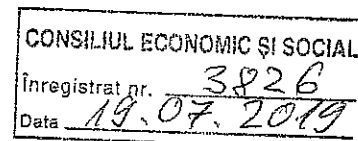


PARLAMENTUL ROMÂNIEI



Către,

BIROUL PERMANENT AL SENATULUI

În conformitate cu prevederile art. 74 alin. (1) și ale art. 75 din Constituția României, republicată și cu prevederile art. 92 și urm. din Regulamentul Senatului, vă înaintez propunerea legislativă **Legea privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice**, spre dezbateră și adoptare.

În baza dispozițiilor art. 111 și urm. din Regulamentul Senatului, solicit aplicarea procedurii de urgență.

Inițiator:

senator PSD
Șerban NICOLAE



PARLAMENTUL ROMÂNIEI

EXPUNERE DE MOTIVE

Intrarea în vigoare a *Regulamentului (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 („Regulamentul eIDAS”)*, denumit în continuare Regulamentul, a adus importante modificări pentru legea semnăturii electronice, Legea nr. 445/2001, în special în ceea ce privește efectele juridice ale înscrisurilor care au anexată sau atașată logic o semnătură electronică.

Printre modificările importante aduse de Regulament se numără: introducerea sigiliului electronic pentru identificarea persoanei juridice, acordarea de efecte juridice tuturor tipurilor de semnături electronice, acordarea efectelor semnăturii olografe cel puțin pentru semnătura calificată, diversificarea mijloacelor de identificare a persoanei, definirea nivelurilor de autentificare în accesarea serviciilor online furnizate de autorități publice.

Prezenta propunere legislativă abrogă Legea nr. 445/2001 în vederea punerii în aplicare a Regulamentului nr. 910/2014, având în vedere că emiterea Ordinului nr. 449/2017 privind procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat în conformitate cu Regulamentul (UE) nr. 910/2014 nu a fost suficientă pentru a asigura implementarea corectă a Regulamentului în România.

Regulamentul lasă la latitudinea statelor membre următoarele aspecte, care au rămas neacoperite de legislația românească: stabilirea sancțiunilor pentru nerespectarea Regulamentului, stabilirea efectelor juridice ale serviciilor de încredere, definirea altor servicii de încredere, desemnarea unui Organism de supraveghere, stabilirea condițiilor în care este suspendat un certificat calificat pentru semnătura electronică, resursele financiare aferente răspunderii pentru daunele care ar putea rezulta, mijloacele de identificare a persoanei potrivit dreptului intern.

Propunerea de lege a pornit de la aceste lacune și de la nevoile reale identificate pe piața privată dar și în funcționarea administrației publice. Aceste nevoi au fost identificate în cadrul lucrărilor grupului de lucru constituit sub egida Comisiei pentru Tehnologia Informației și Comunicațiilor pe data de 3 iulie 2017. La lucrările grupului de lucru au participat reprezentanți ai instituțiilor publice relevante pentru domeniu (Ministerul Finanțelor Publice, Secretariatul General al Guvernului, Agenția Agenda Digitală pentru România, Ministerul Afacerilor Interne, Serviciul de Telecomunicații Speciale, Ministerul Comunicațiilor și Societății Informaționale), precum și din furnizorii de semnături electronice de pe piața românească și Asociația Română a Băncilor. Proiectul a fost trimis spre consultare și Camerei Americane de Comerț.



PARLAMENTUL ROMÂNIEI

Principiile noii reglementări

1. Libertatea contractuală – În spiritul libertății contractuale părțile sunt libere să aleagă tipul de semnătură pe care îl utilizează în cadrul contractelor consensuale, promovând astfel utilizarea semnăturii electronice.
2. Concurență liberă și loială – Reglementarea să fie minimală și puțin birocratică astfel încât să nu fie defavorizați prestatorii de servicii de încredere de pe piața românească față de cei de pe piața altor state membre.
3. Reglementare sustenabilă, pentru viitor – Prevederile legale trebuie să permită evoluțiile tehnologice în domeniu.
4. Interesul public și reducerea birocrăției – Reglementarea trebuie să faciliteze utilizarea semnăturii electronice în rândul populației, mai ales în ceea ce privește interacțiunea cu administrația publică și în accesarea serviciilor publice.

