COMISIA EUROPEANĂ

Bruxelles, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă

(Text cu relevanță pentru SEE)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

Prezenta expunere de motive explică un cadru juridic propus menit să sporească încrederea în tranzacțiile electronice pe piața internă.

Instaurarea încrederii în mediul online este esențială pentru dezvoltarea economică. Lipsa încrederii îi face pe consumatori, întreprinderile și administrațiile să ezite în efectuarea de tranzacții pe cale electronică și în adoptarea de noi servicii.

Agenda digitală pentru Europa[1] identifică obstacolele care stau în prezent în calea dezvoltării digitale a Europei și propune o legislație privind semnăturile electronice (acțiunea cheie nr. 3) și recunoașterea reciprocă a identificării și autentificării electronice (acțiunea cheie nr. 16), stabilind un cadru juridic clar, astfel încât să se elimine fragmentarea și lipsa de interoperabilitate, să se consolideze cetățenia digitală și să se prevină criminalitatea informatică. Legislația care asigură recunoașterea reciprocă a identificării și autentificării electronice în UE și revizuirea directivei privind semnăturile electronice este, de asemenea, o acțiune cheie din *Actul privind piața unică*[2], în vederea realizării pieței unice digitale. *Foaia de parcurs către stabilitate și creștere*[3] subliniază rolul cheie pentru dezvoltarea economiei digitale al viitorului cadru juridic comun pentru recunoașterea și acceptarea reciprocă a identificării și autentificării electronice dincolo de frontiere.

Cadrul juridic propus, constând dintr-un „*Regulament al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă*” urmărește să permită interacțiuni electronice sigure și fără întreruperi între întreprinderi, cetățeni și autoritățile publice, contribuind astfel la creșterea eficienței serviciilor online din sectorul public și privat, a activităților economice electronice și a comerțului electronic în UE.

Legislația UE existentă, și anume Directiva 1999/93/CE privind un „*cadru comunitar pentru semnăturile electronice*”[4], reglementează, în esență, numai semnăturile electronice. Nu există niciun cadru UE transfrontalier și intersectorial cuprinzător pentru tranzacții electronice sigure, demne de încredere și ușor de folosit, care să includă identificarea, autentificarea și semnăturile electronice.

Scopul este de a consolida legislația existentă și de a o extinde pentru a reglementa recunoașterea și acceptarea reciprocă, la nivelul UE, a sistemelor notificate de identificare electronică și a altor servicii de asigurare a încrederii electronice conexe esențiale.

2. REZULTATELE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

Această inițiativă este rezultatul consultărilor extinse asupra unei revizuiri a cadrului juridic actual privind semnăturile electronice în cursul cărora Comisia a colectat reacții din partea statelor membre, a Parlamentului European și a altor părți interesate[5]. Consultarea publică online a fost completată de un „Grup de consultare a IMM-urilor” pentru a identifica punctele

---

1 COM(2010) 245, 19.5.2010.

2 COM(2011) 206 final, 13.4.2011

3 COM(2011) 669, 12.10.2011.

4 JO L 13, 19.1.2000, p. 12.

5 Pentru detalii privind consultările, a se vedea http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

de vedere și nevoile specifice ale IMM-urilor și de alte consultări pe teme specifice cu părțile interesate[6,7] Comisia a lansat, de asemenea, o serie de studii în ceea ce privește identificarea, autentificarea și semnătura electronică și serviciile conexe de asigurare a încrederii.

Consultările au indicat în mod clar că majoritatea părților interesate a fost de acord că este nevoie să se revizuiască actualul cadru pentru a umple golurile lăsate de directiva privind semnătura electronică. S-a considerat că acest lucru ar răspunde mai bine provocărilor reprezentate de dezvoltarea rapidă a noilor tehnologii (în special accesul online și mobil) și de amplificarea globalizării, menținând, în același timp, neutralitatea tehnologică a cadrului juridic.

În conformitate cu politica sa pentru „o mai bună legiferare", Comisia a realizat o evaluare a impactului în ceea ce privește alternativele strategice. Au fost evaluate trei serii de opțiuni strategice, referitoare respectiv la (1) domeniul de aplicare al noului cadru, (2) instrumentul juridic și (3) nivelul de supraveghere necesar[8]. Opțiunea strategică preferată s-a dovedit a fi consolidarea securității juridice, stimularea coordonării supravegherii naționale, garantarea recunoașterii și acceptării reciproce a sistemelor de identificare electronică și încorporarea serviciilor conexe esențiale de asigurare a încrederii. Evaluarea impactului a concluzionat că aceasta ar duce la îmbunătățiri considerabile privind securitatea juridică, securitatea și încredere în ceea ce privește tranzacțiile electronice transfrontaliere, ceea ce ar avea drept rezultat o fragmentare mai diminuată a pieței.

3. ELEMENTELE JURIDICE ALE PROPUNERII

3.1 Temei juridic

Prezenta propunere se bazează pe articolul 114 din TFUE, care se referă la adoptarea de norme menite să înlăture barierele existente în calea funcționării pieței interne. Cetățenii, întreprinderile și administrațiile vor putea beneficia de recunoașterea și acceptarea reciprocă a identificării, autentificării și semnăturilor electronice și ale altor servicii de asigurare a încrederii dincolo de frontiere atunci când sunt necesare pentru accesarea și finalizarea procedurilor sau tranzacțiilor electronice.

Se consideră că un regulament este instrumentul juridic cel mai potrivit. Aplicabilitatea directă a unui regulament în temeiul articolului 288 din TFUE va reduce fragmentarea juridică și va oferi mai multă securitate juridică prin introducerea unui ansamblu armonizat de reguli de bază care va contribui la funcționarea pieței interne.

---

6 La 10.3.2011 a fost organizat un atelier cu părțile interesate, la care au participat reprezentanți din sectorul public, sectorul privat și din mediul academic pentru a discuta ce măsuri legislative sunt necesare pentru abordarea provocărilor viitoare. Acesta a fost un forum interactiv pentru a schimba opinii și pentru a marca diferitele poziții privind temele abordate în timpul consultării publice. Mai multe organizații au trimis spontan documente în care și-au exprimat poziția.

7 Președinția poloneză a UE, în special, a organizat o reuniune cu statele membre privind semnătura electronică la Varșovia la 9.11.2011 și privind identificarea electronică la Poznan la 17.11.2011. La 25.1.2012, Comisia a convocat un atelier cu statele membre pentru a discuta chestiunile nesoluționate cu privire la identificarea, autentificarea și semnăturile electronice.

8 În prima serie, au fost examinate patru opțiuni: abrogarea directivei privind semnătura electronică; nicio modificare a politicii; consolidarea securității juridice, stimularea coordonării supravegherii naționale și garantarea recunoașterii și acceptării reciproce a identificării electronice în întreaga UE; și în al patrulea rând, o extindere pentru a încorpora anumite servicii conexe de asigurare a încrederii. A doua serie a constat în evaluarea meritelor relative ale oportunităților de reglementare prin unul sau două instrumente și printr-o directivă în locul unui regulament. A treia serie a examinat posibilitățile oferite de punerea în aplicare sistemelor naționale de supraveghere bazate pe cerințe esențiale comune de supraveghere în locul unui sistem de supraveghere la nivelul UE. Cu ajutorul unui grup care a reunit toate direcțiile generale interesate ale Comisiei, fiecare opțiune strategică a fost evaluată în ceea ce privește eficacitatea sa în realizarea obiectivelor strategice, impactul său economic asupra părților interesate (inclusiv asupra bugetului instituțiilor UE), impactul său social și la nivelul mediului și efectul său asupra sarcinii administrative.

3.2 Subsidiaritate și proporționalitate

Pentru ca acțiunea UE să fie justificată, trebuie respectat principiul subsidiarității:

a) Natura transnațională a problemei (criteriul necesității)

Natura transnațională a identificării, autentificării și semnăturii electronice și a serviciilor conexe de asigurare a încrederii necesită o acțiune la nivelul UE. Doar acțiunea internă (adică națională) nu ar fi suficientă pentru îndeplinirea obiectivelor și a țintelor fixate în *Strategia Europa 2020*[9]. Dimpotrivă, experiența a arătat că măsurile naționale au creat obstacole, în fapt, în calea interoperabilității semnăturilor electronice la nivelul UE și că acestea au în prezent același efect asupra identificării electronice, autentificării electronice și serviciilor conexe de asigurare a încrederii. Prin urmare, este necesar ca UE să creeze un cadru favorabil abordării interoperabilității transfrontaliere și să îmbunătățească coordonarea sistemelor de supraveghere naționale. Cu toate acestea, identificarea electronică nu poate fi abordată în propunerea de regulament în mod generic, ca celelalte servicii electronice de asigurare a încrederii, deoarece emiterea de mijloace de identificare este o prerogativă națională. Prin urmare, propunerea se concentrează în mod strict pe aspectele transfrontaliere ale identificării electronice.

Regulamentul propus creează condiții de concurență echitabile pentru întreprinderile care prestează servicii de asigurare a încrederii având în vedere că diferențele existente în prezent în legislația națională conduc deseori la incertitudine juridică și la sarcini suplimentare. Securitatea juridică este sporită în mod semnificativ prin obligația de a accepta în mod clar a statelor membre a serviciilor calificate de asigurare a încrederii care vor crea stimulente suplimentare pentru ca întreprinderile să își desfășoare activitatea în străinătate. De exemplu, o societate va fi în măsură să participe în mod electronic la o licitație publică lansată de administrația unui alt stat membru fără ca semnătura sa electronică să fie blocată din cauza unor cerințe naționale specifice și a unor probleme de interoperabilitate. În mod similar, o societate va avea posibilitatea să semneze contracte în mod electronic cu o societate echivalentă cu sediul într-un alt stat membru fără să se teamă că va trebui să respecte cerințe juridice diferite pentru servicii de asigurare a încrederii cum ar fi sigiliile electronice, documentele electronice sau marcarea temporală. De asemenea, scrisorile de punere în întârziere vor fi trimise dintr-un stat membru într-altul având certitudinea valabilității lor juridice în ambele state membre. În sfârșit, comerțul online va fi mai demn de încredere atunci când cumpărătorii vor putea verifica dacă accesează într-adevăr site-ul internet al comerciantului pe care îl aleg și nu un site internet care poate să fie fals.

Mijloacele de identificare electronică recunoscute reciproc și semnăturile electronice larg acceptate vor facilita prestarea transfrontalieră a numeroase servicii de pe piața internă și vor permite întreprinderilor să se extindă dincolo de granițe fără să se confrunte cu obstacole în interacțiunile cu autoritățile publice. În practică, aceasta va însemna îmbunătățiri semnificative ale eficienței atât pentru întreprinderi, cât și pentru cetățeni atunci când se conformează formalităților administrative. De exemplu, va exista posibilitatea ca un student să se înscrie în mod electronic în cadrul unei universități din străinătate, un cetățean să prezinte declarații fiscale online într-un alt stat membru sau un pacient să își acceseze online datele privind sănătatea. În cazul în care nu există astfel de mijloace de identificare electronică recunoscute reciproc, un medic nu va putea accesa datele medicale ale unui pacient necesare pentru a-l trata, iar testele medicale și de laborator pe care pacientul le-a efectuat deja vor trebui să fie repetate.

[9] Comunicarea Comisiei: Europa 2020. O strategie europeană pentru o creștere inteligentă, durabilă și favorabilă incluziunii COM(2010) 2020, 3.3.2010.

b) Valoarea adăugată (criteriul eficacității)

Obiectivele prezentate anterior nu sunt în prezent atinse prin coordonarea voluntară între statele membre și este puțin probabil ca acest lucru să se întâmple în viitor. Acest lucru conduce la dublarea eforturilor, stabilirea de standarde diferite, caracteristici transnaționale ale repercusiunilor generate de TIC și complexitatea administrativă de a stabili o astfel de coordonare prin intermediul unor acorduri bilaterale și multilaterale.

În plus, necesitatea de a depăși astfel de probleme, precum (a) o lipsă de securitate juridică din cauza dispozițiilor naționale eterogene care provin din interpretări divergente ale directivei privind semnătura electronică și (b) o lipsă de interoperabilitate a sistemelor de semnături electronice instituite la nivel național din cauza aplicării neuniforme a standardelor tehnice necesită un tip de coordonare între statele membre ale UE care se poate realiza mai eficient la nivelul UE.

3.3. Explicarea detaliată a propunerii

3.3.1 CAPITOLUL I - DISPOZIȚII GENERALE

Articolul 1 definește obiectul regulamentului.

Articolul 2 definește domeniul de aplicare material al regulamentului.

Articolul 3 conține definițiile termenilor utilizați în regulament. Unele definiții sunt preluate din Directiva 1999/93/CE, altele sunt clarificate, completate cu elemente suplimentare sau sunt nou introduse.

Articolul 4 definește principiile pieței interne cu privire la aplicarea teritorială a regulamentului. Se menționează în mod explicit că nu se impun restricții privind libertatea de a presta servicii și libera circulație a produselor.

3.3.2 CAPITOLUL II – IDENTIFICARE ELECTRONICĂ

Articolul 5 prevede recunoașterea și acceptarea reciprocă a mijloacelor de identificare electronică care intră sub incidența unui sistem care va fi notificat Comisiei în condițiile prevăzute în regulament. Majoritatea statelor membre ale UE au introdus, într-o formă sau alta, un sistem de identificare electronică. Cu toate acestea, ele sunt diferite din multe puncte de vedere. Lipsa unei baze juridice comune care să impună fiecărui stat membru recunoașterea și acceptarea mijloacelor de identificare electronică emise în alte state membre pentru a accesa serviciile online, precum și interoperabilitatea transfrontalieră inadecvată a identificărilor electronice naționale creează bariere care împiedică cetățenii și întreprinderile să beneficieze pe deplin de piața unică digitală. Recunoașterea și acceptarea reciprocă a oricărui mijloc de identificare electronică care intră sub incidența unui sistem notificat în temeiul prezentului regulament înlătură aceste obstacole juridice.

Regulamentul nu obligă statele membre să introducă sau să notifice sisteme de identificare electronică, ci să recunoască și să accepte identificări electronice notificate pentru serviciile online în cazul cărora identificarea electronică este necesară pentru a fi accesate la nivel național. Creșterea potențială a economiilor de scară create prin utilizarea transfrontalieră a mijloacelor de identificare electronică notificate și a sistemelor de autentificare poate stimula statele membre să notifice sistemele lor de identificare electronică. Articolul 6 stabilește cele cinci condiții pentru notificarea sistemelor de identificare electronică:

Statele membre pot notifica sistemele de identificare electronică pe care le acceptă sub jurisdicția lor în cazul în care identificarea electronică este necesară pentru serviciile publice. O cerință suplimentară este ca mijloacele respective de identificare electronică să fie emise de către, în numele sau cel puțin sub responsabilitatea statului membru care notifică un sistem.

Statele membre trebuie să asigure o legătură lipsită de ambiguitate între datele privind identificarea electronică și persoana în cauză. Această obligație nu înseamnă că o persoană nu poate dispune de mai multe mijloace de identificare electronică, dar toate trebuie să trimită către aceeași persoană.

