►B REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 23 iulie 2014

privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE

(JO L 257, 28.8.2014, p. 73)

rectificat prin:

►C1 Rectificare, JO L 110, 30.4.2018, p. 141 (910/2014)

▼B

REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 23 iulie 2014

privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect

În vederea asigurării bunei funcționări a pieței interne, vizând în același timp un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere, prezentul regulament:

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

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

(c) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unui site internet.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică sistemelor de identificare electronică care au fost notificate de către un stat membru și prestatorilor de servicii de încredere cu sediul în Uniune.

(2) Prezentul regulament nu se aplică prestării de servicii de încredere care sunt utilizate exclusiv în sisteme închise care decurg din dreptul intern sau din acordurile încheiate între un set definit de participanți.

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

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 unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;

▼B

2. „mijloace de identificare electronică” înseamnă o unitate materială și/sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării unui serviciu online;

3. „date de identificare personală” înseamnă un set de date care permit stabilirea identității unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;

4. „sistem de identificare electronică” înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice sau persoane fizice reprezentând persoane juridice;

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

6. „beneficiar” înseamnă o persoană fizică sau juridică care beneficiază de un serviciu de identificare electronică sau de un serviciu de încredere;

7. „organism din sectorul public” înseamnă un stat, o autoritate regională sau locală, un organism de drept public sau o asociație formată din una sau mai multe astfel de autorități sau din unul sau mai multe astfel de organisme de drept public; sau o entitate privată mandatată de cel puțin una dintre aceste autorități, organisme sau asociații să presteze servicii publice atunci când acționează în temeiul unui astfel de mandat;

8. „organism de drept public” înseamnă un organism astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE a Parlamentului European și a Consiliului ([1]);

9. „semnatar” înseamnă o persoană fizică care creează o semnătură electronică;

10. „semnătură electronică” înseamnă date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;

11. „semnătură electronică avansată” înseamnă o semnătură electronică ce îndeplinește cerințele prevăzute la articolul 26;

12. „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;

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

([1]) Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65).

▼B

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

15. „certificat calificat pentru semnătură electronică” înseamnă un certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa I;

16. „serviciu de încredere” înseamnă un serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în:

    (a) crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective; sau

    (b) crearea, verificarea și validarea certificatelor pentru autentificarea unui site internet; sau

    (c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;

17. „serviciu de încredere calificat” înseamnă un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezentul regulament;

18. „organism de evaluare a conformității” înseamnă un organism definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care este acreditat în conformitate cu regulamentul în cauză ca fiind competent să efectueze evaluarea conformității unui prestator de servicii de încredere calificat și a serviciilor de încredere calificate pe care acesta le prestează;

19. „prestator de servicii de încredere” înseamnă o persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;

20. „prestator de servicii de încredere calificat” înseamnă un prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere;

21. „produs” înseamnă hardware sau software sau componente relevante de hardware sau software, destinate să fie utilizate pentru prestarea de servicii de încredere;

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

23. „dispozitiv de creare a semnăturilor electronice calificat” înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în anexa II;

24. „creatorul unui sigiliu” înseamnă o persoană juridică care creează un sigiliu electronic;

▼B

25. „sigiliu electronic” înseamnă date în format electronic ataşate la sau asociate logic cu alte date în format electronic pentru asigurarea originii şi integrităţii acestora din urmă;

26. „sigiliu electronic avansat” înseamnă un sigiliu electronic care îndeplineşte cerinţele prevăzute la articolul 36;

27. „sigiliu electronic calificat” înseamnă un sigiliu electronic avansat care este creat de un dispozitiv de creare a sigiliilor electronice calificat şi care se bazează pe un certificat calificat pentru sigiliile electronice;

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

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

30. „certificat calificat pentru sigiliul electronic” înseamnă un certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat şi care îndeplineşte cerinţele prevăzute în anexa III;

31. „dispozitiv de creare a sigiliului electronic” înseamnă software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;

32. „dispozitiv de creare a sigiliului electronic calificat” înseamnă un dispozitiv de creare a sigiliului electronic care îndeplineşte *mutatis mutandis* cerinţele prevăzute în anexa II;

33. „marcă temporală electronică” înseamnă date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind dovezi că acestea din urmă au existat la acel moment;

34. „marcă temporală electronică calificată” înseamnă o marcă temporală electronică care îndeplineşte cerinţele prevăzute la articolul 42;

35. „document electronic” înseamnă orice conţinut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;

36. „serviciu de distribuţie electronică înregistrată” înseamnă un serviciu care permite transmiterea de date între părţi terţe prin mijloace electronice şi furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea şi primirea datelor şi care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;

37. „serviciu de distribuţie electronică înregistrată calificat” înseamnă un serviciu de distribuţie electronică înregistrată care îndeplineşte cerinţele prevăzute la articolul 44;

38. „certificat pentru autentificarea unui site internet” înseamnă o atestare care face posibilă autentificarea unui site internet şi face legătura între site-ul internet şi persoana fizică sau juridică căreia i s-a emis certificatul;

▼B

39. „certificat calificat pentru autentificarea unui site internet” înseamnă un certificat pentru autentificarea unui site internet care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa IV;

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

41. „validare” înseamnă procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.

Articolul 4

Principiul pieței interne

(1) Nu există nicio restricție privind prestarea de servicii de încredere pe teritoriul unui stat membru de către un prestator de servicii de încredere stabilit în alt stat membru, din motive care se încadrează în domeniile reglementate de prezentul regulament.

(2) Produsele și serviciile de încredere care sunt conforme cu prezentul regulament sunt autorizate pentru a circula liber pe piața internă.

Articolul 5

Prelucrarea și protecția datelor

(1) Prelucrarea datelor cu caracter personal se efectuează în conformitate cu Directiva 95/46/CE.

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

CAPITOLUL II

IDENTIFICARE ELECTRONICĂ

Articolul 6

Recunoașterea reciprocă

(1) Atunci când este necesară o identificare electronică care utilizează un mijloc de identificare electronică și o autentificare în temeiul dreptului intern sau al practicii administrative naționale pentru a accesa un serviciu prestat online de un organism din sectorul public într-un stat membru, mijloacele de identificare electronică emise într-un alt stat membru sunt recunoscute în primul stat membru în scopul autentificării transfrontaliere a respectivului serviciu online, cu condiția să fie îndeplinite următoarele condiții:

(a) mijloacele de identificare electronică să fie emise în cadrul unui sistem de identificare electronică inclus în lista publicată de Comisie în temeiul articolului 9;

(b) nivelul de asigurare al respectivelor mijloace de identificare electronică să corespundă unui nivel de asigurare egal sau mai ridicat decât nivelul de asigurare impus de organismul din sectorul public relevant pentru a accesa respectivul serviciu online în primul stat membru, cu condiția ca nivelul de asigurare al mijloacelor de identificare electronică respective să corespundă nivelului de asigurare substanțial sau ridicat;

▼B

(c) organismul din sectorul public relevant utilizează nivelul de asigurare „substanțial” sau „ridicat” în legătură cu accesarea online a serviciului respectiv.

