică calificată a atributelor pun în aplicare separarea funcțională pentru prestarea acestor servicii.

SECȚIUNEA 10

SERVICII DE ARHIVARE ELECTRONICĂ

Articolul 45 g

Efectul juridic al unui serviciu de arhivare electronică

(1) Datelor electronice stocate prin utilizarea unui serviciu de arhivare electronică nu li se refuză efectul juridic și posibilitatea de a fi acceptate ca probă în procedurile judiciare doar din motiv că acestea sunt sub formă electronică sau că nu sunt stocate prin utilizarea unui serviciu de arhivare electronică calificat.

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

(3) Un serviciu de arhivare electronică calificat dintr-un stat membru este recunoscut drept serviciu de arhivare electronică calificat în orice alt stat membru.

Articolul 45ga

Cerințe pentru serviciile de arhivare electronică calificate

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

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

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

(c) garantează că datele 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 extrase dintr-o arhivă electronică calificată beneficiază de prezumția de integritate de la începutul perioadei de păstrare până în momentul extragerii. Acest raport este furnizat într-un mod fiabil și eficient și poartă semnătura electronică calificată sau sigiliul electronic calificat al prestatorului serviciului de arhivare electronică calificat.

(2) În termen de 12 luni de la intrarea în vigoare a prezentului regulament, Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru serviciile de arhivare electronică calificate. În cazul în care un serviciu de arhivare electronică calificat îndeplinește specificațiile și standardele respective, se presupune că cerințele privind serviciile de arhivare electronică calificate sunt respectate. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

SECȚIUNEA 11

REGISTRE ELECTRONICE

Articolul 45h

Efectele juridice ale registrelor electronice

(1) Unui registru electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca probă în procedurile judiciare doar din motiv că acesta este sub formă electronică 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.

(3) Un registru electronic calificat dintr-un stat membru este recunoscut drept registru electronic calificat în orice alt stat membru.

Articolul 45i

Cerințe pentru registrele electronice calificate

(1) Registrele electronice calificate îndeplinesc următoarele cerințe:

(a) sunt create 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 specificațiile și standardele menționate la alineatul (3), se presupune că acesta respectă cerințele prevăzute la alineatul (1).

(3) Comisia stabilește, prin intermediul unor acte de punere în aplicare, specificațiile tehnice și numerele de referință ale standardelor pentru crearea și exploatarea unui registru electronic calificat. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).”

40. Se introduce următorul articol 48a:

„*Articolul 48a*

Cerințe de raportare

(1) Statele membre asigură colectarea statisticilor în legătură cu funcționarea portofelelor europene pentru identitatea digitală odată ce acestea au fost puse la dispoziție pe teritoriile lor.

(2) Statisticile 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) un raport de sinteză care include date privind incidentele care împiedică utilizarea portofelului european pentru identitatea digitală.

(3) Statisticile 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 statisticile colectate în conformitate cu alineatul (2).”

41. Articolul 49 se înlocuiește cu următorul text:

„*Articolul 49*

Revizuire

(1) Comisia revizuiește modul de aplicare a prezentului regulament și prezintă un raport în acest sens Parlamentului European și Consiliului în termen de 36 de luni de la intrarea în vigoare a acestuia. Comisia evaluează, în special, domeniul de aplicare al articolelor 6 și 6db, precum și oportunitatea modificării domeniului de aplicare al prezentului regulament sau a dispozițiilor sale specifice, ținând seama de experiența dobândită în aplicarea prezentului regulament, precum și de evoluțiile tehnologice, juridice, ale pieței și ale cererii clienților. Dacă este necesar, raportul este însoțit de o propunere de modificare a prezentului regulament.

(2) Raportul de evaluare include o analiză a disponibilității și a posibilității de utilizare a portofelelor europene pentru identitatea digitală care intră în domeniul de aplicare al prezentului regulament și stabilește dacă toți prestatorii privați de servicii online care se bazează pe servicii de identificare electronică furnizate de terți pentru autentificarea utilizatorilor ar trebui să fie mandatați să accepte utilizarea portofelelor europene pentru identitatea digitală.

(3) În plus, Comisia prezintă un raport Parlamentului European și Consiliului, o dată la patru ani, ulterior raportului menționat la primul paragraf, cu privire la progresele realizate în vederea atingerii obiectivelor prezentului regulament.”

42. Articolul 51 se înlocuiește cu următorul text:

„*Articolul 51*

Măsuri tranzitorii

(1) Dispozitivele securizate de creare a semnăturilor a căror conformitate a fost stabilită pe baza articolului 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].

(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 intrarea în vigoare a prezentului regulament].

(2a) În ceea ce privește 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 consideră în continuare că nu este necesară obținerea statutului de „calificat” pentru prestarea acestor servicii de gestionare până la [24 de luni de la intrarea în vigoare a prezentului regulament].