Fiabilitatea unei identificări electronice depinde de disponibilitatea mijloacelor de autentificare (și anume posibilitatea de a verifica valabilitatea datelor privind identificarea electronică). Regulamentul obligă statele membre care notifică să furnizeze autentificare online gratuită părților terțe. Posibilitatea de autentificare trebuie să fie disponibilă fără întrerupere. Nu pot fi impuse cerințe tehnice specifice, precum hardware sau software, părților care recurg la o astfel de autentificare. Această dispoziție nu se aplică niciunei cerințe față de utilizatorii (deținătorii) mijloacelor de identificare electronică care sunt necesare din punct de vedere tehnic pentru utilizarea mijloacelor de identificare electronică, precum dispozitivele de citire a cardurilor.

Statele membre trebuie să accepte răspunderea pentru lipsa de ambiguitate a legăturii (și anume că datele privind identificarea atribuite persoanei nu trimit la nicio altă persoană) și posibilitatea de autentificare (și anume posibilitatea de a verifica valabilitatea datelor privind identificarea electronică). Răspunderea statelor membre nu vizează alte aspecte ale procesului de identificare și nici alte tranzacții care necesită identificare.

Articolul 7 cuprinde norme privind notificarea Comisiei cu privire la sistemele de identificare electronică.

Articolul 8 are scopul de a asigura interoperabilitatea tehnică a sistemelor de identificare notificate printr-o abordare de coordonare, inclusiv prin actele delegate.

3.3.3 CAPITOLUL III – SERVICII DE ASIGURARE A ÎNCREDERII

3.3.3.1 Secțiunea 1 – Dispoziții generale

Articolul 9 stabilește principiile referitoare la răspunderea prestatorilor de servicii de asigurare a încrederii calificați și necalificați. El se bazează pe articolul 6 din Directiva 1999/93/CE și extinde dreptul la despăgubiri la daunele cauzate de orice prestator neglijent de servicii de asigurare a încrederii care nu a respectat bunele practici de securitate, ceea ce rezultă într-o încălcare a securității care are un impact important asupra serviciului.

Articolul 10 descrie mecanismul de recunoaștere și acceptare a serviciilor calificate de asigurare a încrederii oferite de un prestator stabilit într-o țară terță. Acesta se bazează pe articolul 7 din Directiva 1999/93/CE, dar reține doar singura opțiune care este posibilă din punct de vedere practic, și anume de a permite o astfel de recunoaștere în conformitate cu un acord internațional între Uniunea Europeană și țări terțe sau organizații internaționale.

Articolul 11 stabilește principiile de protecție și minimizare a datelor. Acesta se bazează pe articolul 8 din Directiva 1999/93/CE.

Articolul 12 prevede că serviciile de asigurare a încrederii trebuie să fie accesibile persoanelor cu handicap.

3.3.3.2 Secțiunea 2 – Supraveghere

Articolul 13 obligă statele membre să instituie organisme de supraveghere, pe baza articolului 3 alineatul (3) din Directiva 1999/93/CE, clarificând și lărgind mandatul acestora cu privire la prestatorii de servicii de asigurare a încrederii și la prestatorii de servicii de asigurare a încrederii calificați.

Articolul 14 introduce un mecanism explicit de asistență reciprocă între organismele de supraveghere din statele membre pentru a facilita supravegherea transfrontalieră a prestatorilor de servicii de asigurare a încrederii. Acesta introduce reguli privind operațiunile comune și dreptul autorităților de supraveghere de a participa la astfel de operațiuni.

Articolul 15 introduce o obligație atât pentru prestatorii de servicii de asigurare a încrederii calificați, cât și pentru cei necalificați, de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura securitatea activităților lor. Mai mult, organismele de supraveghere competente și alte autorități relevante trebuie să fie informate cu privire la orice încălcare a securității. Dacă este cazul, acestea vor informa, la rândul lor, celelalte organisme de supraveghere ale statelor membre și vor informa publicul, direct sau prin intermediul prestatorului de servicii de asigurare a încrederii în cauză.

Articolul 16 stabilește condițiile pentru supravegherea prestatorilor de servicii de asigurare a încrederii calificați și a serviciilor calificate de asigurare a încrederii prestate de aceștia. Acesta obligă prestatorii de servicii de asigurare a încrederii calificați să fie auditați anual de un organism independent recunoscut, pentru a confirma organismului de supraveghere că îndeplinesc obligațiile prevăzute în regulament. Mai mult, articolul 16 alineatul (2) acordă organismului de supraveghere dreptul de a efectua, în orice moment, audituri la fața locului ale prestatorilor de servicii de asigurare a încrederii calificați. Organismul de supraveghere este, de asemenea, împuternicit să emită instrucțiuni obligatorii pentru ca prestatorii de servicii de asigurare a încrederii calificați să remedieze, în mod proporțional, orice nerespectare a unei obligații indicată de un audit privind securitatea.

Articolul 17 se referă la activitatea desfășurată de către organismul de supraveghere la solicitarea unui prestator de servicii de asigurare a încrederii care dorește să inițieze un serviciu de asigurare a încrederii calificat.

Articolul 18 prevede instituirea de liste sigure[10] care conțin informații referitoare la prestatorii de servicii de asigurare a încrederii calificați care fac obiectul supravegherii și la serviciile calificate pe care le oferă. Aceste informații trebuie să fie puse la dispoziția publicului prin intermediul unui model comun, pentru a facilita utilizarea lor automată și pentru a asigura un nivel adecvat de detaliere.

Articolul 19 stabilește cerințele pe care trebuie să le îndeplinească prestatorii de servicii de asigurare a încrederii calificați pentru a fi recunoscuți ca atare. Acesta se inspiră din anexa II la Directiva 1999/93/CE.

3.3.3.3 Secțiunea 3 – Semnătura electronică

[10] Lista sigură, astfel cum a fost instituită prin Decizia 2009/767/CE a Comisiei, astfel cum a fost modificată prin Decizia 2010/425/UE a Comisiei, trebuie să fie baza pentru o nouă decizie a Comisiei privind listele sigure în temeiul prezentului regulament.

Articolul 20 consacră normele referitoare la efectul juridic al semnăturilor electronice ale persoanelor fizice. Acesta clarifică şi extinde articolul 5 din Directiva 1999/93/CE, introducând obligaţia explicită de a da semnăturilor electronice calificate acelaşi efect juridic pe care îl au semnăturile olografe. Mai mult, statele membre trebuie să asigure acceptarea transfrontalieră a semnăturilor electronice calificate, în contextul prestării de servicii publice şi nu trebuie să introducă cerinţe suplimentare care ar putea duce la obstacole în calea utilizării acestor semnături.

Articolul 21 stabileşte cerinţele pentru certificatele de semnături calificate. Acesta clarifică anexa I la Directiva 1999/93/CE şi elimină dispoziţiile care nu au funcţionat în practică (de exemplu, limitările privind valoarea tranzacţiilor).

Articolul 22 stabileşte cerinţele pentru dispozitivele de creare a semnăturilor electronice calificate. Acesta clarifică cerinţele referitoare la dispozitivele sigure de creare a semnăturilor prevăzute la articolul 3 alineatul (5) din Directiva 1999/93/CE, care trebuie acum să fie considerate dispozitive de creare a semnăturilor calificate în temeiul prezentului regulament. De asemenea, acesta indică în mod clar că definiţia unui dispozitiv de creare a semnăturilor poate fi mult mai largă şi nu se limitează doar la datele de creare a semnăturilor. Comisia poate, de asemenea, să întocmească o listă de numere de referinţă ale standardelor pentru cerinţele în materie de securitate privind dispozitivele.

Articolul 23, care se întemeiază pe articolul 3 alineatul (4) din Directiva 1999/93/CE, introduce conceptul de certificare a dispozitivelor de semnături electronice calificate pentru a determina conformitatea acestora cu cerinţele de securitate prevăzute în anexa II. Toate statele membre trebuie să recunoască că aceste dispozitive îndeplinesc cerinţele în cazul în care se realizează o procedură de certificare de către un organism de certificare desemnat de un stat membru. Comisia va publica o listă pozitivă a acestor dispozitive certificate în conformitate cu articolul 24. Comisia poate, de asemenea, să întocmească o listă de numere de referinţă ale standardelor pentru evaluarea securităţii produselor tehnologiei informaţiei menţionate la articolul 23 alineatul (1).

Articolul 24 se referă la publicarea de către Comisie a unei liste de dispozitive de creare a semnăturilor electronice calificate după notificarea conformităţii de către statele membre.

Articolul 25 se bazează pe recomandările din anexa IV la Directiva 1999/93/CE pentru a stabili cerinţe obligatorii pentru validarea semnăturilor electronice calificate, în vederea sporirii securităţii juridice a unei astfel de validări.

Articolul 26 stabileşte condiţiile pentru serviciile de validare calificate.

Articolul 27 stabileşte condiţiile pentru păstrarea pe termen lung a semnăturilor electronice calificate. Acest lucru este posibil datorită utilizării procedurilor şi tehnologiilor capabile să extindă fiabilitatea datelor de validare a semnăturilor electronice calificate după expirarea valabilităţii lor tehnologice, când falsificarea poate deveni uşor de realizat pentru infractorii informatici.

3.3.3.4 Secţiunea 4 – Sigiliile electronice

Articolul 28 se referă la efectul juridic al sigiliilor electronice ale persoanelor juridice. Se acordă o prezumţie juridică specifică unui sigiliu electronic calificat care garantează originea şi integritatea documentelor electronice de care este legat.

Articolul 29 stabilește cerințele pentru certificatele calificate pentru sigilii electronice.

Articolul 30 stabilește cerințele pentru certificarea și publicarea listei pentru dispozitivele de creare a sigiliilor electronice calificate.

Articolul 31 stabilește condițiile de validare și păstrare a sigiliilor electronice calificate.

3.3.3.5 Secțiunea 5 – Marca temporală electronică

Articolul 32 se referă la efectul juridic al mărcilor temporale electronice. Se acordă o prezumție juridică specifică mărcilor temporale electronice calificate în ceea ce privește exactitatea temporală.

Articolul 33 stabilește cerințele pentru mărcile temporale electronice calificate.

3.3.3.6 Secțiunea 6 – Documentele electronice

Articolul 34 se referă la efectele juridice și la condițiile de acceptare a documentelor electronice. Există o prezumție juridică specifică a autenticității și integrității oricărui document electronic semnat cu o semnătură electronică calificată sau care poartă un sigiliu electronic calificat. Cu privire la acceptarea documentelor electronice, atunci când este nevoie de un document original sau de o copie certificată pentru prestarea unui serviciu public, sunt acceptate în alte state membre fără cerințe suplimentare cel puțin documentele electronice emise de persoanele care sunt competente să emită documentele relevante și care sunt considerate a fi originale sau copii certificate în conformitate cu legislația națională a statului membru de origine.

3.3.3.7 Secțiunea 7 – Servicii de distribuție electronică

Articolul 35 se referă la efectul juridic al datelor trimise sau primite folosind un serviciu de distribuție electronică. Se garantează o prezumție juridică specifică pentru serviciile de distribuție electronică calificate, privind integritatea datelor care sunt trimise sau primite și exactitatea momentului în care datele sunt trimise sau primite. Aceasta asigură, de asemenea, recunoașterea reciprocă a serviciilor de distribuție electronică calificate la nivelul UE.

Articolul 36 stabilește cerințele pentru serviciile de distribuție electronică calificate.

3.3.3.8 Secțiunea 8 – Autentificarea unui site internet

Scopul acestei secțiuni este de a se asigura ca autenticitatea unui site internet cu privire la proprietarul site-ului va fi garantată.

Articolul 37 stabilește cerințele pentru certificatele calificate pentru autentificarea unui site internet, care pot fi utilizate pentru a garanta autenticitatea unui site internet. Un certificat calificat pentru autentificarea unui site internet va furniza un set minim de informații demne de încredere privind site-ul internet și existența juridică a proprietarului acestuia.

3.3.4 CAPITOLUL IV – ACTE DELEGATE

Articolul 38 conține dispozițiile standard pentru exercitarea delegărilor în conformitate cu articolul 290 din TFUE (acte delegate). Acesta permite organului legislativ să delege Comisiei

competența de a adopta acte fără caracter legislativ și cu domeniu de aplicare general care completează sau modifică anumite elemente neesențiale ale unui act legislativ.

3.3.5 CAPITOLUL V – ACTE DE PUNERE ÎN APLICARE

Articolul 39 cuprinde dispoziții care vizează procedura comitetului necesară pentru a se acorda Comisiei competențe de executare de fiecare dată când, în conformitate cu articolul 291 din TFUE, sunt necesare condiții unitare de punere în aplicare a actelor obligatorii din punct de vedere juridic ale Uniunii. În acest caz, se aplică procedura de examinare.

3.3.6 CAPITOLUL VI - DISPOZIȚII FINALE

Articolul 40 prevede obligația Comisiei de a evalua regulamentul și de a prezenta rapoarte cu privire la constatările sale.

Articolul 41 abrogă Directiva 1999/93/CE și prevede o tranziție armonioasă a infrastructurii existente privind semnăturile electronice la noile cerințe ale regulamentului.

Articolul 42 stabilește data intrării în vigoare a regulamentului.

4. IMPLICAȚII BUGETARE

Implicațiile bugetare specifice ale propunerii se referă la sarcinile atribuite Comisiei Europene astfel cum se specifică în fișele financiare legislative care însoțesc prezenta propunere.

Propunerea nu are implicații asupra cheltuielilor operaționale.

Fișa financiară legislativă care însoțește prezenta propunere de regulament vizează implicațiile bugetare pentru regulamentul în sine.

2012/0146 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ŞI 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[11],

după consultarea Autorității Europene pentru Protecția Datelor[12],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Instaurarea încrederii în mediul online este esențială pentru dezvoltarea economică. Lipsa încrederii determină consumatorii, întreprinderile și administrațiile să ezite în efectuarea de tranzacții pe cale electronică și în adoptarea de noi servicii.

(2) Obiectivul prezentului regulament este de a crește încrederea în tranzacțiile electronice de pe piața internă prin permiterea realizării de interacțiuni electronice sigure și fără întreruperi între întreprinderi, cetățeni și autoritățile publice, contribuind astfel la creșterea eficienței serviciilor online din sectorul public și privat, a activităților economice electronice și a comerțului electronic în Uniune.

(3) Directiva 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice[13] reglementa, în esență, semnăturile electronice fără să ofere un cadru transfrontalier și intersectorial cuprinzător pentru tranzacții electronice sigure, demne de încredere și ușor de folosit. Prezentul regulament consolidează și extinde *acquis*-ul din directivă.

11 JO C , , p. .

12 JO C , , p. .

13 JO L 13, 19.1.2000, p. 12.

(4) Agenda digitală pentru Europa a Comisiei[14] a identificat fragmentarea pieței digitale, lipsa interoperabilității și creșterea criminalității informatice ca obstacole majore în calea cercului virtuos al economiei digitale. În raportul său privind cetățenia în 2010, Comisia a scos în evidență, de asemenea, necesitatea de a soluționa principalele probleme care îi împiedică pe cetățenii europeni să beneficieze de avantajele unei piețe unice digitale și de serviciile digitale transfrontaliere[15].