Această recunoaștere trebuie să aibă loc în termen de cel mult 12 luni de la publicarea de către Comisie a listei menționate la primul paragraf litera (a).

(2) Mijloacele de identificare electronică eliberate în temeiul unui sistem de identificare electronică inclus în lista publicată de Comisie în conformitate cu articolul 9 și care corespund nivelului de asigurare scăzut pot fi recunoscute de către organismele din sectorul public în scopul autentificării transfrontaliere pentru serviciul furnizat online de către organismele respective.

Articolul 7

Eligibilitatea pentru notificarea sistemelor de identificare electronică

Un sistem de identificare electronică este eligibil pentru notificare în temeiul articolului 9 alineatul (1) în cazul în care sunt îndeplinite toate condițiile de mai jos:

(a) mijloacele de identificare electronică din cadrul sistemului de identificare electronică sunt emise:

(i) de statul membru care notifică;

(ii) pe baza unui mandat din partea statului membru care notifică; sau

(iii) independent de statul membru care notifică și sunt recunoscute de respectivul stat membru;

(b) mijloacele de identificare electronică din cadrul sistemului de identificare electronică pot fi utilizate pentru a accesa cel puțin un serviciu care este prestat de un organism din sectorul public și care necesită identificarea electronică în statul membru care notifică;

(c) sistemul de identificare electronică și mijloacele de identificare electronică emise în temeiul acestuia îndeplinesc cerințele aferente cel puțin unuia dintre nivelurile de asigurare prevăzute în actul de punere în aplicare menționat la articolul 8 alineatul (3);

(d) statul membru care notifică se asigură că datele de identificare personală, reprezentând în mod unic persoana în cauză, sunt atribuite, în conformitate cu specificațiile, standardele și procedurile tehnice aferente nivelului de asigurare relevant prevăzut în actul de punere în aplicare menționat la articolul 8 alineatul (3), persoanei fizice sau juridice menționate la articolul 3 punctul 1 la momentul emiterii mijloacelor de identificare electronică din cadrul sistemului respectiv;

(e) partea care emite mijloacele de identificare electronică din cadrul respectivului sistem se asigură că mijloacele de identificare electronică sunt atribuite persoanelor menționate la litera (d) de la prezentul articol, în conformitate cu specificațiile tehnice, standardele și procedurile aferente nivelului de asigurare corespunzător prevăzut în actul de punere în aplicare menționat la articolul 8 alineatul (3);

(f) statul membru care notifică asigură disponibilitatea autentificării online, astfel încât orice beneficiar stabilit pe teritoriul altui stat membru să poată confirma datele de identificare personală primite în format electronic.

▼B

În cazul altor beneficiari decât organismele din sectorul public, statul membru care notifică poate defini condițiile de acces la mijlocul respectiv de autentificare. Autentificarea transfrontalieră este furnizată gratuit atunci când este efectuată în legătură cu un serviciu online prestat de un organism din sectorul public.

Statele membre nu impun nicio cerință tehnică specifică disproporționată beneficiarilor care intenționează să efectueze o astfel de autentificare, atunci când astfel de cerințe împiedică sau afectează semnificativ interoperabilitatea sistemelor de identificare electronică notificate;

(g) cu cel puțin șase luni înaintea notificării în conformitate cu articolul 9 alineatul (1), statul membru care notifică furnizează celorlalte state membre, în scopul îndeplinirii obligației prevăzute la articolul 12 alineatul (5), o descriere a sistemului respectiv în conformitate cu modalitățile prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul (7);

(h) sistemul de identificare electronică îndeplinește cerințele prevăzute în actul de punere în aplicare menționat la articolul 12 alineatul (8).

Articolul 8

Niveluri de asigurare ale mijloacelor de identificare electronică

(1) Un sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) specifică nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare electronică emise în cadrul sistemului respectiv.

(2) Nivelurile de asigurare scăzut, substanțial și ridicat îndeplinesc următoarele criterii, respectiv:

(a) nivelul de asigurare scăzut se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității;

(b) nivelul de asigurare substanțial se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității;

(c) nivelul de asigurare ridicat se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad mai ridicat de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane decât mijloacele de identificare electronică cu nivel de asigurare substanțial și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a împiedica utilizarea frauduloasă sau modificarea frauduloasă a identității.

(3) Până la 18 septembrie 2015, ținând cont de standardele internaționale relevante și sub rezerva alineatului (2), Comisia, prin intermediul unor acte de punere în aplicare, stabilește specificații tehnice, standarde și proceduri minime, în raport cu care sunt specificate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică în sensul alineatului (1).

▼B

Aceste specificații tehnice, standarde și proceduri minime se stabilesc prin trimitere la fiabilitatea și calitatea următoarelor elemente:

(a) procedura de dovedire și de verificare a identității persoanelor fizice sau juridice care solicită emiterea mijloacelor de identificare electronică;

(b) procedura pentru emiterea mijloacelor de identificare electronică solicitate;

(c) mecanismul de autentificare, prin care persoana fizică sau juridică utilizează mijloacele de identificare electronică pentru a confirma identitatea sa unui beneficiar;

(d) entitatea care emite mijloacele de identificare electronică;

(e) oricare alt organism implicat în solicitarea emiterii mijloacelor de identificare electronică; și

(f) specificațiile tehnice și de securitate ale mijloacelor de identificare electronică emise.

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

Articolul 9

Notificarea

(1) Statul membru care notifică înaintează Comisiei următoarele informații și, fără întârzieri nejustificate, orice modificări ulterioare ale acestora:

(a) o descriere a sistemului de identificare electronică notificat, incluzând nivelurile sale de asigurare și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului;

(b) regimul de supraveghere aplicabil și informații privind regimul de răspundere referitor la următoarele aspecte:

(i) partea care emite mijloacele de identificare electronică; și

(ii) partea care desfășoară procedura de autentificare;

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

(d) informații privind entitatea sau entitățile care gestionează înregistrarea datelor unice de identificare personală;

(e) o descriere a modului în care sunt îndeplinite cerințele prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul (8);

(f) o descriere a autentificării menționate la articolul 7 litera (f);

(g) dispoziții pentru suspendarea sau revocarea sistemului de identificare electronică notificat, a autentificării sau a părților compromise în cauză.