Prin urmare, prezenta propunere legislativă conferă și actelor juridice semnate între părți, electronic, cu o semnătură avansată, necalificată, efectele juridice ale semnăturii olografe, dacă forma scrisă a actului este solicitată doar pentru probarea lui. Opțiunea este lăsată la latitudinea părților pentru a se facilita tranzacționarea online și pentru a fi în acord cu principiul consensualismului și a libertății formei contractuale prevăzută la art. 1178 în Noul Cod Civil. Această abordare este în concordanță cu proiectul de lege privind implementarea cărții electronice de identitate care prevede furnizarea certificatelor necalificate cetățenilor în scopul semnării electronice (Plx nr. 575/2017).

De asemenea, propunerea legislativă introduce posibilitatea identificării persoanei la distanță, astfel încât să nu se creeze dezavantaje concurențiale pentru prestatorii de servicii de încredere înregistrați în România și pentru a fi, totodată, în ton cu evoluția tehnologică. În ceea ce privește contractarea terților de verificare a identității de către prestatorii de servicii de încredere calificați, pentru a nu discrimina prestatorii români raportat la cei străini, au fost stabilite doar clauze contractuale care trebuie incluse și răspunderea, fără a impune obligații de notificare.

Mai mult, propunerea clarifică statutul actelor juridice semnate electronic de funcționari publici, astfel încât să se faciliteze debirocratizarea și comunicarea electronică între instituțiile publice, precum și între acestea și cetățeni. În prezent, doar undeva la 10% dintre români interacționează online cu administrația publică sau trimit formulare online, în timp ce media europeană este de peste 35%. În consecință, digitalizarea administrației publice este un proces esențial pentru facilitarea serviciilor de e-guvernare dar și a tranzacțiilor electronice în general.

Prin propunerea legislativă se stabilesc și o serie de măsuri de securitate care trebuie implementate pentru a asigura condiții minime și uniforme de siguranță în păstrarea documentelor electronice, potrivit Regulamentului. În plus, se instituie principiul proporționalității în stabilirea nivelurilor de autentificare și identificare necesare pentru utilizarea serviciilor de e-guvernare, acestea fiind chestiuni abordate în prezent diferit și aleator de către instituțiile și autoritățile publice. Spre exemplu, solicitarea unei informații de interes public nu necesită stabilirea aceluiași nivel de încredere și identificare precum acordarea indemnizației pentru creșterea copilului.



PARLAMENTUL ROMÂNIEI

Articolul 1245 din Noul Cod Civil lasă la nivelul legii speciale reglementarea condițiilor de formă ale contractelor încheiate prin mijloace electronice, astfel încât adoptarea unei legi este urgentă pentru securitatea circuitului civil, în ceea ce privește contractele semnate electronic. Prezenta propunere legislativă nu implică costuri sau modificări instituționale în vederea implementării. Aceasta vine în sprijinul mediului de afaceri, oferind predictibilitate și coerență legislativă pentru piața furnizorilor de servicii de încredere. De asemenea, propunerea ajută la implementarea fluxurilor electronice în instituțiile publice în furnizarea serviciilor către cetățeni și în desfășurarea obiectului de activitate.

Potrivit regulamentului, statele membre au deplina libertate de a stabili efectele juridice ale celorlalte tipuri de semnături electronice (simplă sau avansată), respectiv de a acorda oricărui tip de semnătură electronică efectul juridic al semnăturii olografe, inclusiv celor utilizate în sisteme închise decurgând din dreptul intern.

De asemenea, se lasă la aprecierea statelor membre stabilirea condițiilor pe care trebuie să le îndeplinească semnăturile electronice (de securitate, verificare a identității, eventuale certificări ale organelor abilitate etc.), acestea având datoria de a elabora reglementări prin care să poată conferi efecte juridice și semnăturilor electronice cu un nivel mai scăzut de securitate decât semnătura calificată. Altfel spus, statul membru nu se poate prevala de nivelul de securitate diferit al semnăturilor simplă și avansată, pentru a nu le conferi nici un fel de efecte juridice, fiind obligat să găsească o cale astfel încât să poată asigura folosirea acestor tipuri de semnături în siguranță. Bineînțeles, în acest proces de elaborare a normelor juridice, statul membru are datoria de a avea în vedere pe de-o parte, crearea unei piețe unice digitale și un cadru de reglementare cât mai accesibil, care să favorizeze creșterea nivelului de digitalizare, iar pe de altă parte, principiul proporționalității la stabilirea nivelului de autentificare.