(5) Consiliul European a invitat Comisia să creeze o piață unică digitală până în 2015[16] pentru a realiza progrese rapide în domenii esențiale ale economiei digitale și pentru a promova o piață unică digitală integrată în totalitate[17], prin facilitarea utilizării transfrontaliere a serviciilor online, acordând atenție în special facilitării identificării și autentificării electronice sigure.

(6) Consiliul a invitat Comisia să contribuie la piața unică digitală prin crearea condițiilor adecvate pentru recunoașterea reciprocă a elementelor cheie dincolo de frontiere, cum ar fi identificarea electronică, documentele electronice, semnăturile electronice și serviciile de distribuție electronică, precum și pentru serviciile de e-guvernare interoperabile pe întreg teritoriul Uniunii Europene[18].

(7) Parlamentul European a subliniat importanța securității serviciilor electronice, în special a semnăturilor electronice și importanța necesității de a crea o infrastructură publică cheie la nivel paneuropean și a solicitat Comisiei să creeze un portal european al autorităților de validare pentru a asigura interoperabilitatea transfrontalieră a semnăturilor electronice și pentru a crește gradul de securitate a tranzacțiilor efectuate prin intermediul internetului[19].

(8) Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne[20] solicită statelor membre să instituie „ghișee unice” pentru a se asigura că toate procedurile și formalitățile cu privire la accesul la o activitate de servicii și la exercitarea acesteia pot fi îndeplinite cu ușurință, de la distanță și prin mijloace electronice, prin intermediul ghișeului unic adecvat și al autorităților adecvate. Multe servicii online accesibile prin intermediul ghișeelor unice necesită identificare, autentificare și semnătură electronică.

(9) În majoritatea cazurilor, prestatorii de servicii din alt stat membru nu își pot utiliza identificarea electronică pentru a accesa aceste servicii din cauza că sistemele naționale de identificare electronică din țara lor nu sunt recunoscute și acceptate în alte state membre. Această barieră electronică împiedică prestatorii de servicii să se bucure pe deplin de avantajele oferite de piața internă. Mijloacele de identificare electronică recunoscute și acceptate reciproc vor facilita prestarea transfrontalieră de numeroase servicii în piața internă și vor permite întreprinderilor să își extindă activitatea peste granițe fără să se confrunte cu multe obstacole în interacțiunile cu autoritățile publice.

---

14 COM(2010) 245 final/2

15 Raport privind cetățenia UE în 2010: Eliminarea obstacolelor din calea drepturilor cetățenilor UE, COM(2010) 603 final, punctul 2.2.2, pagina 13.

16 4/2/2011: EUCO 2/1/11.

17 23/10/2011: EUCO 52/1/11.

18 Concluziile Consiliului privind Planul european de acțiune privind guvernarea electronică 2011-2015, a 3093-a reuniune a Consiliului pentru transporturi, telecomunicații și energie, Bruxelles, 27 mai 2011.

19 Rezoluția Parlamentului European din 21.9.2010 privind realizarea pieței interne pentru comerțul electronic, 21.9.10, P7_TA(2010)0320 și rezoluția Parlamentului European din 15.6.2010 referitoare la guvernarea internetului: următoarele etape, P7_TA(2010)0208.

20 JO L 376, 27.12.2006, p. 36.

(10) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere[21] instituie o rețea de autorități naționale responsabile pentru e-sănătate. Pentru a spori siguranța și continuitatea asistenței medicale transfrontaliere, rețeaua trebuie să elaboreze orientări privind accesul transfrontalier la datele și serviciile legate de e-sănătate, inclusiv prin sprijinirea de *„măsuri comune de identificare și de autentificare pentru a facilita transferabilitatea datelor în cadrul asistenței medicale transfrontaliere”*. Recunoașterea și acceptarea reciprocă a identificării și autentificării electronice sunt esențiale pentru ca asistența medicală transfrontalieră pentru cetățenii europeni să devină o realitate. Când oamenii călătoresc în scopul realizării unui tratament, datele lor medicale trebuie să fie accesibile în țara în care se realizează tratamentul. Acest lucru necesită un cadru de identificare electronică solid, sigur și fiabil.

(11) Unul din obiectivele prezentului regulament este de a elimina barierele existente în calea utilizării transfrontaliere a mijloacelor de identificare electronică utilizate în statele membre pentru a accesa cel puțin serviciile publice. Prezentul regulament nu are drept obiectiv să intervină în sistemele de gestionare a identității electronice și infrastructurile conexe stabilite în statele membre. Obiectivul prezentului regulament este de a garanta că, pentru accesul la serviciile transfrontaliere online oferite de către statele membre, este posibilă identificarea și autentificarea electronică sigură.

(12) Statele membre ar trebui să dispună în continuare de libertatea de a utiliza sau de a introduce, în scopuri de identificare electronică, mijloace pentru accesarea serviciilor online. Acestea ar trebui, de asemenea, să fie în măsură să decidă dacă să implice sectorul privat în furnizarea acestor mijloace. Statele membre nu ar trebui să fie obligate să notifice sistemele lor de identificare electronică. Alegerea de a notifica fie toate, unele sau niciunul din sistemele de identificare electronică utilizate la nivel național pentru a accesa cel puțin serviciile publice online sau serviciile specifice este la latitudinea statelor membre.

(13) Trebuie să fie stabilite în regulament unele condiții cu privire la mijloacele de identificare electronică care trebuie să fie acceptate și la modul în care sistemele ar trebui să fie notificate. Acestea ar trebui să ajute statele membre să dobândească încrederea reciprocă necesară în sistemele lor de identificare electronică și să recunoască și să accepte reciproc mijloacele de identificare electronică care intră sub incidența sistemelor lor notificate. Ar trebui să se aplice principiul recunoașterii și acceptării reciproce în cazul în care statul membru care notifică îndeplinește condițiile de notificare, iar notificarea a fost publicată în Jurnalul Oficial al Uniunii Europene. Totuși, accesul la aceste servicii online și furnizarea lor finală către solicitant ar trebui să fie strâns legate de dreptul de a primi astfel de servicii în condițiile stabilite de legislația națională.

(14) Statele membre ar trebui să fie în măsură să decidă să implice sectorul privat în emiterea de mijloace de identificare electronică și să permită sectorului privat să utilizeze mijloace de identificare electronică în cadrul unui sistem notificat, în scopuri de identificare, atunci când este nevoie pentru servicii online sau tranzacții electronice. Posibilitatea de a utiliza aceste mijloace de identificare electronică ar permite sectorului privat să se bazeze pe identificarea și autentificarea electronică deja utilizată

[21] JO L 88, 4.4.2011, p. 45.

pe scară largă în multe state membre cel puțin pentru serviciile publice și să faciliteze accesul întreprinderilor și cetățenilor la serviciile lor online dincolo de frontiere. Pentru a facilita utilizarea acestor mijloace de identificare electronică dincolo de frontiere de către sectorul privat, posibilitatea de autentificare furnizată de statele membre ar trebui să fie disponibilă beneficiarilor, fără discriminări între sectorul public sau privat.

(15) Utilizarea transfrontalieră a mijloacelor de identificare electronică în cadrul unui sistem notificat necesită cooperarea statelor membre în vederea realizării interoperabilității tehnice. Aceasta exclude orice norme tehnice naționale specifice care solicită, de exemplu, părților din alte țări să obțină hardware sau software specific pentru a verifica și valida identificarea electronică notificată. Cerințele tehnice privind utilizatorii, pe de altă parte, care decurg din specificațiile intrinsece referitoare la tipul de dispozitiv „token" care este utilizat (de exemplu, cardurile cu memorie) sunt inevitabile.

(16) Cooperarea statelor membre ar trebui să contribuie la interoperabilitatea tehnică a sistemelor de identificare electronică notificate pentru a stimula un nivel ridicat de încredere și securitate corespunzător gradului de risc. Schimbul de informații și de cele mai bune practici între statele membre, în vederea recunoașterii lor reciproce, ar trebui să contribuie la această cooperare.

(17) Prezentul regulament ar trebui, de asemenea, să stabilească un cadru juridic general pentru utilizarea serviciilor electronice de asigurare a încrederii. Totuși, el nu ar trebui să creeze o obligație generală de a le utiliza. În special, regulamentul nu ar trebui să reglementeze prestarea de servicii bazate pe acorduri voluntare de drept privat, nici aspecte privind încheierea și valabilitatea contractelor sau a altor obligații juridice, în cazul în care există cerințe cu privire la formă prevăzute de legislația națională sau a Uniunii.

(18) Pentru a contribui la utilizarea transfrontalieră generală a serviciilor electronice de asigurare a încrederii, ar trebui să fie posibilă utilizarea acestora ca probe în procedurile judiciare în toate statele membre.

(19) Statele membre ar trebui să dispună în continuare de libertatea de a defini alte tipuri de servicii de asigurare a încrederii, în plus față de cele care fac parte din lista închisă de servicii de asigurare a încrederii prevăzută în prezentul regulament, în scopul recunoașterii la nivel național ca servicii calificate de asigurare a încrederii.

(20) Datorită ritmului schimbărilor tehnologice, prezentul regulament ar trebui să adopte o abordare deschisă inovațiilor.

(21) Prezentul regulament ar trebui să fie neutru din punct de vedere al tehnologiei. Efectele juridice pe care le acordă ar trebui să fie realizabile prin orice mijloc tehnic, cu condiția ca cerințele prezentului regulament să fie îndeplinite.

(22) Pentru a spori încrederea cetățenilor în piața internă și pentru a promova utilizarea serviciilor și produselor de asigurare a încrederii, noțiunile de servicii calificate de asigurare a încrederii și prestator de servicii de asigurare a încrederii calificat ar trebui să fie introduse pentru a indica cerințele și obligațiile de a asigura securitatea la nivel înalt a oricăror servicii și produse calificate de asigurare a încrederii utilizate sau furnizate.

(23) În conformitate cu obligațiile în temeiul Convenției Națiunilor Unite privind drepturile persoanelor cu handicap, care a intrat în vigoare în UE, persoanele cu handicap ar trebui să aibă posibilitatea de a utiliza serviciile de asigurare a încrederii și produsele destinate utilizatorului final utilizate la prestarea serviciilor respective, în aceleași condiții ca și ceilalți consumatori.

(24) Un prestator de servicii de asigurare a încrederii este un operator al datelor cu caracter personal și, prin urmare, trebuie să respecte obligațiile prevăzute de Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[22]. În special colectarea de date ar trebui să fie minimizată cât se poate de mult, ținând cont de scopul serviciului prestat.

(25) Organismele de supraveghere ar trebui să coopereze și să facă schimb de informații cu autoritățile pentru protecția datelor, pentru a asigura punerea în aplicare corespunzătoare a legislației privind protecția datelor de către prestatorii de servicii. Schimbul de informații ar trebui să vizeze în special incidentele privind securitatea și încălcarea securității datelor cu caracter personal.

(26) Ar trebui să fie obligatoriu pentru toți prestatorii de servicii de asigurare a încrederii să aplice bune practici de securitate corespunzătoare riscurilor legate de activitățile lor, pentru a spori încrederea utilizatorilor în piața unică.

(27) Dispozițiile privind utilizarea pseudonimelor în certificate nu trebuie să împiedice statele membre să solicite identificarea persoanelor în conformitate cu legislația Uniunii sau cea națională.

(28) Toate statele membre ar trebui să respecte cerințele esențiale comune de supraveghere pentru a se asigura un nivel de securitate comparabil al serviciilor calificate de asigurare a încrederii. Pentru a facilita aplicarea consecventă a acestor cerințe pe întreg teritoriul Uniunii, statele membre ar trebui să adopte proceduri comparabile și ar trebui să efectueze schimburi de informații cu privire la activitățile lor de supraveghere și la cele mai bune practici în domeniu.

(29) Notificarea cazurilor de încălcare a securității și evaluarea riscurilor privind securitatea sunt esențiale în vederea furnizării de informații corespunzătoare către părțile în cauză, în caz de încălcare a securității sau de pierdere a integrității.

(30) Pentru a permite Comisiei și statelor membre să evalueze eficiența mecanismului de notificare a încălcărilor introdus prin prezentul regulament, ar trebui să li se solicite organismelor de supraveghere să furnizeze informații sintetizate Comisiei și Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA).

(31) Pentru a permite Comisiei și statelor membre să evalueze impactul prezentului regulament, ar trebui să li se solicite organismelor de supraveghere să furnizeze statistici cu privire la serviciile calificate de asigurare a încrederii și utilizarea lor.

(32) Pentru a permite Comisiei și statelor membre să evalueze eficiența mecanismului de supraveghere consolidată introdus prin prezentul regulament, ar trebui să li se solicite organismelor de supraveghere să prezinte un raport cu privire la activitățile lor. Acest

[22] JO L 281, 23.11.1995, p. 31.

lucru ar contribui la facilitarea schimbului de bune practici între organismele de supraveghere și ar asigura verificarea punerii în aplicare în mod consecvent și eficient în toate statele membre a cerințelor esențiale privind supravegherea.

(33) Pentru a garanta sustenabilitatea și durabilitatea serviciilor calificate de asigurare a încrederii și pentru a spori încrederea utilizatorilor în continuitatea serviciilor calificate de asigurare a încrederii, organismele de supraveghere ar trebui să se asigure că datele prestatorilor de servicii de asigurare a încrederii calificați sunt conservate și păstrate accesibile pentru o perioadă de timp corespunzătoare, chiar și în cazul în care un prestator de servicii de asigurare a încrederii calificat încetează să existe.

(34) Pentru a facilita supravegherea prestatorilor de servicii de asigurare a încrederii calificați, de exemplu, atunci când un furnizor își prestează serviciile pe teritoriul unui alt stat membru și nu face acolo obiectul supravegherii sau în cazul în care calculatoarele unui prestator sunt situate pe teritoriul unui alt stat membru decât cel în care este stabilit, ar trebui să fie instituit un sistem de asistență reciprocă între organismele de supraveghere din statele membre.

(35) Este responsabilitatea prestatorilor de servicii de asigurare a încrederii să îndeplinească cerințele stabilite în prezentul regulament pentru prestarea de servicii de asigurare a încrederii, în special pentru serviciile calificate de asigurare a încrederii. Organismele de supraveghere au responsabilitatea de a supraveghea modul în care prestatorii de servicii de asigurare a încrederii îndeplinesc aceste cerințe.

(36) Pentru a permite un proces de inițiere eficient, care ar trebui să ducă la includerea prestatorilor de servicii de asigurare a încrederii calificați și a serviciilor calificate de asigurare a încrederii pe care le prestează în listele sigure, interacțiunile preliminare dintre potențialii prestatori de servicii de asigurare a încrederii calificați și organismul de supraveghere competent ar trebui să fie încurajate, în scopul facilitării diligenței necesare care conduce la prestarea de servicii calificate de asigurare a încrederii.

(37) Listele sigure sunt elemente esențiale pentru construirea încrederii între operatorii de piață, deoarece ele indică statutul de calificat al prestatorului de servicii în momentul supravegherii; pe de altă parte, acestea nu sunt o condiție necesară pentru obținerea statutului de calificat și pentru prestarea de servicii calificate de asigurare a încrederii care rezultă din respectarea cerințelor din prezentul regulament.