(2) La un an de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8), Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a sistemelor de identificare electronică care au fost notificate în temeiul alineatului (1) de la prezentul articol și informațiile de bază cu privire la acestea.

▼B

(3) În cazul în care Comisia primește o notificare după expirarea perioadei menționate la alineatul (2), aceasta publică în *Jurnalul Oficial al Uniunii Europene* modificările la lista menționată la alineatul (2) în termen de două luni de la data primirii respectivei notificări.

(4) Un stat membru poate înainta Comisiei o cerere de eliminare a unui sistem de identificare electronică notificat de respectivul stat membru din lista menționată la alineatul (2). Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările corespunzătoare aduse listei, în termen de o lună de la primirea cererii statului membru.

(5) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească circumstanțele, formatele și procedurile pentru notificările în temeiul alineatului (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 10

Încălcarea securității

(1) În cazul în care fie sistemul de identificare electronică notificat în conformitate cu articolul 9 alineatul (1), fie autentificarea menționată la articolul 7 litera (f) este încălcată sau parțial compromisă într-un mod care afectează fiabilitatea autentificării transfrontaliere a sistemului respectiv, statul membru care notifică suspendă sau revocă, fără întârziere, respectiva autentificare transfrontalieră sau părțile compromise în cauză și informează celelalte state membre și Comisia.

(2) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) este remediată, statul membru care notifică reinstituie autentificarea transfrontalieră și informează celelalte state membre și Comisia fără întârzieri nejustificate.

(3) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) nu este remediată în termen de trei luni de la suspendare sau revocare, statul membru care notifică comunică celorlalte state membre și Comisiei retragerea sistemului de identificare electronică.

Comisia publică în *Jurnalul Oficial al Uniunii Europene*, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la articolul 9 alineatul (2).

Articolul 11

Răspunderea

(1) Statul membru care notifică este răspunzător pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligațiilor care îi revin în temeiul articolului 7 literele (d) și (f).

(2) Partea care emite mijloacele de identificare electronică este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligației menționate la articolul 7 litera (e).

(3) Partea care execută procedura de autentificare este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere pentru neasigurarea executării corecte a autentificării menționate la articolul 7 litera (f).

▼B

(4) Alineatele (1), (2) și (3) se aplică în conformitate cu normele de drept intern privind răspunderea.

(5) Alineatele (1), (2) și (3) nu aduc atingere răspunderii care revine, în conformitate cu dreptul intern, părților la o tranzacție în care sunt utilizate mijloace de identificare electronică care intră sub incidența sistemului de identificare electronică notificat în temeiul articolului 9 alineatul (1).

Articolul 12

Cooperarea și interoperabilitatea

(1) Sistemele naționale de identificare electronică notificate în temeiul articolului 9 alineatul (1) sunt interoperabile.

(2) În sensul alineatului (1), se stabilește un cadru de interoperabilitate.

(3) Cadrul de interoperabilitate îndeplinește următoarele criterii:

(a) urmărește să fie neutru din punctul de vedere al tehnologiei și nu acordă prioritate niciuneia dintre soluțiile tehnice naționale specifice pentru identificarea electronică pe teritoriul statului membru;

(b) respectă standardele europene și internaționale, atunci când este posibil;

(c) facilitează punerea în aplicare a principiului luării în considerare a vieții private începând cu momentul conceperii (*privacy by design*); și

(d) garantează că datele cu caracter personal sunt prelucrate în conformitate cu Directiva 95/46/CE.

(4) Cadru de interoperabilitate este alcătuit din următoarele elemente:

(a) o trimitere la cerințele tehnice minime aferente nivelurilor de asigurare menționate la articolul 8;

(b) o clasificare a nivelurilor naționale de asigurare aferente sistemelor de identificare electronică notificate în funcție de nivelurile de asigurare menționate la articolul 8;

(c) o trimitere la cerințele tehnice minime referitoare la interoperabilitate;

(d) o trimitere la un set minim de date de identificare personală, reprezentând în mod unic o persoană fizică sau juridică, care sunt disponibile din sistemele de identificare electronică;

(e) regulamentul de procedură;

(f) dispoziții referitoare la soluționarea litigiilor; și

(g) standarde de securitate operaționale comune.

(5) Statele membre cooperează cu privire la următoarele aspecte:

(a) interoperabilitatea sistemelor de identificare electronică notificate în conformitate cu articolul 9 alineatul (1) și a sistemelor de identificare electronică pe care statele membre intenționează să le notifice; și

(b) securitatea sistemelor de identificare electronică.

(6) Cooperarea dintre statele membre constă în:

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

▼B

(b) schimbul de informații, de experiență și de bune practici cu privire la modul de lucru cu nivelurile de asigurare ale sistemelor de identificare electronică menționate la articolul 8;

(c) evaluarea *inter pares* privind sistemele de identificare electronică care fac obiectul prezentului regulament; și

(d) analiza evoluțiilor relevante din domeniul identificării electronice.

(7) Până la 18 martie 2015, Comisia stabilește, prin intermediul actelor de punere în aplicare, modalitățile procedurale necesare pentru a facilita cooperarea între statele membre menționate la alineatele (5) și (6), în vederea stimulării unui nivel ridicat de încredere și securitate corespunzător gradului de risc.

(8) Până la 18 septembrie 2015, în vederea stabilirii de condiții uniforme pentru punerea în aplicare a cerinței menționate la alineatul (1), sub rezerva criteriilor stabilite la alineatul (3) și luând în considerare rezultatele cooperării dintre statele membre, Comisia adoptă acte de punere în aplicare privind cadrul de interoperabilitate, astfel cum este prevăzut la alineatul (4).

(9) Actele de punere în aplicare menționate la alineatele (7) și (8) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

CAPITOLUL III

SERVICII DE ÎNCREDERE

SECȚIUNEA 1

Dispoziții generale

Articolul 13

Răspunderea și sarcina probei

(1) Fără a aduce atingere alineatului (2), prestatorii de servicii de încredere sunt răspunzători pentru prejudiciile cauzate în mod intenționat sau din neglijență oricărei persoane fizice sau juridice ca urmare a nerespectării obligațiilor prevăzute în prezentul regulament.

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

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

(2) În cazul în care prestatorii de servicii de încredere își informează clienții în prealabil în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care aceștia le prestează și în cazul în care aceste restricții pot fi recunoscute de părțile terțe, prestatorii de servicii de încredere nu sunt răspunzători pentru prejudiciile rezultate din utilizarea serviciilor care depășesc restricțiile indicate.

(3) Alineatele (1) și (2) se aplică în conformitate cu normele de drept intern privind răspunderea.