(2b) 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 regulamentului de modificare] și care utilizează metode de verificare a identității pentru emiterea certificatelor calificate în conformitate cu articolul 24 alineatul (1) prezintă organismului de supraveghere un raport de evaluare a conformității care dovedește conformitatea cu articolul 24 alineatul (1) cât mai curând posibil și în termen de 30 de luni de la intrarea în vigoare a regulamentului de modificare. Până la prezentarea unui astfel de raport de evaluare a conformității și până la finalizarea evaluării sale de către organismul de supraveghere, prestatorul de servicii de încredere calificat se poate baza în continuare pe metodele de verificare a identității prevăzute la articolul 24 alineatul (1) din Regulamentul (UE) nr. 910/2014.

43. Anexa I se modifică în conformitate cu anexa I la prezentul regulament.

44. Anexa II se înlocuiește cu textul din anexa II la prezentul regulament.

45. Anexa III se modifică în conformitate cu anexa III la prezentul regulament.

46. Anexa IV se modifică în conformitate cu anexa IV la prezentul regulament.

47. Se adaugă o nouă anexă V în conformitate cu anexa V la prezentul regulament.

48. O nouă anexă VI se adaugă la prezentul regulament.

Articolul 2

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
Președintele	Președintele

ANEXA I

În anexa I, punctul (i) se înlocuiește cu următorul text:

„(i) informațiile privind statutul valabilității certificatului calificat sau localizarea serviciilor care pot fi utilizate pentru a cunoaște acest statut;”.

ANEXA II

CERINȚE PENTRU DISPOZITIVELE DE CREARE A SEMNĂTURILOR ELECTRONICE CALIFICATE

1. Dispozitivele de creare a semnăturilor electronice calificate asigură, prin mijloace tehnice și procedurale adecvate, cel puțin că:

(a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil;

(b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată;

(c) există asigurări rezonabile că datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice nu pot să fie descoperite prin deducție și că semnătura electronică este protejată în mod fiabil împotriva falsificării utilizând tehnologia disponibilă în prezent;

(d) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot să fie protejate în mod fiabil de către semnatarul legitim împotriva utilizării de către alte persoane.

2. Dispozitivele de creare a semnăturilor electronice calificate nu modifică datele care urmează să fie semnate sau nu împiedică prezentarea lor semnatarului înainte de a semna.

ANEXA III

În anexa III, punctul (i) se înlocuiește cu următorul text:

„(i) informațiile privind statutul valabilității certificatului calificat sau localizarea serviciilor care pot fi utilizate pentru a cunoaște acest statut;”.

ANEXA IV

În anexa IV, punctul (j) se înlocuiește cu următorul text:

„(j) informațiile privind statutul valabilității certificatului calificat sau localizarea serviciilor responsabile cu statutul valabilității certificatului care pot fi utilizate pentru a cunoaște acest statut;”.

ANEXA V

CERINȚE PENTRU ATESTAREA ELECTRONICĂ CALIFICATĂ A ATRIBUTELOR

Atestarea electronică calificată a atributelor conține:

(e) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, a faptului că atestarea a fost emisă ca atestare electronică calificată a atributelor;

(f) un set de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite atestarea electronică calificată a atributelor, incluzând cel puțin statul membru în care este stabilit prestatorul respectiv și:

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

– în cazul unei persoane fizice: numele persoanei;

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

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

(i) detalii privind începutul și sfârșitul perioadei de valabilitate a atestării;

(j) codul de identificare al atestării, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat și, în cazurile aplicabile, indicarea sistemului de atestări din care face parte atestarea atributelor;

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

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

(m) informații privind statutul valabilității atestării calificate sau localizarea serviciilor care pot fi utilizate pentru a cunoaște acest statut.

ANEXA VI

LISTA MINIMĂ A ATRIBUTELOR

În temeiul articolului 45d, statele membre se asigură că sunt adoptate măsuri pentru a le permite prestatorilor calificați de atestări electronice ale atributelor să verifice prin mijloace electronice, la cererea utilizatorului, autenticitatea următoarelor atribute prin raportare la sursa autentică relevantă de la nivel național, în mod direct sau prin intermediul unor intermediari desemnați recunoscuți la nivel național, în conformitate cu dreptul intern sau cu dreptul Uniunii 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. calificări educaționale, titluri și licențe;
8. calificări profesionale, titluri și licențe;
9. autorizații publice și licențe;
10. date financiare și date privind societatea comercială.

ANEXA VII

CERINȚE PRIVIND ATESTAREA ELECTRONICĂ A ATRIBUTELOR EMISĂ DE UN ORGANISM PUBLIC RESPONSABIL DE O SURSĂ AUTENTICĂ SAU ÎN NUMELE UNUI ASTFEL DE ORGANISM

O atestare electronică a atributelor emisă de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism conține:

a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, a faptului că atestarea a fost emisă ca atestare electronică a atributelor emisă de un organism public responsabil de o sursă autentică sau în numele unui astfel de organism;
b) un set de date care reprezintă fără ambiguitate organismul public care eliberează atestarea electronică a 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 ambiguitate 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 atestării;
f) codul de identificare al atestării, care trebuie să fie unic pentru organismul public emitent și, în cazurile aplicabile, indicarea sistemului de atestări din care face parte atestarea 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) informații privind statutul valabilității atestării sau localizarea serviciilor care pot fi utilizate pentru a cunoaște acest statut.

_____