(38) După ce a făcut obiectul unei notificări, un serviciu de asigurare a încrederii calificat nu poate fi refuzat pentru îndeplinirea unei proceduri sau formalități administrative de către organismul din sectorul public în cauză pentru că nu a fost inclus în listele sigure stabilite de către statele membre. În acest sens, un organism din sectorul public se referă la orice autoritate publică sau altă entitate căreia i s-a încredințat prestarea de servicii de e-guvernare, precum declarațiile fiscale online, cererile pentru certificate de naștere, participarea la procedurile de achiziții publice electronice etc.

(39) Deși un nivel ridicat de securitate este necesar pentru a asigura recunoașterea reciprocă a semnăturilor electronice, în cazuri speciale, cum ar fi în contextul Deciziei 2009/767/CE a Comisiei din 16 octombrie 2009 de stabilire a unor măsuri de facilitare a utilizării procedurilor prin mijloace electronice prin intermediul „ghișeelor unice” în temeiul Directivei 2006/123/CE a Parlamentului European și a Consiliului privind

serviciile în cadrul pieței interne[23], semnăturile electronice cu un nivel mai scăzut de asigurare a securității ar trebui să fie, de asemenea, acceptate.

(40) Ar trebui să fie posibil să se încredințeze dispozitivele de creare a semnăturilor electronice calificate unei părți terțe de către semnatar, cu condiția ca mecanismele și procedurile adecvate să fie puse în aplicare pentru a se asigura că semnatarul are control unic asupra utilizării datelor sale de creare a semnăturilor electronice și cu condiția ca utilizarea dispozitivului să îndeplinească cerințele privind semnătura calificată.

(41) Pentru a asigura securitatea juridică cu privire la valabilitatea semnăturii, este esențial să se ofere detalii referitoare la componentele unei semnături electronice calificate care trebuie să fie evaluate de către beneficiarul care efectuează validarea. Mai mult, definirea cerințelor prestatorilor de servicii de asigurare a încrederii calificați care pot presta un serviciu de validare calificat beneficiarilor care nu vor sau care nu pot îndeplini ei înșiși validarea semnăturilor electronice calificate ar trebui să stimuleze sectorul public sau privat să investească în astfel de servicii. Ambele elemente ar trebui să facă validarea semnăturilor electronice calificate ușoară și convenabilă pentru toate părțile la nivelul Uniunii.

(42) Atunci când o tranzacție necesită un sigiliu electronic calificat de la o persoană juridică, o semnătură electronică calificată de la reprezentantul autorizat al persoanei juridice ar trebui să fie, de asemenea, acceptabilă.

(43) Sigiliile electronice ar trebui să servească drept dovadă că un document electronic a fost emis de către o persoană juridică, asigurând certitudinea originii și integrității documentului.

(44) Prezentul regulament ar trebui să asigure păstrarea pe termen lung a informațiilor, adică valabilitatea juridică a semnăturilor și sigiliilor electronice pe perioade lungi de timp, garantând că acestea pot fi validate indiferent de schimbările tehnologice viitoare.

(45) Pentru a spori utilizarea transfrontalieră a documentelor electronice, prezentul regulament ar trebui să prevadă efectul juridic al documentelor electronice care ar trebui să fie considerate ca fiind echivalente cu documentele pe suport de hârtie, în funcție de evaluarea riscului și cu condiția asigurării autenticității și integrității documentelor. De asemenea, este important pentru dezvoltarea în continuare a tranzacțiilor electronice transfrontaliere în cadrul pieței interne ca documentele electronice originale sau copiile certificate emise de organismele competente relevante într-un stat membru conform legislației lor naționale să fie acceptate ca atare, de asemenea, în alte state membre. Prezentul regulament nu ar trebui să aducă atingere dreptului statelor membre de a stabili ce constituie un original sau o copie la nivel național, însă garantează că acestea pot fi utilizate ca atare și dincolo de frontiere.

(46) Deoarece autoritățile competente din statele membre utilizează, în prezent, formate diferite de semnături electronice avansate pentru a-și semna documentele în mod electronic, este necesar să se asigure că cel puțin un număr de formate de semnături electronice avansate pot fi procesate tehnic de statele membre atunci când primesc documente semnate în mod electronic. În mod similar, în cazul în care autoritățile

[23] JO L 274, 20.10.2009, p. 36.

competente din statele membre utilizează sigilii electronice avansate, ar fi necesar să se asigure că acestea pot procesa cel puțin un număr de formate de sigilii electronice avansate.

(47) În plus față de autentificarea documentului emis de persoana juridică, sigiliile electronice pot fi utilizate pentru autentificarea oricărui bun digital al persoanei juridice, de exemplu, cod de software, servere.

(48) Posibilitatea de a autentifica site-urile internet și persoana care le deține ar face mai dificilă falsificarea site-urilor internet și ar reduce, astfel, frauda.

(49) Pentru a completa anumite aspecte tehnice detaliate ale prezentului regulament într-o manieră flexibilă și rapidă, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui să fie delegată Comisiei în ceea ce privește interoperabilitatea identificării electronice, măsurile de securitate solicitate din partea prestatorilor de servicii de asigurare a încrederii, organismele independente recunoscute responsabile de auditarea prestatorilor de servicii, listele sigure, cerințele referitoare la nivelurile de securitate a semnăturilor electronice, cerințele certificatelor calificate pentru semnături electronice și validarea și păstrarea lor, organismele responsabile de certificarea dispozitivelor de creare a semnăturilor electronice calificate, cerințele legate de nivelurile de securitate a sigiliilor electronice și de certificatele calificate pentru sigilii electronice și interoperabilitatea între serviciile de distribuție. Este deosebit de important ca, pe parcursul activităților pregătitoare, Comisia să desfășoare consultări adecvate, inclusiv la nivel de experți.

(50) Atunci când pregătește și elaborează acte delegate, Comisia ar trebui să asigure transmiterea simultană, la timp și adecvată a documentelor relevante către Parlamentul European și către Consiliu.

(51) Pentru a se asigura condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui să se confere competențe de executare Comisiei, în special pentru a specifica numerele de referință ale standardelor a căror utilizare ar oferi o prezumție de conformitate cu anumite cerințe prevăzute în prezentul regulament sau definite în actele delegate. Aceste competențe ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie[24].

(52) Din motive de securitate juridică și claritate, Directiva 1999/93/CE ar trebui abrogată.

(53) Pentru a se asigura securitatea juridică pentru operatorii de piață care utilizează deja certificate calificate emise în conformitate cu Directiva 1999/93/CE, este necesar să se prevadă o perioadă de timp suficientă în scopuri de tranziție. Este necesar, de asemenea, să se furnizeze Comisiei mijloacele de a adopta actele de punere în aplicare și actele delegate înainte de data respectivă.

(54) Deoarece obiectivele prezentului regulament nu pot fi realizate în mod satisfăcător de către statele membre și, în consecință, datorită amplorii acțiunii, pot fi realizate mai

[24] JO L 55, 28.2.2011, p. 13

bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea respectivului obiectiv, în special în privința rolului Comisiei de coordonator al activităților naționale,

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect

1. Prezentul regulament stabilește norme pentru identificarea electronică și serviciile electronice de asigurare a încrederii pentru tranzacțiile electronice în vederea asigurării bunei funcționări a pieței interne.

2. Prezentul regulament stabilește condițiile în care statele membre recunosc și acceptă mijloacele de identificare electronică ale persoanelor fizice și juridice care intră sub incidența unui sistem notificat de identificare electronică al unui alt stat membru.

3. Prezentul regulament stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică și autentificarea unui site internet.

4. Prezentul regulament se asigură că serviciile și produsele de asigurare a încrederii care sunt conforme cu prezentul regulament sunt autorizate să circule liber pe piața internă.

Articolul 2

Domeniul de aplicare

1. Prezentul regulament se aplică identificării electronice furnizate de, în numele sau sub responsabilitatea statelor membre și prestatorilor de servicii de asigurare a încrederii stabiliți în Uniune.

2. Prezentul regulament nu se aplică prestării de servicii electronice de asigurare a încrederii bazate pe acorduri voluntare de drept privat.

3. Prezentul regulament nu se aplică în cazul aspectelor privind încheierea și valabilitatea contractelor sau a altor obligații juridice, în cazul în care există cerințe cu privire la formă prevăzute de legislația națională sau a Uniunii.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „identificare electronică” înseamnă procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând, în mod lipsit de ambiguitate, o persoană fizică sau juridică;

(2) „mijloace de identificare electronică” înseamnă o unitate materială sau imaterială care conține datele menționate la punctul 1 din prezentul articol și care este utilizată pentru a accesa serviciile online menționate la articolul 5;

(3) „sistem de identificare electronică” înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoanele menționate la punctul 1 din prezentul articol;

(4) „autentificare” înseamnă un proces electronic care permite validarea identificării electronice a unei persoane fizice sau juridice sau a originii și integrității unor date electronice;

(5) „semnatar” înseamnă o persoană fizică care creează o semnătură electronică;

(6) „semnătură electronică” înseamnă date în formă electronică, atașate la sau asociate logic cu alte date electronice și care sunt utilizate de semnatar pentru a semna;

(7) „semnătură electronică avansată” înseamnă o semnătură electronică care îndeplinește următoarele cerințe:

(a) face trimitere exclusiv la semnatar;

(b) permite identificarea semnatarului;

(c) este creată utilizând date de creare a semnăturilor electronice pe care semnatarul le poate utiliza exclusiv sub controlul său, cu un nivel ridicat de încredere; precum și

(d) este legată de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată;

(8) „semnătură electronică calificată” înseamnă o semnătură electronică avansată care este creată de un dispozitiv de creare a semnăturilor electronice calificat și care se bazează pe un certificat calificat pentru semnăturile electronice;

(9) „date de creare a semnăturilor electronice” înseamnă date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;

(10) „certificat” înseamnă o atestare electronică care face legătura între datele de validare a semnăturilor sau sigiliilor electronice ale unei persoane fizice sau, respectiv, juridice și certificat și confirmă acele date ca fiind ale persoanei respective;

(11) „certificat calificat pentru semnătură electronică” înseamnă o atestare care este utilizată pentru a susține semnăturile electronice, este emisă de un prestator de servicii de asigurare a încrederii calificat și îndeplinește cerințele prevăzute în anexa I;

(12) „serviciu de asigurare a încrederii” înseamnă orice serviciu electronic care constă în crearea, verificarea, validarea, manipularea și păstrarea semnăturilor electronice, a sigiliilor electronice, a mărcilor temporale electronice, a documentelor electronice, a serviciilor de distribuție electronică, a autentificării unui site internet și a certificatelor electronice, inclusiv certificatele pentru semnăturile și sigiliile electronice;

(13) „serviciu de asigurare a încrederii calificat” înseamnă un serviciu de asigurare a încrederii care îndeplinește cerințele aplicabile prevăzute de prezentul regulament;

(14) „prestator de servicii de asigurare a încrederii” înseamnă o persoană fizică sau juridică care prestează unul sau mai multe servicii de asigurare a încrederii;

(15) „prestator de servicii de asigurare a încrederii calificat” înseamnă un prestator de servicii de asigurare a încrederii care îndeplinește cerințele prevăzute în prezentul regulament;

(16) „produs” înseamnă hardware sau software sau componente relevante ale acestora, destinate să fie utilizate pentru prestarea de servicii de asigurare a încrederii;

(17) „dispozitiv de creare a semnăturilor electronice” înseamnă software sau hardware configurat, utilizat pentru a crea o semnătură electronică;

(18) „dispozitiv de creare a semnăturilor electronice calificat” înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în anexa II;

(19) „creatorul unui sigiliu” înseamnă o persoană juridică care creează un sigiliu electronic;

(20) „sigiliu electronic” înseamnă date în formă electronică, atașate la sau asociate logic cu alte date electronice pentru asigurarea originii și integrității datelor asociate;

(21) „sigiliu electronic avansat” înseamnă un sigiliu electronic care îndeplinește următoarele cerințe:

(a) face trimitere exclusiv la creatorul sigiliului;

(b) permite identificarea creatorului sigiliului;

(c) este creat utilizând date de creare a sigiliilor electronice pe care creatorul sigiliului le poate utiliza sub controlul său, cu un nivel ridicat de încredere, pentru crearea sigiliilor electronice; precum și

(d) este legat de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată;

(22) „sigiliu electronic calificat” înseamnă un sigiliu electronic avansat care este creat de un dispozitiv de creare a sigiliilor electronice calificat și care se bazează pe un certificat calificat pentru sigiliile electronice;

(23) „date de creare a sigiliilor electronice” înseamnă date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;

(24) „certificat calificat pentru sigiliu electronic” înseamnă o atestare care este utilizată pentru a susține un sigiliu electronic, este emisă de un prestator de servicii de asigurare a încrederii calificat și îndeplinește cerințele prevăzute în anexa III;

(25) „marcă temporală electronică” înseamnă date în formă electronică care leagă alte date electronice de un anumit moment, stabilind dovezi că aceste date au existat la acel moment;

(26) „marcă temporală electronică calificată” înseamnă o marcă temporală electronică care îndeplinește cerințele prevăzute la articolul 33;

(27) „document electronic” înseamnă un document în orice format electronic;

(28) „serviciu de distribuție electronică” înseamnă un serviciu care permite transmiterea de date prin mijloace electronice și furnizează dovezi referitoare la tratamentul datele transmise, inclusiv dovezi privind trimiterea sau primirea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificări neautorizate;

(29) „serviciu de distribuție electronică calificat” înseamnă un serviciu de distribuție electronică care îndeplinește cerințele prevăzute la articolul 36;

(30) „certificat calificat pentru autentificarea unui site internet” înseamnă o atestare care face posibilă autentificarea unui site internet, face legătura între site-ul internet și persoana căreia i s-a emis certificatul (de către un prestator de servicii de asigurare a încrederii calificat) și îndeplinește cerințele prevăzute în anexa IV;

(31) „date de validare” înseamnă date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic.

Articolul 4

Principiul pieței interne

1. Nu există nicio restricție privind prestarea de servicii de asigurare a încrederii pe teritoriul unui stat membru de către un prestator de servicii de asigurare a încrederii stabilit în alte state membre, din motive care se încadrează în domeniile reglementate de prezentul regulament.

2. Produsele care sunt conforme cu prezentul regulament sunt autorizate pentru a circula liber pe piața internă.

CAPITOLUL II

IDENTIFICARE ELECTRONICĂ

Articolul 5

Recunoașterea și acceptarea reciprocă

Atunci când este necesară o identificare electronică care utilizează un mijloc de identificare electronică și o autentificare în temeiul legislației naționale sau a practicii administrative naționale pentru a accesa un serviciu online, orice mijloace de identificare electronică emise în alt stat membru care intră sub incidența unui sistem inclus în lista publicată de Comisie în conformitate cu procedura menționată la articolul 7 sunt recunoscute și acceptate în scopul accesării acestui serviciu.