▼B

Articolul 14

Aspecte internaționale

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

(2) Acordurile menționate la alineatul (1) garantează, în special, că:

(a) cerințele aplicabile prestatorilor de servicii de încredere calificați stabiliți în Uniune și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de prestatorii de servicii de încredere din țara terță sau de organizațiile internaționale cu care a fost încheiat acordul, precum și de serviciile de încredere pe care aceștia le prestează;

(b) serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune sunt recunoscute ca echivalente din punct de vedere juridic cu serviciile de încredere prestate de prestatorii de servicii de încredere din țara terță sau de organizația internațională cu care a fost încheiat acordul.

Articolul 15

Accesibilitatea pentru persoanele cu handicap

Dacă este posibil, serviciile de încredere prestate și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu handicap.

Articolul 16

Sancțiuni

Statele membre stabilesc normele referitoare la sancțiunile aplicabile în cazul încălcării prezentului regulament. Sancțiunile prevăzute sunt eficace, proporționale și disuasive.

SECȚIUNEA 2

Supravegherea

Articolul 17

Organismul de supraveghere

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

Organismelor de supraveghere li se conferă competențele necesare și resursele adecvate pentru exercitarea sarcinilor lor.

(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate.

(3) Rolul organismului de supraveghere constă în:

▼B

(a) supravegherea prestatorilor de servicii de încredere calificați stabiliți pe teritoriul statului membru care l-a desemnat pentru a se asigura, prin intermediul activităților de supraveghere *ex ante* și *ex post*, că respectivii prestatori de servicii de încredere calificați, precum și serviciile de încredere calificate pe care le prestează, îndeplinesc cerințele stabilite în prezentul regulament;

(b) luarea de măsuri, după caz, în legătură cu prestatorii de servicii de încredere necalificați stabiliți pe teritoriul statului membru care l-a desemnat, prin intermediul activităților de supraveghere *ex post*, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere calificați sau serviciile de încredere pe care le prestează nu îndeplinesc cerințele stabilite în prezentul regulament.

(4) În sensul alineatului (3) și sub rezerva restricțiilor prevăzute de acesta, sarcinile organismului de supraveghere includ, în special:

(a) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolul 18;

(b) să efectueze analiza rapoartelor de evaluare a conformității menționate la articolul 20 alineatul (1) și la articolul 21 alineatul (1);

(c) să informeze celelalte organisme de supraveghere și publicul cu privire la încălcarea securității sau la pierderea integrității, în conformitate cu articolul 19 alineatul (2);

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

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

(f) să coopereze cu autoritățile de protecție a datelor, în special prin informarea acestora, fără întârzieri nejustificate, cu privire la rezultatele auditurilor prestatorilor de servicii de încredere calificați, în cazul în care se presupune că normele de protecție a datelor cu caracter personal au fost încălcate;

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

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

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

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

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

▼B

(6) În fiecare an, până la 31 martie, fiecare organism de supraveghere înaintează Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior, însoțit de un rezumat al notificărilor încălcărilor primit de la prestatorii de servicii de încredere, în conformitate cu articolul 19 alineatul (2).

(7) Comisia pune la dispoziția statelor membre raportul anual menționat la alineatul (6).

(8) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile pentru raportul menționat la alineatul (6). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 18

Asistență reciprocă

(1) Organismele de supraveghere cooperează cu scopul de a face schimb de bune practici.

Pe baza unei solicitări justificate din partea unui alt organism de supraveghere, un organism de supraveghere acordă respectivului organism asistență astfel încât activitățile organismelor de supraveghere să poată fi desfășurate în mod coerent. Asistența reciprocă poate viza, în special, solicitările de informații și măsurile de supraveghere, cum ar fi solicitările de a desfășura inspecții legate de rapoartele de evaluare a conformității menționate la articolele 20 și 21.

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

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

(b) asistența solicitată nu este proporțională cu activitățile de supraveghere ale organismului de supraveghere desfășurate în conformitate cu articolul 17;

(c) acordarea asistenței solicitate ar contraveni prezentului regulament.

(3) După caz, statele membre pot autoriza organismele lor de supraveghere să efectueze anchete comune în care este implicat personalul din organismele de supraveghere ale celorlalte state membre. Mecanismele și procedurile pentru astfel de acțiuni în comun sunt convenite și stabilite de către statele membre în cauză, în conformitate cu dreptul lor intern.

Articolul 19

Cerințe de securitate aplicabile prestatorilor de servicii de încredere

(1) Prestatorii de servicii de încredere calificați și necalificați iau măsurile tehnice și organizaționale corespunzătoare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează. Ținând cont de cele mai recente evoluții tehnologice, aceste măsuri garantează că nivelul securității este proporțional cu gradul 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 de acest tip.

▼B

(2) Prestatorii de servicii de încredere calificați și necalificați notifică, fără întârzieri nejustificate, însă, în orice caz, în termen de 24 de ore după ce au aflat, organismului de supraveghere competent și, dacă este cazul, altor organisme relevante, cum sunt organismul național competent pentru securitatea informațiilor sau autoritatea pentru protecția datelor, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta.

Atunci când încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice încălcarea securității sau pierderea integrității fără întârzieri nejustificate.

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 notificat informează organismele de supraveghere vizate din alte state membre și ENISA.

Organismul de supraveghere notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării securității sau pierderea integrității servește interesului public.

(3) Organismul de supraveghere furnizează ENISA, o dată pe an, un rezumat al notificărilor privind încălcarea securității sau pierderea integrității primite de la prestatorii de servicii de încredere.

(4) Prin intermediul unor acte de punere în aplicare, Comisia poate:

(a) elabora specificații suplimentare referitoare la măsurile menționate la alineatul (1); și

(b) defini formatele și procedurile, inclusiv termenele, aplicabile în sensul alineatului (2).

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

SECȚIUNEA 3

Servicii de încredere calificate

Articolul 20

Supravegherea prestatorilor de servicii de încredere calificați

(1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin o dată la 24 de luni, de către un organism de evaluare a conformității. Scopul auditului este de a confirma că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament. Prestatorii de servicii de încredere calificați transmit raportul de evaluare a conformității care a rezultat organismului de supraveghere în termen de trei zile lucrătoare de la primirea lui.

▼B

(2) Fără a aduce atingere alineatului (1), organismul de supraveghere poate, în orice moment, să efectueze un audit sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității privind prestatorii de servicii de încredere calificați, pe cheltuiala prestatorilor de servcii de încredere respectivi, pentru a confirma că aceştia şi serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament. În cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, organismul de supraveghere informează autoritățile pentru protecția datelor cu privire la rezultatele auditurilor sale.

(3) În cazul în care organismul de supraveghere solicită prestatorului de servicii de încredere calificat să remedieze neîndeplinirea obligațiilor care îi revin în temeiul prezentului regulament, iar respectivul prestator nu acționează în consecință şi, după caz, într-un termen stabilit de organismul de supraveghere, organismul de supraveghere, ținând seama în special de amploarea, de durata şi de consecințele respectivei neîndepliniri, poate retrage statutul de calificat al respectivului prestator sau al serviciului prestat de acesta care este afectat şi informează organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1). Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire la retragerea statutului de calificat, al său sau al serviciului în cauză.

(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale următoarelor standarde:

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

(b) privind normele de audit în temeiul cărora organismele de evaluare a conformității își vor desfăşura evaluarea conformității prestatorilor de servicii de încredere calificați, astfel cum se menționează la alineatul (1).

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

Articolul 21

Inițierea unui serviciu de încredere calificat

(1) În cazul în care prestatorii de servicii de încredere care nu au statutul de calificat intenționează să înceapă să presteze servicii de încredere calificate, aceştia transmit organismului de supraveghere o notificare a intenției lor, împreună cu un raport de evaluare a conformității emis de un organism de evaluare a conformității.

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

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

▼B

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

(3) Prestatorii de servicii de încredere calificați pot începe furnizarea serviciului de încredere calificat după ce statutul de calificat a fost indicat în listele sigure menționate la articolul 22 alineatul (1).

(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile în sensul alineatelor (1) și (2). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 22

Listele sigure

(1) Fiecare stat membru instituie, menține și publică liste care includ informații referitoare la prestatorii de servicii de încredere calificați pentru care este responsabil, împreună cu informații referitoare la serviciile de încredere calificate prestate de aceștia.

(2) Statele membre instituie, mențin și publică, în mod securizat, listele sigure semnate sau sigilate electronic menționate 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, certificatele utilizate 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 adecvate pentru prelucrarea automată.

(5) Până la 18 septembrie 2015, Comisia specifică, prin intermediul unor acte de punere în aplicare, informațiile menționate la alineatul (1) și definește specificațiile tehnice și formatele pentru listele sigure aplicabile în sensul alineatelor (1)-(4). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 23

Marca de încredere a UE pentru serviciile de încredere calificate

(1) După indicarea statutului de calificat menționat la articolul 21 alineatul (2) al doilea paragraf pe lista sigură menționată la articolul 22 alineatul (1), prestatorii de servicii de încredere calificați pot utiliza o marcă de încredere a UE pentru a indica într-un mod simplu, ușor de recunoscut și clar serviciile de încredere calificate pe care le prestează.

▼B

(2) În cazul utilizării mărcii de încredere a UE pentru serviciile de încredere calificate menționate la alineatul (1), prestatorii de servicii de încredere calificați se asigură că pe site-ul lor internet este disponibil un link către lista sigură relevantă.

(3) Până la 1 iulie 2015, Comisia, prin intermediul unor acte de punere în aplicare, stabilește specificațiile referitoare la forma și, în special, prezentarea, componența, mărimea și designul mărcii de încredere a UE pentru serviciile de încredere calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 24

Cerințe pentru prestatorii de servicii de încredere calificați

(1) Atunci când emite un certificat calificat pentru un serviciu de încredere, un prestator de servicii de încredere calificat verifică, prin mijloace corespunzătoare și în conformitate cu legislația națională, identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat.

Informațiile menționate la primul paragraf sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe, în conformitate cu dreptul intern:

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

(b) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului calificat, a fost asigurată prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice și care îndeplinesc cerințele stabilite la articolul 8 în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”; sau

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

(d) prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică. Nivelul de asigurare echivalent este confirmat de un organism de evaluare a conformității.

(2) Un prestator de servicii de încredere calificat care prestează servicii de încredere calificate:

(a) informează organismul de supraveghere cu privire la orice schimbare survenită în prestarea sa de servicii de încredere calificate și cu privire la vreo intenție de a își înceta activitatea respectivă;

(b) angajează personal și, după caz, subcontractanți care dețin cunoștințele, credibilitatea, experiența și calificările necesare și care au beneficiat de formare adecvată în ceea ce privește normele de siguranță și protecție a datelor cu caracter personal și aplică proceduri administrative și de gestiune care corespund standardelor europene sau internaționale;

▼B

(c) în ceea ce privește riscul de răspundere pentru daune în conformitate cu articolul 13, menține suficiente resurse financiare și/sau obține o asigurare de răspundere adecvată, în conformitate cu dreptul intern;

(d) înainte de stabilirea unei relații contractuale, informează, în mod clar și cuprinzător, orice persoană care dorește să utilizeze un serviciu de încredere calificat de clauzele și condițiile exacte privind utilizarea acelui serviciu, inclusiv orice restricție privind utilizarea acestuia;

(e) utilizează sisteme și produse demne de încredere care sunt protejate împotriva modificărilor și asigură siguranța tehnică și fiabilitatea proceselor susținute de acestea;

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

(i) acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obținut consimțământul persoanei la care se referă datele;

(ii) numai persoanele autorizate să poată introduce și modifica datele stocate;

(iii) autenticitatea datelor să poată fi controlată;

(g) ia măsuri adecvate împotriva falsificării și furtului de date;

(h) înregistrează și menține accesibile pentru o perioadă de timp corespunzătoare, inclusiv ulterior încetării activității prestatorului de servicii de încredere calificat, toate informațiile relevante referitoare la datele emise și primite de către prestatorul de servicii de încredere calificat, în special în scopul de a furniza dovezi în procedurile judiciare și în scopul asigurării continuității serviciului. Aceste înregistrări pot fi efectuate în mod electronic;

(i) are un plan actualizat, în cazul încetării serviciului, pentru a asigura continuitatea serviciului conform dispozițiilor verificate de către organismul de supraveghere, în conformitate cu articolul 17 alineatul (4) litera (i);

(j) asigură prelucrarea legală a datelor cu caracter personal în conformitate cu Directiva 95/46/CE;

(k) în cazul prestatorilor de servicii de încredere calificați care eliberează certificate calificate, instituie și actualizează permanent o bază de date a certificatelor.

(3) Dacă un prestator de servicii de încredere calificat care eliberează certificate calificate decide să revoce un certificat, acesta înregistrează respectiva revocare în baza sa de date privind certificatele și publică statutul de revocat al certificatului în timp util și în orice caz în termen de 24 de ore de la primirea cererii. Revocarea intră în vigoare imediat după publicare.

▼B

(4) Cu privire la alineatul (3), prestatorii de servicii de încredere 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 cel puțin pentru fiecare certificat în parte, în orice moment și după expirarea perioadei de valabilitate a certificatului, în mod automat, fiabil, gratuit și eficient.