Articolul 6

Condiții de notificare a sistemelor de identificare electronică

1. Sistemele de identificare electronică sunt eligibile pentru notificare în temeiul articolului 7, în cazul în care sunt îndeplinite toate condițiile de mai jos:

(a) mijloacele de identificare electronică sunt emise de către, în numele sau sub responsabilitatea statului membru care notifică;

(b) mijloacele de identificare electronică pot fi utilizate pentru a accesa cel puțin serviciile publice care necesită identificarea electronică în statul membru care notifică;

(c) statul membru care notifică se asigură că datele de identificare a persoanelor sunt atribuite fără ambiguitate persoanei fizice sau juridice menționate la articolul 3 alineatul (1);

(d) statul membru care notifică asigură disponibilitatea unei posibilități de autentificare online, în orice moment și gratuit, astfel încât orice beneficiar să poată valida datele de identificare personală primite în formă electronică. Statele membre nu impun nicio cerință tehnică specifică beneficiarilor stabiliți în afara teritoriului lor care intenționează să efectueze o astfel de autentificare. În cazul în care fie sistemul de identificare notificat, fie posibilitatea de autentificare este încălcată sau parțial compromisă, statele membre suspendă sau revocă imediat sistemul de identificare notificat, posibilitatea de autentificare sau părțile compromise în cauză și informează celelalte state membre și Comisia în temeiul articolului 7;

(e) statul membru care notifică își asumă răspunderea pentru:

– (i) atribuirea lipsită de ambiguitate a datelor de identificare personală menționate la litera (c) și

– (ii) posibilitatea de autentificare specificată la litera (d).

2. Alineatul (1) litera (e) nu aduce atingere răspunderii părților la o tranzacție în care sunt utilizate mijloacele de identificare electronică care intră sub incidența sistemului notificat.

Articolul 7

Notificare

1. Statele membre care notifică un sistem de identificare electronică înaintează Comisiei următoarele informații și, fără întârzieri nejustificate, orice modificări ulterioare ale acestora:

(a) o descriere a sistemului de identificare electronică notificat;

(b) autoritățile responsabile pentru sistemul de identificare electronică notificat;

(c) informații cu privire la cine gestionează înregistrarea identificatorilor cu caracter personal lipsiți de ambiguitate;

(d) o descriere a posibilității de autentificare;

(e) dispoziții pentru suspendarea sau revocarea sistemului de identificare notificat, a posibilității de autentificare sau a părților compromise în cauză.

2. La șase luni de la intrarea în vigoare a regulamentului, Comisia publică în *Jurnalul Oficial al Uniunii Europene* lista sistemelor de identificare electronică care au fost notificate în temeiul alineatului (1) și informațiile de bază cu privire la acestea.

3. În cazul în care Comisia primește o notificare după expirarea perioadei menționate la alineatul (2), aceasta modifică lista în termen de trei luni.

4. Comisia poate, prin intermediul actelor de punere în aplicare, să definească circumstanțele, formatele și procedurile de notificare menționate la alineatele (1) și (3). Actele respective de

punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 8

Coordonare

1. Statele membre cooperează pentru a asigura interoperabilitatea mijloacelor de identificare electronică care intră sub incidența unui sistem notificat și pentru a spori securitatea acestora.

2. Comisia stabilește, prin intermediul actelor de punere în aplicare, modalitățile necesare pentru a facilita cooperarea între statele membre menționate la alineatul (1), în vederea stimulării unui nivel ridicat de încredere și securitate corespunzător gradului de risc. Actele respective de punere în aplicare se referă, în special, la schimbul de informații, de experiență și de bune practici privind sistemele de identificare electronică, evaluarea *inter pares* a sistemelor de identificare electronică notificate și examinarea evoluțiilor relevante care au loc în sectorul identificării electronice de către autoritățile competente ale statelor membre. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind facilitarea interoperabilității transfrontaliere a mijloacelor de identificare electronică prin stabilirea de cerințe tehnice minime.

CAPITOLUL III

SERVICII DE ASIGURARE A ÎNCREDERII

Secțiunea 1

Dispoziții generale

Articolul 9

Răspundere

1. Un prestator de servicii de asigurare a încrederii este răspunzător pentru orice daune directe cauzate oricărei persoane fizice sau juridice din cauza nerespectării obligațiilor prevăzute la articolul 15 alineatul (1), cu excepția cazului în care prestatorul de servicii de asigurare a încrederii poate dovedi că nu a acționat cu neglijență.

2. Un prestator de servicii de asigurare a încrederii calificat este răspunzător pentru orice daune directe cauzate oricărei persoane fizice sau juridice din cauza neîndeplinirii cerințelor prevăzute în prezentul regulament, în special la articolul 19, cu excepția cazului în care prestatorul de servicii de asigurare a încrederii calificat poate dovedi că nu a acționat cu neglijență.

Articolul 10

Prestatori de servicii de asigurare a încrederii din țări terțe

1. Serviciile calificate de asigurare a încrederii și certificatele calificate furnizate de prestatori de servicii de asigurare a încrederii calificați stabiliți într-o țară terță sunt acceptate ca servicii calificate de asigurare a încrederii și certificate calificate furnizate de prestatori de servicii de asigurare a încrederii calificați stabiliți pe teritoriul Uniunii în cazul în care serviciile calificate de asigurare a încrederii sau certificatele calificate originare din țara terță sunt recunoscute în cadrul unui acord dintre Uniune și țările terțe sau organizațiile internaționale în conformitate cu articolul 218 din TFUE.

2. Cu trimitere la alineatul (1), aceste acorduri garantează că cerințele aplicabile serviciilor calificate de asigurare a încrederii și certificatelor calificate furnizate de prestatorii de servicii de asigurare a încrederii calificați stabiliți pe teritoriul Uniunii sunt îndeplinite de prestatorii de servicii de asigurare a încrederii din țările terțe sau organizațiile internaționale, în special cu privire la protecția datelor cu caracter personal, la securitate și la supraveghere.

Articolul 11

Prelucrarea și protecția datelor

1. Prestatorii de servicii de asigurare a încrederii și organismele de supraveghere asigură prelucrarea corectă și legală în conformitate cu Directiva 95/46/CE în ceea ce privește prelucrarea datelor cu caracter personal.

2. Prestatorii de servicii de asigurare a încrederii prelucrează datele cu caracter personal în conformitate cu Directiva 95/46/CE. Această prelucrare este limitată strict la datele minime necesare pentru emiterea și menținerea unui certificat sau pentru prestarea unui serviciu de asigurare a încrederii.

3. Prestatorii de servicii de asigurare a încrederii garantează confidențialitatea și integritatea datelor referitoare la persoana căreia îi este furnizat serviciul de asigurare a încrederii.

4. Fără să aducă atingere efectului juridic acordat pseudonimelor în temeiul legislației naționale, statele membre nu împiedică prestatorii de servicii de asigurare a încrederii să indice în certificatele pentru semnăturile electronice un pseudonim în loc de numele semnatarului.

Articolul 12

Accesibilitatea pentru persoanele cu handicap

Serviciile de asigurare a încrederii prestate și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile pentru persoanele cu handicap ori de câte ori este posibil.

Secțiunea 2

Supraveghere

Articolul 13

Organismul de supraveghere

1. Statele membre desemnează un organism adecvat stabilit pe teritoriul lor sau, de comun acord, în alt stat membru, sub responsabilitatea statului membru care l-a desemnat. Organismele de supraveghere sunt învestite cu toate competențele de supraveghere și de investigare necesare pentru exercitarea sarcinilor lor.

2. Organismul de supraveghere este responsabil de îndeplinirea următoarelor sarcini:

(a) monitorizarea prestatorilor de servicii de asigurare a încrederii stabiliți pe teritoriul statului membru care a efectuat desemnarea, pentru a se asigura că îndeplinesc cerințele prevăzute la articolul 15;

(b) supravegherea prestatorilor de servicii de asigurare a încrederii calificați stabiliți pe teritoriul statului membru care a efectuat desemnarea și a serviciilor calificate de asigurare a încrederii pe care le prestează pentru a se asigura că aceștia și serviciile calificate de asigurare a încrederii prestate de aceștia îndeplinesc cerințele aplicabile prevăzute în prezentul regulament;

(c) asigurarea faptului că informațiile și datele relevante menționate la articolul 19 alineatul (2) litera (g) și înregistrate de prestatorii de servicii de asigurare a încrederii calificați sunt conservate și păstrate accesibile după ce activitățile unui prestator de servicii de asigurare a încrederii calificat au încetat, pentru o perioadă de timp corespunzătoare, în vederea garantării continuității serviciului.

3. Fiecare organism de supraveghere prezintă Comisiei și statelor membre un raport anual privind activitățile de supraveghere din ultimul an calendaristic, până la sfârșitul primului trimestru al anului următor. Acesta include, cel puțin:

(a) informații privind activitățile sale de supraveghere;

(b) un rezumat al notificărilor încălcărilor primit de la prestatorii de servicii de asigurare a încrederii, în conformitate cu articolul 15 alineatul (2);

(c) statistici privind piața și utilizarea serviciilor calificate de asigurare a încrederii, inclusiv informații privind înșiși prestatorii de servicii de asigurare a încrederii calificați, serviciile calificate de asigurare a încrederii pe care le oferă, produsele pe care le utilizează și descrierea generală a clienților lor.

4. Statele membre notifică Comisiei și celorlalte state membre denumirile și adresele organismelor lor respective de supraveghere desemnate.

5. Comisia este împuternicită să adopte acte delegate, în conformitate cu articolul 38, cu privire la definiția procedurilor aplicabile sarcinilor menționate la alineatul (2).

6. Comisia poate, prin intermediul actelor de punere în aplicare, să definească circumstanțele, formatele și procedurile pentru raportul menționat la alineatul (3). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 14

Asistență reciprocă

1. Organismele de supraveghere cooperează cu scopul de a face schimb de bune practici și de a-și oferi reciproc, în cel mai scurt timp, informații relevante și asistență reciprocă, astfel încât activitățile să poată fi efectuate în mod coerent. Asistența reciprocă vizează, în special, solicitările de informații și măsurile de supraveghere, cum ar fi solicitările de a desfășura inspecții legate de auditurile privind securitatea menționate la articolele 15, 16 și 17.

2. Un organism de supraveghere căruia i se adresează o solicitare de asistență nu poate refuza să îi dea curs, cu excepția cazului în care:

(a) nu are competența de a trata solicitarea sau

(b) a da curs solicitării ar contraveni prezentului regulament.

3. După caz, organismele de supraveghere pot efectua anchete comune în care este implicat personalul din organismele de supraveghere ale celorlalte state membre.

Organismul de supraveghere al statului membru în care urmează să aibă loc ancheta, în conformitate cu propria legislație națională, poate să delege misiuni de anchetă personalului organismului de supraveghere asistat. Aceste competențe pot fi exercitate doar sub îndrumarea și în prezența personalului din organismul de supraveghere-gazdă. Personalul organismului de supraveghere asistat este supus legislației naționale a organismului de supraveghere-gazdă. Organismul de supraveghere-gazdă își asumă responsabilitatea pentru acțiunile personalului organismului de supraveghere asistat.

4. Comisia poate, prin intermediul actelor de punere în aplicare, să specifice formatele și procedurile pentru asistența reciprocă prevăzută la prezentul articol. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 15

Cerințe de securitate aplicabile prestatorilor de servicii de asigurare a încrederii

1. Prestatorii de servicii de asigurare a încrederii care sunt stabiliți pe teritoriul Uniunii iau măsurile tehnice și organizatorice corespunzătoare pentru a gestiona riscurile pentru securitatea serviciilor de asigurare a încrederii pe care le prestează. Având în vedere stadiul actual al tehnologiei, aceste măsuri garantează că nivelul securității este corespunzător gradului de risc. În special, se iau măsuri pentru a preveni și minimiza impactul incidentelor legate de securitate și pentru a informa părțile interesate cu privire la efectele negative ale oricăror incidente.

Fără a aduce atingere articolului 16 alineatul (1), orice prestator de servicii de asigurare a încrederii poate prezenta organismului de supraveghere raportul unui audit privind securitatea efectuat de un organism independent recunoscut pentru a confirma faptul că au fost luate măsuri de securitate corespunzătoare.

2. Prestatorii de servicii de asigurare a încrederii notifică, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 24 de ore după ce au aflat, organismului de supraveghere competent, organismului național competent pentru securitatea informațiilor și altor părți terțe relevante, precum autoritățile pentru protecția datelor, orice încălcare a securității sau pierdere

a integrității care are un impact semnificativ asupra serviciului de asigurare a încrederii prestat și asupra datelor cu caracter personal păstrate de acesta.

După caz, în special dacă o încălcare a securității sau o pierdere a integrității se referă la două sau mai multe state membre, organismul de supraveghere în cauză informează organismele de supraveghere din alte state membre și Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA).

Organismul de supraveghere în cauză poate, de asemenea, să informeze publicul sau să solicite prestatorului de servicii de asigurare a încrederii să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării servește interesului public.

3. Organismul de supraveghere furnizează ENISA și Comisiei, o dată pe an, un rezumat al notificărilor încălcărilor primite de la prestatorii de servicii de asigurare a încrederii.

4. În scopul punerii în aplicare a alineatelor (1) și (2), organismul de supraveghere competent are competența de a emite instrucțiuni obligatorii pentru prestatorii de servicii de asigurare a încrederii.

5. Comisia este împuternicită să adopte acte delegate, în conformitate cu articolul 38, privind definirea mai precisă a măsurilor menționate la alineatul (1).

6. Comisia poate, prin intermediul actelor de punere în aplicare, să definească circumstanțele, formatele și procedurile, inclusiv termenele, aplicabile în sensul alineatelor (1) - (3). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 16

Supravegherea prestatorilor de servicii de asigurare a încrederii calificați

1. Prestatorii de servicii de asigurare a încrederii calificați sunt auditați de către un organism independent recunoscut o dată pe an pentru a se confirma că atât ei, cât și serviciile calificate de asigurare a încrederii pe care le prestează îndeplinesc cerințele stabilite în prezentul regulament și prezintă organismului de supraveghere raportul care rezultă în urma auditului privind securitatea.

2. Fără a aduce atingere alineatului (1), organismul de supraveghere poate, în orice moment, să auditeze prestatorii de servicii de asigurare a încrederii calificați pentru a confirma că atât ei, cât și serviciile calificate de asigurare a încrederii prestate de aceștia continuă să îndeplinească condițiile stabilite în prezentul regulament, fie din proprie inițiativă, fie ca răspuns la o solicitare din partea Comisiei. Organismul de supraveghere informează autoritățile pentru protecția datelor cu privire la rezultatele auditurilor sale, în cazul în care par să fi fost încălcate normele de protecție a datelor cu caracter personal.

3. Organismul de supraveghere are competența de a da instrucțiuni obligatorii prestatorilor de servicii de asigurare a încrederii calificați pentru a remedia orice nerespectare a cerințelor indicate în raportul auditului privind securitatea.

4. Cu trimitere la alineatul (3), în cazul în care prestatorul de servicii de asigurare a încrederii calificat nu remediază orice astfel de nerespectare într-un termen stabilit de către organismul

de supraveghere, acesta își pierde statutul de calificat și este informat de către organismul de supraveghere că statutul său va fi modificat în consecință în listele sigure menționate la articolul 18.