(5) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numerele de referință ale standardelor pentru sisteme și produse demne de încredere, care respectă cerințele prevăzute la alineatul (2) literele (e) și (f) de la prezentul articol. În cazul în care sistemele și produsele demne de încredere respectă standardele respective, se presupune că acestea respectă cerințele prevăzute la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

SECȚIUNEA 4

Semnătura electronică

Articolul 25

Efectele juridice ale semnăturilor electronice

(1) Unei semnături electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este în format electronic sau că nu îndeplinește cerințele pentru semnăturile electronice calificate.

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

(3) O semnătură electronică calificată bazată pe un certificat calificat eliberat de un stat membru este recunoscută drept semnătură electronică calificată în toate celelalte state membre.

Articolul 26

Cerințe pentru semnături electronice avansate

O semnătura electronică avansată 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, cu un nivel ridicat de încredere, exclusiv sub controlul său; și

(d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.

Articolul 27

Semnăturile electronice în cadrul serviciilor publice

(1) În cazul în care un stat membru solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat

▼B

membru recunoaşte semnăturile electronice avansate, semnăturile electronice avansate bazate pe un certificat calificat pentru semnături electronice şi semnăturile electronice calificate care întrebuinţează cel puţin formatele sau metodele definite în actele de punere în aplicare menţionate la alineatul (5).

(2) În cazul în care un stat membru solicită o semnătură electronică avansată bazată pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaşte semnăturile electronice avansate bazate pe un certificat calificat şi semnăturile electronice calificate care întrebuinţează cel puţin formatele sau metodele definite în actele de punere în aplicare menţionate la alineatul (5).

(3) Statele membre nu solicită o semnătură electronică la un nivel de securitate mai ridicat decât cel al semnăturii electronice calificate pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public.

(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referinţă ale standardelor pentru semnături electronice avansate. În cazul în care o semnătură electronică avansată îndeplineşte respectivele standarde, se presupune că aceasta respectă cerinţele referitoare la semnăturile electronice avansate menţionate în prezentul articol alineatele (1) şi (2) şi la articolul 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).

(5) Până la 18 septembrie 2015 şi ţinând cont de practicile, standardele şi actele juridice ale Uniunii existente, Comisia defineşte, prin intermediul unor acte de punere în aplicare, formate de referinţă ale semnăturilor electronice avansate sau metode de referinţă, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).

Articolul 28

Certificate calificate pentru semnăturile electronice

(1) Certificatele calificate pentru semnăturile electronice îndeplinesc cerinţele prevăzute în anexa I.

(2) Certificatele calificate pentru semnăturile electronice nu fac obiectul niciunei cerinţe obligatorii în plus faţă de cerinţele prevăzute în anexa I.

(3) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea şi recunoaşterea semnăturilor electronice calificate.

(4) În cazul în care un certificat calificat pentru semnăturile electronice a fost revocat după activarea iniţială, acesta îşi pierde valabilitatea din momentul în care a fost revocat şi nu se revine în niciun caz la statutul său anterior.

(5) Sub rezerva următoarelor condiţii, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a unui certificat calificat pentru semnătura electronică:

▼B

(a) în cazul în care un certificat calificat pentru semnătura electronică a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare;

(b) perioada de suspendare este clar indicată în baza de date privind certificatele și statutul de suspendat este vizibil, pe perioada suspendării, din serviciul care oferă informații privind statutul certificatului.

(6) Comisia poate, prin intermediul unor acte 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 acesta respectă cerințele prevăzute în anexa I. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 29

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 unor acte 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 acesta respectă cerințele prevăzute în anexa II. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 30

Certificarea dispozitivelor de creare a semnăturilor electronice calificate

(1) Conformitatea dispozitivelor de creare a semnăturii electronice calificate cu cerințele prevăzute în anexa II este certificată de organisme publice sau private adecvate desemnate de statele membre.

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

(3) Certificarea menționată la alineatul (1) se bazează pe unul dintre următoarele elemente:

(a) un proces de evaluare de securitate efectuat în conformitate cu unul dintre standardele pentru evaluarea securității produselor din domeniul tehnologiei informației incluse în lista instituită în conformitate cu al doilea paragraf; sau

(b) un alt proces decât procesul prevăzut la litera (a), cu condiția ca acest proces să utilizeze niveluri de securitate comparabile și ca organismul public sau privat menționat la alineatul (1) să notifice Comisiei respectivul proces. Procesul respectiv poate fi utilizat numai în absența standardelor menționate la litera (a) sau dacă un proces de evaluare de securitate menționat la litera (a) este în curs de desfășurare.

▼B

Comisia stabilește, prin intermediul unor acte de punere în aplicare, lista standardelor pentru evaluarea de securitate a produselor din domeniul tehnologiei informației menționate la litera (a). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(4) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47 privind stabilirea de criterii specifice care urmează să fie îndeplinite de către organismele desemnate menționate la alineatul (1) de la prezentul articol.

Articolul 31

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

(1) Statele membre notifică Comisiei, fără întârzieri nejustificate și în termen de maximum o lună de la încheierea certificării, informații cu privire la dispozitivele de creare a semnăturilor electronice calificate care au fost certificate de către organismele menționate la articolul 30 alineatul (1). De asemenea, statele membre notifică Comisiei, fără întârziere și în termen de maximum o lună de la anularea certificării, informații cu privire la dispozitivele de creare a semnăturii electronice care nu mai sunt 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 unor acte de punere în aplicare, să definească formatele și procedurile aplicabile în sensul alineatului (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 32

Cerințe pentru validarea semnăturilor electronice calificate

(1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții:

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

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

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

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

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

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

▼B

(g) integritatea datelor semnate nu a fost compromisă;

(h) cerințele prevăzute la articolul 26 au fost îndeplinite la momentul semnării.

(2) Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice aspect relevant pentru securitate.

(3) Comisia poate, prin intermediul unor acte 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 aceasta respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 33

▼C1

Serviciul calificat de validare a semnăturilor electronice calificate

(1) Un serviciu calificat de validare a semnăturilor electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care:

▼B

(a) realizează validarea în conformitate cu articolul 32 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 unor acte de punere în aplicare, să stabilească numere de referință pentru standardele referitoare la serviciul de validare calificat menționat la alineatul (1). În cazul în care serviciul de validare a semnăturilor electronice calificate îndeplinește standardele respective, se prezumă că acesta respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 34

Serviciul calificat de păstrare a semnăturilor electronice calificate

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

▼B

(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru serviciul calificat de păstrare a semnăturilor electronice calificate. În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele respective, se presupune că acestea respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

SECȚIUNEA 5

Sigiliile electronice

Articolul 35

Efectele juridice ale sigiliilor electronice

(1) Unui sigiliu electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca probă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru sigiliile electronice calificate.

(2) Un sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă sigiliul electronic calificat.

(3) Un sigiliu electronic calificat bazat pe un certificat calificat eliberat de un stat membru este recunoscut drept sigiliu electronic calificat în toate celelalte state membre.

Articolul 36

Cerințele pentru sigiliile electronice avansate

Un sigiliu electronic avansat îndeplinește următoarele cerințele:

(a) face trimitere exclusiv la creatorul sigiliului;

(b) permite identificarea creatorului sigiliului;

(c) este creat cu ajutorul datelor 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; și

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

Articolul 37

Sigiliile electronice în cadrul serviciilor publice

(1) În cazul în care un stat membru solicită un sigiliu electronic avansat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate, sigiliile electronice avansate bazate pe un certificat calificat pentru sigilii electronice și sigiliile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

▼B

(2) În cazul în care un stat membru solicită un sigiliu electronic bazat pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate bazate pe un certificat calificat și sigiliile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).

(3) Statele membre nu solicită un sigiliu electronic la un nivel de securitate mai ridicat decât cel al sigiliului electronic calificat pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public.

(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru sigilii electronice avansate. În cazul în care un sigiliu electronic avansat îndeplinește standardele respective, se presupune că acesta respectă cerințele referitoare la sigiliile electronice avansate menționate la alineatele (1) și (2) de la prezentul articol și la articolul 36. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

(5) Până la 18 septembrie 2015 și ținând cont de practicile, standardele și actele juridice ale Uniunii existente, Comisia definește, prin intermediul unor acte de punere în aplicare, formate de referință ale sigiliilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 38

Certificate calificate pentru sigiliul electronic

(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) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea sigiliilor electronice calificate.

(4) În cazul în care un certificat calificat pentru un sigiliu electronic a fost revocat după activarea inițială, acesta își pierde valabilitatea din momentul în care a fost revocat și nu se revine în niciun caz la statutul său anterior.

(5) Sub rezerva următoarelor condiții, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a certificatelor calificate pentru sigiliile electronice:

(a) în cazul în care un certificat calificat pentru sigilii electronice a fost suspendat temporar, respectivul certificat își pierde valabilitatea pe parcursul perioadei de suspendare;

▼B

(b) perioada de suspendare este clar indicată în baza de date privind certificatele și statutul de suspendat este vizibil, pe perioada suspendării, din serviciul care oferă informații privind statutul certificatului.

(6) Comisia poate, prin intermediul unor acte 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 acesta respectă cerințele prevăzute în anexa III. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

Articolul 39

Dispozitive de creare a sigiliilor electronice calificate

(1) Articolul 29 se aplică *mutatis mutandis* cerințelor pentru dispozitivele de creare a sigiliilor electronice calificate.

(2) Articolul 30 se aplică *mutatis mutandis* certificării dispozitivelor de creare a sigiliilor electronice calificate.

(3) Articolul 31 se aplică *mutatis mutandis* publicării unei liste a dispozitivelor de creare a sigiliilor electronice certificate și calificate.

Articolul 40

Validarea și păstrarea sigiliilor electronice calificate

Articolele 32, 33 și 34 se aplică *mutatis mutandis* validării și păstrării sigiliilor electronice calificate.

SECȚIUNEA 6

Mărcile temporale electronice

Articolul 41

Efectul juridic al mărcilor temporale electronice

(1) Unei mărci temporale electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru marca temporală electronică calificată.

(2) O marcă temporală electronică calificată beneficiază de prezumția corectitudinii datei și orei pe care le indică și a integrității datelor la care se raportează data și ora indicate.

(3) O marcă temporală electronică calificată emisă într-un stat membru este recunoscută drept marcă temporală electronică calificată în toate statele membre.

Articolul 42

Cerințe pentru mărcile temporale electronice calificate

(1) O marcă temporală electronică calificată îndeplinește următoarele cerințe:

(a) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat;

▼B

(b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată; și

(c) este semnată utilizând o semnătură electronică avansată sau sigilată cu un sigiliu electronic avansat al prestatorului de servicii de încredere calificat sau printr-o metodă echivalentă.

(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru legătura între dată și oră și date și pentru exactitatea surselor orei indicate. În cazul în care legătura între dată și oră și date și exactitatea surselor orei indicate îndeplinesc standardele respective, se presupune că se respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

SECȚIUNEA 7

Serviciul de distribuție electronică înregistrată

Articolul 43

Efectul juridic al unui serviciu de distribuție electronică înregistrată

(1) Datelor trimise și primite prin utilizarea unui serviciu de distribuție electronică înregistrată nu li se refuză efectul juridic și posibilitatea de a fi acceptate ca dovadă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru serviciul de distribuție electronică înregistrată.

(2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată beneficiază de prezumția integrității datelor, a trimiterii datelor respective de către expeditorul identificat și a primirii acestora de către destinatarul identificat și a preciziei datei și orei trimiterii și primirii datelor indicate de serviciul de distribuție electronică înregistrată.

Articolul 44

Cerințe pentru serviciile de distribuție electronică înregistrată calificate

(1) Serviciile de distribuție electronică înregistrată calificate îndeplinesc următoarele cerințe:

(a) sunt prestate de către unul sau mai mulți prestatori de servicii de încredere calificați;

(b) asigură identificarea expeditorului cu un nivel de încredere ridicat;

(c) asigură identificarea destinatarului înainte de furnizarea datelor;

(d) trimiterea și primirea datelor este securizată printr-o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de încredere calificat astfel încât să se excludă posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat;

(e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului și destinatarului datelor;

(f) data și ora trimiterii, primirii și ale oricărei modificări a datelor este indicată printr-o marcă temporală electronică calificată.

▼B

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

(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru procesele de trimitere și primire de date. În cazul în care procesul de trimitere și primire de date îndeplinește standardele respective, se presupune că se respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

SECȚIUNEA 8

Autentificarea unui site internet

Articolul 45

Cerințe pentru certificatele calificate pentru autentificarea unui site internet

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

(2) Comisia poate, prin intermediul unor acte 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. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).

CAPITOLUL IV

DOCUMENTE ELECTRONICE

Articolul 46

Efectele juridice ale documentelor electronice

Unui document electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca dovadă în procedurile judiciare doar din motiv că este sub formă electronică.

CAPITOLUL V

DELEGAREA DE COMPETENȚE ȘI MĂSURI DE PUNERE ÎN APLICARE

Articolul 47

Exercitarea delegării

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

(2) Se conferă Comisiei, pentru o perioadă de timp nedeterminată de la 17 septembrie 2014, competența de a adopta actele delegate menționate la articolul 30 alineatul (4).