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind specificarea condițiilor în care este recunoscut organismul independent care efectuează auditul menționat la alineatul (1) din prezentul articol, la articolul 15 alineatul (1) și la articolul 17 alineatul (1).

6. Comisia poate, prin intermediul actelor de punere în aplicare, să definească circumstanțele, procedurile și formatele aplicabile în sensul alineatelor (1), (2) și (4). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 17

Inițierea unui serviciu de asigurare a încrederii calificat

1. Prestatorii de servicii de asigurare a încrederii calificați notifică organismului de supraveghere intenția lor de a începe prestarea unui serviciu de asigurare a încrederii calificat și prezintă organismului de supraveghere un raport al auditului privind securitatea efectuat de un organism independent recunoscut, astfel cum este prevăzut la articolul 16 alineatul (1). Prestatorii de servicii de asigurare a încrederii calificați pot începe să furnizeze serviciul de asigurare a încrederii calificat după ce au prezentat organismului de supraveghere notificarea și raportul auditului privind securitatea.

2. De îndată ce documentele relevante sunt prezentate organismului de supraveghere în conformitate cu alineatul (1), prestatorii de servicii calificați sunt incluși în listele sigure menționate la articolul 18, indicând că notificarea a fost prezentată.

3. Organismul de supraveghere verifică respectarea de către prestatorul de servicii de asigurare a încrederii calificat și de către serviciile calificate de asigurare a încrederii prestate de acesta a cerințelor regulamentului.

Dacă verificarea dă naștere unor concluzii pozitive, organismul de supraveghere indică statutul de calificat al prestatorilor de servicii calificați și al serviciilor calificate de asigurare a încrederii pe care aceștia le prestează în listele sigure, în termen de cel mult o lună de la notificare, în conformitate cu alineatul (1).

În cazul în care verificarea nu este încheiată în termen de o lună, organismul de supraveghere informează prestatorul de servicii de asigurare a încrederii calificat, specificând motivele întârzierii și termenul în care se încheie verificarea.

4. Un serviciu de asigurare a încrederii calificat care a făcut obiectul notificării menționate la alineatul (1) nu poate fi refuzat pentru îndeplinirea unei proceduri sau formalități administrative de către organismul din sectorul public în cauză pentru că nu a fost inclus în listele menționate la alineatul (3).

5. Comisia poate, prin intermediul actelor de punere în aplicare, să definească circumstanțele, formatele și procedurile în sensul alineatelor (1), (2) și (3). Actele respective de punere în

aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 18

Listele sigure

1. Fiecare stat membru instituie, menține și publică liste sigure cu informații referitoare la prestatorii de servicii de asigurare a încrederii calificați pentru care este competent, împreună cu informații referitoare la serviciile calificate de asigurare a încrederii prestate de aceștia.

2. Statele membre instituie, mențin și publică, în mod sigur, listele sigure semnate sau sigilate electronic prevăzute la alineatul (1), într-o formă adecvată pentru prelucrarea automată.

3. Statele membre notifică Comisiei, fără întârzieri nejustificate, informații cu privire la organismul responsabil pentru instituirea, menținerea și publicarea listelor sigure naționale și detalii despre locul unde sunt publicate aceste liste, certificatul utilizat pentru semnarea sau sigilarea listelor sigure și orice modificări ale acestora.

4. Comisia pune la dispoziția publicului, printr-un canal sigur, informațiile menționate la alineatul (3) într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvată pentru prelucrarea automată.

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind definirea informațiilor menționate la alineatul (1).

6. Comisia poate, prin intermediul actelor de punere în aplicare, să definească specificațiile tehnice și formatele pentru listele sigure aplicabile în sensul alineatelor (1) - (4). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 19

Cerințe pentru prestatorii de servicii de asigurare a încrederii calificați

1. Atunci când emite un certificat calificat, un prestator de servicii de asigurare a încrederii calificat verifică, prin mijloace corespunzătoare și în conformitate cu legislația națională, identitatea și, atunci când este cazul, calitățile speciale ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat.

Aceste informații sunt verificate de către prestatorul de servicii calificat sau de către o parte terță autorizată care acționează sub responsabilitatea prestatorului de servicii calificat:

(a) de către persoana fizică sau un reprezentant autorizat al persoanei juridice, în persoană sau

(b) de la distanță, utilizând mijloace de identificare electronică în cadrul unui sistem notificat emis în conformitate cu litera (a).

2. Prestatorii de servicii de asigurare a încrederii calificați care prestează servicii calificate de asigurare a încrederii:

(a) angajează personal care posedă expertiza, experiența și calificările necesare, care aplică proceduri administrative și de gestionare care corespund standardelor europene sau internaționale și care a beneficiat de o formare adecvată cu privire la normele de protecție a securității și a datelor cu caracter personal;

(b) își asumă răspunderea pentru daune prin menținerea de resurse financiare suficiente sau printr-un sistem adecvat de asigurări de răspundere;

(c) înainte de stabilirea unei relații contractuale, informează orice persoană care dorește să utilizeze un serviciu de asigurare a încrederii calificat de clauzele și condițiile exacte privind utilizarea acelui serviciu;

(d) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și garantează siguranța tehnică și fiabilitatea procesului susținut de acestea;

(e) utilizează sisteme demne de încredere pentru a stoca datele care le sunt furnizate, într-o formă care poate fi verificată, astfel încât:

– acestea sunt disponibile publicului pentru cercetări numai în cazul în care a fost obținut consimțământul persoanei căreia i-au fost emise datele,

– numai persoanele autorizate pot introduce și modifica date,

– autenticitatea informației poată fi controlată;

(f) iau măsuri împotriva falsificării și furtului de date;

(g) înregistrează pentru o perioadă de timp corespunzătoare toate informațiile relevante referitoare la datele emise și primite de către prestatorul de servicii de asigurare a încrederii calificat, în special în scopul de a furniza dovezi în procedurile judiciare. Aceste înregistrări pot fi efectuate în mod electronic;

(h) au un plan actualizat, în cazul încetării serviciului, pentru a asigura continuitatea serviciului în conformitate cu dispozițiile emise de către organismul de supraveghere, în conformitate cu articolul 13 alineatul (2) litera (c);

(i) asigură prelucrarea legală a datelor cu caracter personal în conformitate cu articolul 11.

3. Prestatorii de servicii de asigurare a încrederii calificați care emit certificate calificate înregistrează în baza lor de date de certificate revocarea certificatului în zece minute după această revocare.

4. Cu privire la alineatul (3), prestatorii de servicii de asigurare a încrederii calificați care emit certificate calificate furnizează oricărui beneficiar informații cu privire la valabilitatea sau revocarea statutului de certificate calificate emise de aceștia. Aceste informații sunt puse la dispoziție în orice moment cel puțin pe baza unui certificat în mod automat, fiabil, gratuit și eficient.

5. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru sisteme și produse demne de încredere. Conformitatea cu

cerințele prevăzute la articolul 19 este presupusă atunci când sistemele și produsele demne de încredere respectă standardele respective. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Secțiunea 3

Semnătura electronică

Articolul 20

Efecte juridice și acceptarea semnăturilor electronice

1. Unei semnături electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca dovadă în procedurile judiciare doar din motiv că este sub formă electronică.

2. O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe.

3. Semnăturile electronice calificate sunt recunoscute și acceptate în toate statele membre.

4. Dacă se solicită o semnătură electronică cu un nivel de asigurare a securității sub cel al semnăturii electronice calificate, în special de un stat membru pentru a accesa un serviciu online oferit de un organism din sectorul public pe baza unei evaluări adecvate a riscurilor implicate într-un astfel de serviciu, sunt recunoscute și acceptate toate semnăturile electronice care au cel puțin același nivel de asigurare a securității.

5. Statele membre nu solicită pentru accesul transfrontalier la un serviciu online oferit de un organism din sectorul public o semnătură electronică la un nivel de asigurare a securității mai ridicat decât cel al semnăturii electronice calificate.

6. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 în ceea ce privește definirea diferitelor niveluri de securitate a semnăturii electronice menționate la alineatul (4).

7. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru nivelurile de securitate ale semnăturii electronice. Conformitatea cu nivelul de securitate definit într-un act delegat adoptat în temeiul alineatului (6) este presupusă atunci când o semnătură electronică îndeplinește standardele respective. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 21

Certificate calificate pentru semnătura electronică

1. Certificatele calificate pentru semnătura electronică îndeplinesc cerințele prevăzute în anexa I.

2. Certificatele calificate pentru semnătura electronică nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa I.

3. În cazul în care un certificat calificat pentru semnătura electronică a fost revocat după activarea inițială, acesta își pierde valabilitatea și nu se revine în niciun caz la statutul său prin reînnoirea valabilității sale.

4. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind definirea mai precisă a cerințelor prevăzute în anexa I.

5. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru semnătura electronică. În cazul în care un certificat calificat pentru semnătura electronică îndeplinește standardele respective, se presupune că respectă cerințele prevăzute în anexa I. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 22

Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate

1. Dispozitivele de creare a semnăturilor electronice calificate îndeplinesc cerințele prevăzute în anexa II.

2. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru dispozitivele de creare a semnăturilor electronice calificate. În cazul în care un dispozitiv de creare a semnăturilor electronice calificat îndeplinește standardele respective, se presupune că respectă cerințele prevăzute în anexa II. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 23

Certificarea dispozitivelor de creare a semnăturilor electronice calificate

1. Dispozitivele de creare a semnăturilor electronice calificate pot fi certificate de organisme publice sau private adecvate desemnate de statele membre, cu condiția ca acestea să fi fost supuse unui proces de evaluare a securității efectuat în conformitate cu una din normele pentru evaluarea securității produselor tehnologiei informației incluse pe o listă care este stabilită de Comisie prin intermediul actelor de punere în aplicare. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

2. Statele membre notifică Comisiei și celorlalte state membre denumirile și adresele organismului public sau privat desemnat de acestea, astfel cum se menționează la alineatul (1).

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind stabilirea de criterii specifice care urmează să fie îndeplinite de către organismele desemnate menționate la alineatul (1).

Articolul 24

Publicarea unei liste de dispozitive de creare a semnăturilor electronice certificate și calificate

1. Statele membre notifică Comisiei fără întârzieri nejustificate informații cu privire la dispozitivele de creare a semnăturilor electronice calificate care au fost certificate de către organismele menționate la articolul 23. Ele notifică Comisiei, de asemenea, fără întârzieri nejustificate, informații cu privire la dispozitivele de creare a semnăturilor electronice care nu ar mai fi certificate.

2. Pe baza informațiilor primite, Comisia stabilește, publică și menține o listă a dispozitivelor de creare a semnăturilor electronice certificate și calificate.

3. Comisia poate, prin intermediul actelor de punere în aplicare, să definească circumstanțele, formatele și procedurile aplicabile în sensul alineatului (1). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Articolul 25

Cerințe pentru validarea semnăturilor electronice calificate

1. O semnătură electronică calificată este considerată valabilă dacă se poate stabili, cu un grad ridicat de certitudine, că în momentul semnării:

(a) certificatul care stă la baza semnăturii este un certificat calificat pentru semnătura electronică care respectă dispozițiile prevăzute în anexa I;

(b) certificatul calificat necesar este autentic și valabil;

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

(d) setul de date care reprezintă fără ambiguitate semnatarul este furnizat corect beneficiarului;

(e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care se folosește un pseudonim;

(f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat;

(g) integritatea datelor semnate nu a fost compromisă;

(h) cerințele prevăzute la articolul 3 alineatul (7) sunt respectate;

(i) sistemul utilizat pentru validarea semnăturii furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspecte relevante pentru securitate.

2. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind definirea mai precisă a cerințelor prevăzute la alineatul (1).

3. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru validarea semnăturilor electronice calificate. În cazul în care validarea semnăturilor electronice calificate îndeplinește standardele respective, se presupune că respectă cerințele prevăzute la alineatul (1). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 26

Serviciul de validare calificat pentru semnăturile electronice calificate

1. Un serviciu de validare calificat pentru semnături electronice calificate este prestat de către un prestator de servicii de asigurare a încrederii calificat care:

(a) furnizează validare în conformitate cu articolul 25 alineatul (1) și

(b) permite beneficiarilor să primească rezultatul procesului de validare în mod automat, fiabil, eficient și care poartă semnătura electronică avansată sau sigiliul electronic avansat al prestatorului care oferă serviciul de validare calificat.

2. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru serviciul de validare calificat menționat la alineatul (1). În cazul în care serviciul de validare pentru semnătura electronică calificată îndeplinește standardele respective, se presupune că respectă cerințele prevăzute la alineatul (1) litera (b). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 27

Păstrarea semnăturilor electronice calificate

1. Un serviciu de păstrare a semnăturilor electronice calificate este prestat de un prestator de servicii de asigurare a încrederii calificat care utilizează proceduri și tehnologii capabile să extindă fiabilitatea datelor de validare a semnăturilor electronice calificate dincolo de perioada de valabilitate tehnologică.

2. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind definirea mai precisă a cerințelor prevăzute la alineatul (1).

3. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru păstrarea semnăturilor electronice calificate. În cazul în care dispozițiile pentru păstrarea semnăturilor electronice calificate îndeplinesc standardele respective, se presupune că respectă cerințele prevăzute la alineatul (1). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Secțiunea 4

Sigilii electronice

Articolul 28

Efectele juridice ale sigiliilor electronice

1. Nu se refuză efectul juridic al unui sigiliu electronic și posibilitatea de a fi acceptat ca dovadă în procedurile judiciare doar din motiv că este sub formă electronică.

2. Un sigiliu electronic calificat beneficiază de prezumția juridică de a garanta originea și integritatea datelor de care este legat.

3. Un sigiliu electronic calificat este recunoscut și acceptat în toate statele membre.

4. Dacă se solicită un nivel de asigurare a securității sigiliului electronic sub cel al sigiliului electronic calificat, în special de un stat membru pentru a accesa un serviciu online oferit de un organism din sectorul public pe baza unei evaluări adecvate a riscurilor implicate de un astfel de serviciu, sunt acceptate toate sigiliile electronice care au cel puțin același nivel de asigurare a securității.

5. Statele membre nu solicită pentru a accesa un serviciu online oferit de un organism din sectorul public un sigiliu electronic la un nivel de asigurare a securității mai ridicat decât cel al sigiliilor electronice calificate.

6. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 în ceea ce privește definirea diferitelor niveluri de asigurare a securității sigiliilor electronice menționate la alineatul (4).

7. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru nivelurile de asigurare a securității sigiliilor electronice. Conformitatea cu nivelul de asigurare a securității definit într-un act delegat adoptat în temeiul alineatului (6) este presupusă atunci când un sigiliu electronic îndeplinește standardele respective. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 29

Cerințe pentru certificatele calificate pentru sigilii electronice

1. Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute în anexa III.

2. Certificatele calificate pentru sigiliile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa III.

3. În cazul în care un certificat calificat pentru un sigiliu electronic a fost revocat după activarea inițială, acesta își pierde valabilitatea și nu se revine în niciun caz la statutul său anterior prin reînnoirea valabilității sale.

4. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind definirea mai precisă a cerințelor prevăzute în anexa III.

5. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru sigiliile electronice. În cazul în care un certificat calificat pentru sigiliul electronic îndeplinește standardele respective, se presupune că respectă cerințele prevăzute în anexa III. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Articolul 30

Dispozitive de creare a sigiliilor electronice calificate

1. Articolul 22 se aplică *mutatis mutandis* cerințelor pentru dispozitivele de creare a sigiliilor electronice calificate.

2. Articolul 23 se aplică *mutatis mutandis* certificării dispozitivelor de creare a sigiliilor electronice calificate.

3. Articolul 24 se aplică *mutatis mutandis* publicării unei liste a dispozitivelor de creare a sigiliilor electronice certificate și calificate.

Articolul 31

Validarea și păstrarea sigiliilor electronice calificate

Articolele 25, 26 și 27 se aplică *mutatis mutandis* validării și păstrării sigiliilor electronice calificate.

Secțiunea 5

Marca temporală electronică

Articolul 32

Efectul juridic al mărcii temporale electronice

1. Nu se refuză efectul juridic al unei mărci temporale electronice și posibilitatea de a fi acceptată ca dovadă în procedurile judiciare doar din motiv că este sub formă electronică.

2. Marca temporală electronică calificată beneficiază de o prezumție juridică de a garanta timpul pe care îl indică și integritatea datelor la care se raportează timpul indicat.

3. O marcă temporală electronică calificată este recunoscută și acceptată în toate statele membre.

Articolul 33

Cerințe pentru mărcile temporale electronice calificate

1. O marcă temporală electronică calificată îndeplinește următoarele cerințe:

(a) este precis legată de ora universală coordonată astfel încât să excludă orice posibilitate ca datele să fie schimbate fără ca acest lucru să fie detectat;

(b) se bazează pe o sursă de timp precisă;

(c) este emisă de un prestator de servicii de asigurare a încrederii calificat;

(d) este semnată utilizând o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de asigurare a încrederii calificat sau printr-o metodă echivalentă.

2. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru exactitatea legăturii între timp și date și exactitatea sursei timpului indicat. În cazul în care exactitatea legăturii între timp și date și exactitatea sursei timpului indicat îndeplinesc standardele respective, se presupune că se respectă cerințele prevăzute la alineatul (1). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Secțiunea 6

Documente electronice

Articolul 34

Efecte juridice și acceptarea documentelor electronice

1. Un document electronic este considerat echivalent cu un document pe suport de hârtie și admisibil ca dovadă în procedurile judiciare, având în vedere nivelul său de asigurare a autenticității și integrității.

2. Un document care poartă o semnătură electronică calificată sau un sigiliu electronic calificat al persoanei care este competentă să emită documentul relevant beneficiază de prezumția juridică a autenticității și integrității sale, cu condiția ca documentul să nu conțină niciun element dinamic capabil să modifice automat documentul.

3. Atunci când un document original sau o copie certificată este necesar(ă) pentru prestarea unui serviciu online oferit de un organism din sectorul public, sunt acceptate în alte state membre fără cerințe suplimentare cel puțin documentele electronice emise de persoanele care sunt competente să emită documentele relevante și care sunt considerate a fi originale sau copii certificate în conformitate cu legislația națională a statului membru de origine.

4. Comisia poate, prin intermediul actelor de punere în aplicare, să definească formatele semnăturilor și sigiliilor electronice care se acceptă ori de câte ori un document semnat sau sigilat este solicitat de un stat membru pentru prestarea unui serviciu online oferit de un organism din sectorul public menționat la alineatul (2). Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Secțiunea 7

Servicii de distribuție electronică calificate

Articolul 35

Efectul juridic al unui serviciu de distribuție electronică

1. Datele trimise sau primite utilizând un serviciu de distribuție electronică sunt admisibile ca dovezi în procedurile judiciare cu privire la integritatea datelor și exactitatea datei și orei la care datele au fost trimise sau primite de către un destinatar precizat.

2. Datele trimise sau primite utilizând un serviciu de distribuție electronică calificat beneficiază de prezumția juridică a integrității datelor și preciziei datei și orei trimiterii sau primirii datelor indicate de sistemul de distribuție electronică calificat.

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind specificarea mecanismelor pentru trimiterea sau primirea datelor utilizând serviciile de distribuție electronică, care sunt utilizate în scopul stimulării interoperabilității între serviciile de distribuție electronică.

Articolul 36

Cerințe pentru serviciile de distribuție electronică calificate

1. Serviciile de distribuție electronică calificate îndeplinesc următoarele cerințe:

(a) trebuie să fie prestate de către unul sau mai mulți prestatori de servicii de asigurare a încrederii calificați;

(b) trebuie să permită identificarea lipsită de ambiguitate a expeditorului și, dacă este cazul, a destinatarului;

(c) procesul de trimitere sau primire a datelor trebuie să fie sigur printr-o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de asigurare a încrederii calificat astfel încât să excludă posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat;

(d) orice modificare a datelor necesare în scopul de a trimite sau primi datele trebuie să fie clar indicată expeditorului și destinatarului datelor;

(e) data trimiterii, primirii și a oricărei modificări a datelor trebuie să fie indicată printr-o marcă temporală electronică calificată;

(f) în cazul datelor transferate între doi sau mai mulți prestatori de servicii de asigurare a încrederii calificați, cerințele de la literele (a) - (e) se aplică tuturor prestatorilor de servicii de asigurare a încrederii calificați.

2. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru procesele de trimitere și primire de date. Conformitatea cu cerințele prevăzute la alineatul (1) este presupusă în cazul în care procesul de trimitere și primire de date îndeplinește standardele respective. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

Secțiunea 8

Autentificarea unui site internet

Articolul 37

Cerințe pentru certificatele calificate pentru autentificarea unui site internet

1. Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute în anexa IV.

2. Certificatele calificate pentru autentificarea unui site internet sunt recunoscute și acceptate în toate statele membre.

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 38 privind definirea mai precisă a cerințelor prevăzute în anexa IV.

4. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru autentificarea unui site internet. În cazul în care un certificat calificat pentru autentificarea unui site internet îndeplinește standardele respective, se presupune că respectă cerințele prevăzute în anexa IV. Actele respective de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). Comisia publică actele respective în *Jurnalul Oficial al Uniunii Europene*.

CAPITOLUL IV

ACTE DELEGATE

Articolul 38

Exercitarea delegării

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

2. Competența de a adopta actele delegate menționată la articolul 8 alineatul (3), articolul 13 alineatul (5), articolul 15 alineatul (5), articolul 16 alineatul (5), articolul 18 alineatul (5), articolul 20 alineatul (6), articolul 21 alineatul (4), articolul 23 alineatul (3), articolul 25 alineatul (2), articolul 27 alineatul (2), articolul 28 alineatul (6), articolul 29 alineatul (4), articolul 30 alineatul (2), articolul 31, articolul 35 alineatul (3) și articolul 37 alineatul (3) este conferită Comisiei pentru o perioadă de timp nedeterminată de la data intrării în vigoare a prezentului regulament.

3. Delegarea competenței menționate la articolul 8 alineatul (3), articolul 13 alineatul (5), articolul 15 alineatul (5), articolul 16 alineatul (5), articolul 18 alineatul (5), articolul 20 alineatul (6), articolul 21 alineatul (4), articolul 23 alineatul (3), articolul 25 alineatul (2), articolul 27 alineatul (2), articolul 28 alineatul (6), articolul 29 alineatul (4), articolul 30 alineatul (2), articolul 31, articolul 35 alineatul (3) și articolul 37 alineatul (3) poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. Decizia de revocare pune capăt delegării competenței menționate în decizia respectivă. Aceasta produce efecte începând cu ziua următoare datei publicării deciziei în *Jurnalul Oficial al Uniunii*

Europene sau la o dată ulterioară specificată în decizie. Aceasta nu aduce atingere valabilității actelor delegate aflate deja în vigoare.

4. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

5. Un act delegat adoptat în temeiul articolului 8 alineatul (3), articolului 13 alineatul (5), articolului 15 alineatul (5), articolului 16 alineatul (5), articolului 18 alineatul (5), articolului 20 alineatul (6), articolului 21 alineatul (4), articolului 23 alineatul (3), articolului 25 alineatul (2), articolului 27 alineatul (2), articolului 28 alineatul (6), articolului 29 alineatul (4), articolului 30 alineatul (2), articolului 31, articolului 35 alineatul (3) și articolului 37 alineatul (3) intră în vigoare numai în cazul în care Parlamentul European sau Consiliul nu a exprimat nicio obiecție în termen de două luni de la notificarea actului respectiv Parlamentului European și Consiliului sau dacă, înainte de expirarea termenului respectiv, atât Parlamentul European, cât și Consiliul informează Comisia că nu vor formula obiecții. La inițiativa Parlamentului European sau a Consiliului, termenul respectiv se prelungește cu două luni.

CAPITOLUL V

ACTE DE PUNERE ÎN APLICARE

Articolul 39

Procedura comitetelor

1. Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.

2. Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

CAPITOLUL VI

DISPOZIȚII FINALE

Articolul 40

Raportare

Comisia prezintă Parlamentului European și Consiliului rapoarte cu privire la aplicarea prezentului regulament. Primul raport se transmite în termen de cel mult patru ani de la data intrării în vigoare a prezentului regulament. Ulterior, următoarele rapoarte se transmit o dată la patru ani.

Articolul 41

Abrogare

1. Directiva 1999/93/CE se abrogă.

2. Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament.

3. Dispozitivele sigure de creare a semnăturilor a căror conformitate a fost determinată în conformitate cu articolul 3 alineatul (4) din Directiva 1999/93/CE sunt considerate dispozitive de creare a semnăturilor calificate în temeiul prezentului regulament.

4. Certificatele calificate emise în temeiul Directivei 1999/93/CE sunt considerate certificate calificate pentru semnături electronice în temeiul prezentului regulament până la expirare, dar nu mai mult de cinci ani de la intrarea în vigoare a prezentului regulament.

Articolul 42

Intrarea în vigoare

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

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

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

ANEXA I

Cerințe pentru certificatele calificate pentru semnături electronice

Certificatele calificate pentru semnături electronice conțin:

(a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice;

(b) un set de date reprezintă fără ambiguitate prestatorul de servicii de asigurare a încrederii calificat care emite certificatele calificate care includ cel puțin statul membru în care este stabilit prestatorul respectiv și

– pentru o persoană juridică: numele și numărul de înregistrare astfel cum se menționează în registrele oficiale,

– pentru o persoană fizică: numele persoanei;

(c) un set de date care reprezintă fără ambiguitate semnatarul căruia i-a fost emis certificatul care include cel puțin numele semnatarului sau un pseudonim, care este identificat ca atare;

(d) datele de validare a semnăturilor electronice care corespund datelor de creare a semnăturilor electronice;

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

(f) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de asigurare a încrederii calificat;

(g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de asigurare a încrederii calificat emitent;

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

(i) localizarea serviciilor privind statutul valabilității certificatului care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat;

(j) în cazul în care datele de creare a semnăturilor electronice legate de datele de validare a semnăturilor electronice sunt situate într-un dispozitiv de creare a semnăturilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.

ANEXA II

Cerințe pentru dispozitivele de creare a semnăturilor calificate

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

(a) secretul datelor de creare a semnăturilor electronice utilizate pentru generarea semnăturii electronice este asigurat;

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

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

(d) datele de creare a semnăturilor electronice utilizate pentru generarea semnăturilor 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.

3. Generarea sau gestionarea datelor de creare a semnăturilor electronice în numele semnatarului se realizează de către un prestator de servicii de asigurare a încrederii calificat.

4. Prestatorii de servicii de asigurare a încrederii calificați care gestionează datele de creare a semnăturilor electronice în numele semnatarului pot duplica datele de creare a semnăturilor electronice în scopul de a le avea de rezervă, cu condiția ca următoarele cerințe să fie îndeplinite:

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

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

ANEXA III

Cerințe pentru certificatele calificate pentru sigilii electronice

Certificatele calificate pentru sigilii electronice conțin:

(a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru sigilii electronice;

(b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de asigurare a încrederii calificat care emite certificatele calificate care include cel puțin statul membru în care este stabilit prestatorul respectiv și

– pentru o persoană juridică: numele și numărul de înregistrare astfel cum se menționează în registrele oficiale,

– pentru o persoană fizică: numele persoanei;

(c) un set de date care reprezintă fără ambiguitate persoana juridică căreia i s-a emis certificatul, care include cel puțin numele și numărul de înregistrare astfel cum se menționează în registrele oficiale;

(d) datele de validare a sigiliilor electronice care corespund datelor de creare a sigiliilor electronice;

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

(f) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de asigurare a încrederii calificat;

(g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de asigurare a încrederii calificat emitent;

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

(i) localizarea serviciilor privind statutul valabilității certificatului care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat;

(j) în cazul în care datele de creare a sigiliilor electronice legate de datele de validare a sigiliilor electronice sunt situate într-un dispozitiv de creare a sigiliilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.

ANEXA IV

Cerințe pentru certificatele calificate pentru autentificarea unui site internet

Certificatele calificate pentru autentificarea unui site internet conțin:

(a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unui site internet;

(b) un set de date care reprezintă fără ambiguitate prestatorul de servicii de asigurare a încrederii calificat care emite certificatele calificate care include cel puțin statul membru în care este stabilit prestatorul respectiv și

– pentru o persoană juridică: numele și numărul de înregistrare astfel cum se menționează în registrele oficiale,

– pentru o persoană fizică: numele persoanei;

(c) un set de date care reprezintă fără ambiguitate persoana juridică căreia i s-a emis certificatul, care include cel puțin numele și numărul de înregistrare astfel cum se menționează în registrele oficiale;

(d) elemente ale adresei, care includ cel puțin orașul și statul membru, ale persoanei juridice căreia i s-a emis certificatul, astfel cum se menționează în registrele oficiale;

(e) numele domeniului gestionat de persoana juridică căreia i s-a emis certificatul;

(f) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului;

(g) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de asigurare a încrederii calificat;

(h) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de asigurare a încrederii calificat emitent;

(i) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (g) este disponibil gratuit;

(j) localizarea serviciilor privind statutul valabilității certificatului care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat.

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

Prezenta fișă financiară detaliază cerințele în ceea ce privește cheltuielile administrative în vederea punerii în aplicare a regulamentului propus *privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă*.

În urma procedurii legislative și a discuției pentru adoptarea de către Parlamentul European și Consiliu a regulamentului propus, Comisia va avea nevoie de douăsprezece persoane ocupate în echivalent normă întreagă (ENI) pentru a elabora actele delegate și de punere în aplicare conexe, pentru a asigura disponibilitatea standardelor organizaționale și tehnice, pentru a trata informațiile notificate de statele membre, în special pentru a menține informațiile referitoare la listele sigure, pentru a asigura sensibilizarea părților interesate – în special cetățeni și IMM-uri – cu privire la avantajele utilizării identificării, autentificării și semnăturii electronice și a serviciilor conexe de asigurare a încrederii și pentru a angaja discuții cu țările terțe în vederea realizării interoperabilității identificării, autentificării și semnăturii electronice și a serviciilor conexe de asigurare a încrederii la nivel mondial.