▼B

(3) Delegarea competențelor menționată la articolul 30 alineatul (4) 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 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 conformitate cu articolul 30 alineatul (4) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea actului respectiv Parlamentului European și Consiliului sau în cazul în care, înainte de expirarea termenului respectiv, Parlamentul European și Consiliul au informat Comisia cu privire la faptul că nu vor formula obiecții. La inițiativa Parlamentului European sau a Consiliului, termenul respectiv se prelungește cu două luni.

Articolul 48

Procedura comitetului

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

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

CAPITOLUL VI

DISPOZIȚII FINALE

Articolul 49

Revizuire

Comisia evaluează modul de aplicare a prezentului regulament și prezintă un raport în acest sens Parlamentului European și Consiliului cel mai târziu la 1 iulie 2020. Comisia evaluează, în special, dacă este oportun să se modifice domeniul de aplicare al prezentului regulament sau dispozițiile sale specifice, inclusiv articolul 6, articolul 7 litera (f), articolele 34, 43, 44 și 45, ținând seama de experiența dobândită în aplicarea prezentului regulament, precum și de evoluțiile tehnologice, ale pieței și juridice.

Raportul menționat la primul paragraf este însoțit, după caz, de propuneri legislative.

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

Articolul 50

Abrogare

(1) Directiva 1999/93/CE se abrogă cu efect de la 1 iulie 2016.

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

▼B

Articolul 51

Măsuri tranzitorii

(1) 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 electronice calificate în temeiul prezentului regulament.

(2) Certificatele calificate emise pentru persoane fizice în conformitate cu Directiva 1999/93/CE sunt considerate drept certificate calificate pentru semnături electronice în temeiul prezentului regulament, până la expirarea lor.

(3) Un prestator de servicii de certificare care eliberează certificate calificate în temeiul Directivei 1999/93/CE prezintă un raport de evaluare a conformității către organismul de supraveghere cât mai curând posibil, dar nu mai târziu de 1 iulie 2017. Până la prezentarea unui astfel de raport de evaluare a conformității și până la finalizarea de către organismul de supraveghere a evaluării sale, prestatorul de servicii de certificare respectiv este considerat ca fiind prestator de servicii de încredere calificat în temeiul prezentului regulament.

(4) În cazul în care un prestator de servicii de certificare care eliberează certificate calificate în temeiul Directivei 1999/93/CE nu prezintă un raport de evaluare a conformității către organismul de supraveghere în termenul prevăzut la alineatul (3), respectivul prestator de servicii de certificare nu este considerat ca fiind prestator de servicii de încredere calificat în temeiul prezentului regulament începând cu data de 2 iulie 2017.

Articolul 52

Intrarea în vigoare

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

(2) Prezentul regulament se aplică de la 1 iulie 2016, cu excepția următoarelor dispoziții:

(a) articolul 8 alineatul (3), articolul 9 alineatul (5), articolul 12 alineatele (2)-(9), articolul 17 alineatul (8), articolul 19 alineatul (4), articolul 20 alineatul (4), articolul 21 alineatul (4), articolul 22 alineatul (5), articolul 23 alineatul (3), articolul 24 alineatul (5), articolul 27 alineatele (4) și (5), articolul 28 alineatul (6), articolul 29 alineatul (2), articolul 30 alineatele (3) și (4), articolul 31 alineatul (3), articolul 32 alineatul (3), articolul 33 alineatul (2), articolul 34 alineatul (2), articolul 37 alineatele (4) și (5), articolul 38 alineatul (6), articolul 42 alineatul (2), articolul 44 alineatul (2), articolul 45 alineatul (2) și articolele 47 și 48 se aplică de la 17 septembrie 2014;

(b) articolul 7, articolul 8 alineatele (1) și (2), articolele 9, 10, 11 și articolul 12 alineatul (1) se aplică de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8);

(c) articolul 6 se aplică după trei ani de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8).

(3) În cazul în care sistemul de identificare electronică notificat este inclus în lista publicată de Comisie în conformitate cu articolul 9 înainte de data menționată la alineatul (2) litera (c) de la prezentul articol, recunoașterea mijloacelor de identificare electronică din cadrul sistemului respectiv în temeiul articolului 6 are loc cel târziu în termen de 12 luni de la publicarea respectivului sistem, dar nu înainte de data menționată la alineatul (2) litera (c) de la prezentul articol.

▼B

(4) Fără a aduce atingere alineatului (2) litera (c) de la prezentul articol, un stat membru poate decide ca mijloacele de identificare electronică din cadrul unui sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) de către un alt stat membru să fie recunoscute de primul stat membru de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8). Statele membre vizate informează Comisia. Comisia publică aceste informații.

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

▼B

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 care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care includ cel puțin statul membru în care este stabilit prestatorul respectiv; și

— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;

— în cazul unei persoane fizice: numele persoanei;

(c) cel puțin numele semnatarului sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;

(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 încredere calificat;

(g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere 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 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.

▼B

ANEXA II

CERINȚE PENTRU DISPOZITIVELE DE CREARE A SEMNĂTURILOR ELECTRONICE CALIFICATE

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

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

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

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

   (d) datele de creare a semnăturilor electronice utilizate pentru crearea 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 pot realiza numai de către un prestator de servicii de încredere calificat.

4. Fără a aduce atingere punctului 1 litera (d), prestatorii de servicii de încredere calificați care gestionează datele de creare a semnăturilor electronice în numele semnatarului pot duplica datele de creare a semnăturilor electronice numai 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.

▼B

ANEXA III

CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU SIGILIILE ELECTRONICE

Certificatele calificate pentru sigiliile 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 încredere calificat care emite certificatele calificate, care include cel puțin statul membru în care este stabilit prestatorul respectiv; și

— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;

— în cazul unei persoane fizice: numele persoanei;

(c) cel puțin numele creatorului sigiliului și, după caz, 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 încredere calificat;

(g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere 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 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.

▼B

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 încredere calificat care emite certificatele calificate, care include cel puțin statul membru în care este stabilit prestatorul respectiv; și

— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale,

— în cazul unei persoane fizice: numele persoanei;

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

în cazul persoanelor juridice: cel puțin denumirea persoanei juridice căreia i se eliberează certificatul și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;

(d) elemente ale adresei persoanei fizice sau juridice căreia i s-a eliberat certificatul, incluzând cel puțin orașul și statul, și, dacă este cazul, în forma în care sunt înscrise în registrele oficiale;

(e) numele domeniului (domeniilor) gestionat(e) de persoana fizică sau 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 încredere calificat;

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

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

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