1.1. Denumirea propunerii/inițiativei

Propunere a Comisiei de regulament privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB[25]

09 SOCIETATEA INFORMAȚIONALĂ

1.3. Tipul propunerii/inițiativei

☐ Propunerea/inițiativa se referă la **o acțiune nouă**

☐ Propunerea/inițiativa se referă la **o acțiune nouă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[26]

☐ Propunerea/inițiativa se referă la **prelungirea unei acțiuni existente**

☑ Propunerea/inițiativa se referă la **o acțiune reorientată către o acțiune nouă**

25 ABM (Activity Based Management): gestionarea pe activități – ABB (Activity Based Budgeting): stabilirea bugetului pe activități.

26 Astfel cum se menționează la articolul 49 alineatul (6) litera (a) sau (b) din Regulamentul financiar.

1.4. Obiective

1.4.1. Obiectivul (obiectivele) strategic(e) multianual(e) al(e) Comisiei vizat(e) de propunere/inițiativă

Obiectivele generale ale propunerii sunt cele din politicile generale ale UE în care se situează propunerea, precum Strategia UE 2020. Aceasta vizează să garanteze că Europa ar „fi transformată într-o economie inteligentă, durabilă și favorabilă incluziunii, care obține un nivel ridicat de ocupare a forței de muncă, de productivitate și de coeziune socială.”

1.4.2. Obiectiv(e) specific(e) și activitatea (activitățile) ABM/ABB în cauză

Pentru a spori încrederea în tranzacțiile electronice paneuropene și pentru a asigura recunoașterea juridică transfrontalieră a identificării, autentificării și semnăturii electronice și a serviciilor conexe de asigurare a încrederii, precum și un nivel ridicat de protecție a datelor și responsabilizarea utilizatorilor pe piața unică (a se vedea Agenda digitală pentru Europa, acțiunile-cheie 3 și 16).

Activitatea (activitățile) ABM/ABB în cauză

09 02 - Cadru de reglementare pentru Agenda digitală pentru Europa

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/grupurilor vizate.

Stabilirea unui mediu de reglementare clar pentru identificarea, autentificarea și semnătura electronică și serviciile conexe de asigurare a încrederii, care ar spori confortul și încrederea utilizatorilor în lumea digitală.

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

1. Existența furnizorilor de identificare, autentificare și semnătură electronică și servicii conexe de asigurare a încrederii care desfășoară activități în mai multe state membre ale UE:

2. Gradul de interoperabilitate pe care îl ating dispozitivele (de exemplu, dispozitive de citire a cardurilor cu memorie) între sectoare și țări;

3. Utilizarea identificării, autentificării și semnăturii electronice și a serviciilor conexe de asigurare a încrederii de către toate categoriilor de populație;

4. Măsura în care identificarea, autentificarea și semnătura electronică și serviciile conexe de asigurare a încrederii sunt utilizate de către utilizatorii finali pentru tranzacțiile naționale și internaționale (transfrontaliere);

5. Gradul de armonizare între statele membre a legislației privind identificarea, autentificarea și semnătura electronică și serviciile conexe de asigurare a încrederii;

6. Sistemele de identificare electronică notificate Comisiei;

7. Servicii accesibile prin mijloace notificate de identificare electronică în sectorul public (de exemplu, e-guvernare, e-sănătate, e-justiție și achiziții publice electronice);

8. Servicii accesibile prin mijloace notificate de identificare electronică în sectorul privat (de exemplu, servicii bancare online, comerț electronic, jocuri de noroc online, conectare la site-uri internet și servicii de internet mai sigure).

1.5. Motivul (motivele) propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung

Divergențele în ceea ce privește punerea în aplicare la nivel național a directivei privind semnătura electronică ca urmare a diferitelor interpretări ale statelor membre conduc la probleme de interoperabilitate transfrontalieră, și, astfel, la o situație segmentată în UE și la denaturări pe piața internă. Acestea sunt însoțite de o lipsă de încredere în sistemele electronice care împiedică cetățenii europeni să beneficieze de același tip de servicii în mediul digital ca și în viața reală.

1.5.2. Valoarea adăugată a implicării UE

Acțiunea la nivelul UE ar prezenta avantaje clare în comparație cu acțiunea la nivelul statelor membre. Experiența a arătat, într-adevăr, că măsurile naționale nu sunt numai insuficiente pentru a face ca tranzacțiile electronice să devină posibile peste granițe, ci dimpotrivă, au creat obstacole în calea interoperabilității semnăturilor electronice la nivelul UE și au în prezent același efect pentru identificarea electronică, autentificarea electronică și serviciile conexe de asigurare a încrederii.

1.5.3. Învățăminte desprinse din experiențe anterioare similare

Propunerea se bazează pe experiența acumulată în contextul directivei privind semnătura electronică și pe problemele întâlnite din cauza transpunerii și punerii în aplicare fragmentate a directivei respective, care au împiedicat-o să își realizeze obiectivele.

1.5.4. Coerența și posibila sinergie cu alte instrumente relevante

Mai multe alte inițiative ale UE care vizează eliminarea problemelor legate de interoperabilitate și de recunoașterea și acceptarea transfrontalieră referitoare la anumite tipuri de interacțiuni electronice, de exemplu, directiva privind serviciile, directivele privind achizițiile publice, directiva TVA revizuită (facturarea electronică) sau regulamentul privind inițiativa cetățenească europeană fac referire la directiva privind semnătura electronică.

În plus, regulamentul propus va oferi un cadru juridic benefic pentru adoptarea generalizată a proiectelor-pilot la scară largă care au fost instituite la nivelul UE pentru a sprijini dezvoltarea mijloacelor de comunicare electronică interoperabile și demne de încredere (inclusiv SPOCS, care sprijină punerea în aplicare a directivei privind serviciile; STORK, care sprijină elaborarea și utilizarea identificărilor electronice interoperabile; PEPPOL, care sprijină elaborarea și utilizarea soluțiilor interoperabile în domeniul achizițiilor publice electronice; epSOS, care sprijină

elaborarea și utilizarea soluțiilor interoperabile în domeniul e-sănătății; eCodex, care sprijină elaborarea și utilizarea soluțiilor interoperabile în domeniul e-justiției).

1.6. Durata și impactul financiar

☐ Propunere/inițiativă cu **durată limitată**

– ☐ Propunere/inițiativă în vigoare din [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ Impact financiar din AAAA până în AAAA

☑ Propunere/inițiativă cu **durată nelimitată**

1.7. Modul (modurile) de gestiune preconizat(e)[27]

☑ **Gestiune centralizată directă** de către Comisie

☐ **Gestiune centralizată indirectă**, prin delegarea sarcinilor de execuție către:

– ☐ agenții executive

– ☐ organisme instituite de Comunități[28]

– ☐ organisme publice naționale/organisme cu misiune de serviciu public

– ☐ persoane cărora li se încredințează executarea unor acțiuni specifice în temeiul titlului V din Tratatul privind Uniunea Europeană, identificate în actul de bază relevant în sensul articolului 49 din Regulamentul financiar

☐ **Gestiune partajată** cu statele membre

☐ **Gestiune descentralizată** împreună cu țări terțe

☐ **Gestiune în comun** cu organizații internaționale ***(a se preciza)***

Dacă se indică mai multe moduri de gestiune, se furnizează detalii suplimentare în secțiunea „Observații”.

Observații

[//]

[27] Detalii privind modurile de gestionare, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[28] Astfel cum sunt menționate la articolul 185 din Regulamentul financiar.

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Prima evaluare va avea loc la patru ani după intrarea în vigoare a regulamentului. În regulament este inclusă o clauză explicită privind raportul pe care Comisia îl va prezenta Parlamentului European și Consiliului privind punerea în aplicare a regulamentului. Ulterior, următoarele rapoarte vor fi transmise o dată la patru ani. Se va aplica metodologia Comisiei privind evaluarea. Aceste evaluări vor fi efectuate cu ajutorul unor studii specifice privind punerea în aplicare a instrumentelor juridice, al unor chestionare adresate autorităților naționale, al unor discuții cu experți, al unor ateliere, al unor sondaje Eurobarometru etc.

2.2. Sistemul de gestiune și control

2.2.1. Riscul (riscurile) identificat(e)

S-a efectuat o evaluare a impactului care să însoțească propunerea de regulament. Noul instrument juridic va prevedea recunoașterea și acceptarea reciprocă a identificării electronice peste granițe, îmbunătățirea cadrului actual privind semnăturile electronice, consolidarea supravegherii naționale a prestatorilor de servicii de asigurare a încrederii și oferirea de efect juridic și recunoaștere juridică serviciilor conexe de asigurare a încrederii. Acesta introduce, de asemenea, utilizarea actelor delegate și de punere în aplicare ca un mecanism care să asigure flexibilitate în raport cu evoluțiile tehnologice.

2.2.2. Metoda (metodele) de control preconizată (preconizate)

Metodele de control existente aplicate de către Comisie vor acoperi creditele suplimentare.

2.3. Măsurile de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate.

Măsurile existente de prevenire a fraudelor aplicate de către Comisie vor acoperi creditele suplimentare.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare de cheltuieli existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tip de cheltuieli	Contribuție			
	Numărul [Descrierea……...…….]	Dif./ Nedif. (29)	din partea țărilor AELS[30]	din partea țărilor candidate[31]	din partea țărilor terțe	în sensul articolului 18 alineatul (1) litera (aa) din Regulamentul financiar
5	09. 01 01 01 Cheltuieli cu personalul în activitate din cadrul Direcției Generale Societatea Informațională și Media	Nedif.	NU	NU	NU	NU
5	09. 01 02 01 Personal extern	Nedif.	NU	NU	NU	NU

29 Dif. = credite diferențiate / Nedif. = credite nediferențiate

30 AELS: Asociația Europeană a Liberului Schimb.

31 Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

Rubrica din cadrul financiar multianual:	Numărul	[Rubrica 1. **Creștere inteligentă și favorabilă incluziunii** ……..……]

DG: INFSO			Anul **2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul 2018	**Anul 2019**	**Anul 2020**	**TOTAL**
• Credite operaționale										
Numărul liniei bugetare - N.A.	Angajamente	(1)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Plăți	(2)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Numărul liniei bugetare - N.A.	Angajamente	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Plăți	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Credite cu caracter administrativ finanțate din bugetul anumitor programe[32]			0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Numărul liniei bugetare		(3)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
TOTAL credite pentru DG INFSO	Angajamente	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
	Plăți	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**

Rubrica din cadrul financiar multianual:	**5**	„Cheltuieli administrative”

[32] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

milioane EUR (cu 3 zecimale)

		Anul **2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
		DG: INFSO							
• Resurse umane		1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**
• Alte cheltuieli administrative									
TOTAL DG INFSO	Credite	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

TOTAL credite în cadrul RUBRICII 5 din cadrul financiar multianual	(Total angajamente = Total plăți)	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

milioane EUR (cu 3 zecimale)

		Anul **2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1 - 5 din cadrul financiar multianual	Angajamente	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**
	Plăți	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

3.2.2. Impactul estimat asupra creditelor operaționale

– ☑ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☐ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.3.1. Sinteză

– ☐ Propunerea/inițiativa nu implică utilizarea de credite administrative

– ☑ Propunerea/inițiativa implică utilizarea de credite administrative, conform explicațiilor de mai jos:

milioane EUR (cu 3 zecimale)

	Anul **N 2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**	**TOTAL**
RUBRICA 5 din cadrul financiar multianual								
Resurse umane	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**
Alte cheltuieli administrative								
Subtotal RUBRICA 5 din cadrul financiar multianual	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

În afara RUBRICII 5[33] din cadrul financiar multianual								
Resurse umane								
Alte cheltuieli cu caracter administrativ								
Subtotal în afara RUBRICII 5 din cadrul financiar multianual								

TOTAL	1 344	1 344	1 344	1 344	1 344	1 344	1 344	**9 408**

[33] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.3.2. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane

– ☑ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimarea trebuie exprimată în valoare întreagă (sau cel mult cu o zecimală)

		Anul **2014**	Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anul **2019**	Anul **2020**
• Posturi din schema de personal (posturi de funcționari și de agenți temporari)								
09 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)		9	9	9	9	9	9	9
XX 01 01 02 (în delegații)								
XX 01 05 01 (cercetare indirectă)								
10 01 05 01 (cercetare directă)								
• Personal extern (în unități echivalent normă întreagă: ENI)[34]								
09 01 02 01 (AC, INT, END din „pachetul global")		3	3	3	3	3	3	3
XX 01 02 02 (AC, INT, JED, AL și END în delegații)								
XX 01 04 ***yy***[35]	- la sediu[36]							
	- în delegații							
XX 01 05 02 (AC, INT, END - în cadrul cercetării indirecte)								
10 01 05 02 (AC, INT, END - în cadrul cercetării directe)								
Alte linii bugetare (a se preciza)								
TOTAL		**12**	**12**	**12**	**12**	**12**	**12**	**12**

Necesarul de resurse umane va fi acoperit de efectivele de personal ale DG-ului în cauză alocate deja gestionării acțiunii și/sau realocate intern în cadrul DG-ului, completate, după caz, prin resurse suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	Gestionarea procedurilor legislative pentru adoptarea de către Parlamentul European și Consiliu a regulamentului planificat și a actelor delegate/de punere în aplicare conexe. Domenii prioritare: 1. Stabilirea unui nou cadru legislativ privind serviciile electronice de asigurare a încrederii 2. Stimularea adoptării serviciilor electronice de asigurare a încrederii prin sporirea sensibilizării IMM-urilor și a cetățenilor cu privire la potențialul lor 3. Monitorizarea Directivei 1999/93/CE, inclusiv aspectele internaționale 4. Exploatarea efectului de pârghie a proiectelor-pilot la scară largă pentru a accelera

34 AC= agent contractual; INT = personal pus la dispoziție de agenți de muncă temporară („Intérimaire"); JED = „Jeune Expert en Délégation" (expert tânăr în delegații); AL= agent local; END= expert național detașat.

35 Sub plafonul pentru personal extern din credite operaționale (fostele linii „BA").

36 În special pentru fonduri structurale, Fondul european agricol pentru dezvoltare rurală (FEADR) și Fondul european pentru pescuit (FEP).

	realizarea concretă a obiectivul noului cadru legislativ.
Personal extern	La fel ca mai sus

3.2.4. Compatibilitatea cu cadrul financiar multianual existent

– ☑ Propunerea/inițiativa este compatibilă cu cadrul financiar multianual existent.

– ☐ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

A se explica reprogramarea necesară, precizându-se liniile bugetare în cauză și sumele aferente.

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual[37].

A se explica acțiunea necesară, precizând rubricile și liniile bugetare în cauză, precum și sumele aferente.

3.2.5. Participarea terților

– ☑ Propunerea/inițiativa nu prevede cofinanțare din partea terților

– ☐ Propunerea/inițiativa prevede cofinanțare, estimată în cele ce urmează:

3.3. Impactul estimat asupra veniturilor

– ☑ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

- ☐ asupra resurselor proprii
- ☐ asupra diverselor venituri

[37] A se vedea punctele 19 și 24 din Acordul interinstituțional.