În paragraful 48 din preambulul Regulamentului se menționează că, deși un nivel ridicat de securitate este necesar pentru a asigura recunoașterea reciprocă a semnăturilor electronice, în cazuri speciale, cum ar fi în contextul Deciziei 2009/767/CE a Comisiei, semnăturile electronice cu un nivel mai scăzut de asigurare a securității ar trebui să fie, de asemenea, acceptate. În art. 25 alin. (1) din Regulament se stabilește în mod clar că *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.*

Necesitatea reglementării efectelor juridice ale semnăturilor electronice simplă și avansată

Lipsa unui act normativ cu puterea juridică a legii, care să consacre efectele juridice și forța probantă a diferitelor tipuri de semnătură electronică întârzie adoptarea programelor de digitizare și aduce prejudicii majore consumatorilor și pieței de profil din România. Nu trebuie uitat faptul că, așa cum reiese din Raportul DESI, România ocupă ultimul loc din punctul de vedere al digitalizării. Legiuitorul român trebuie să țină cont de realitățile din piață și să acționeze într-o manieră armonizată, în raport cu standardele și bunele practici în domeniu, pentru a permite pieței de profil să se dezvolte în mod natural, cu beneficii evidente pentru consumatorul final, cât și în ceea ce privește exportul de servicii și soluții românești la nivel european.



PARLAMENTUL ROMÂNIEI

Deși potrivit art. 256 C. proc. civ.: „*Convențiile asupra admisibilității, obiectului sau sarcinii probelor sunt valabile, cu excepția celor care privesc drepturi de care părțile nu pot dispune, a celor care fac imposibilă ori dificilă dovada actelor sau faptelor juridice ori, după caz, contravin ordinii publice sau bunelor moravuri*”, apreciem că este necesară reluarea principiului și în cuprinsul actului normativ ce va reglementa regimul juridic al semnăturii electronice, pentru a asigura destinatarilor asupra posibilității de a încheia convenții cu privire la admisibilitatea probatorie a înscrisurilor în formă electronică. Cu alte cuvinte, se admite valabilitatea unor astfel de convenții, în măsura în care ele largesc posibilitățile de probă, ușurează sarcina judecătorului de a descoperi adevărul și nu încalcă normele imperative ale legii. Din interpretarea textului legal, rezultă foarte clar că nu sunt valabile convențiile asupra admisibilității, sarcinii și obiectului probei care privesc drepturi de care părțile nu pot dispune, precum cele referitoare la raporturile juridice de muncă, la starea persoanelor etc.

În acest fel, părțile vor fi stimulate în a explora modalități prin care să faciliteze încheierea de acte juridice care să poată fi dovedite prin semnături electronice concepute prin acordul părților.

Totodată, în paragraful 49 din preambulul Regulamentului eIDAS se menționează, în mod expres, că „*Prezentul regulament ar trebui să stabilească principiul conform căruia unei semnături electronice nu ar trebui să i se refuze efectul juridic din motiv că aceasta este în format electronic sau că nu îndeplinește cerințele pentru semnătura electronică calificată. Cu toate acestea, efectul juridic al semnăturilor electronice se definește în dreptul intern, cu excepția cerinței prevăzute în prezentul regulament, conform căreia o semnătură electronică calificată ar trebui să aibă efecte juridice echivalente cu cele ale semnăturii olografe.*”

În acest sens apare ca necesară reglementarea posibilității dovedirii unui act juridic prin înscrisuri în formă electronică ce poartă și un alt tip de semnătură electronică decât cea calificată. Or, în aceste condiții, în vederea asigurării unui grad ridicat de protecție, în special a categoriei consumatorilor, apreciem că este necesară indicarea limitativă a actelor juridice care pot fi dovedite prin înscrisuri în formă electronică ce poartă semnături electronice simple

Bineînțeles că nu se poate discuta despre încheierea unor astfel de convenții decât cu privire la înscrisurile a căror formă scrisă este necesară *ad probationem*, astfel încât lipsa ori neregularitatea ei să nu afecteze existența operațiunii juridice, iar nu *ad validitatem*, deoarece, în această ipoteză, actul juridic, în sens de *negotium*, este lovit de nulitate.

Raportat la contextul efectelor juridice ale semnăturii electronice, apreciem că, în cazul înscrisurilor pentru care forma scrisă este cerută *ad probationem*, legiuitorul ar trebui să confere valoarea unei semnături olografe (bucurându-se de o prezumție de validitate) și semnăturii electronice simple, în situația în care:

- există o convenție referitoare la puterea doveditoare a înscrisului;
- înscrisul se referă la încheiere unor acte juridice de dispoziție de valoare redusă, de conservare sau de administrare.



PARLAMENTUL ROMÂNIEI

Semnătura electronică avansată prezintă suficiente garanții pentru a avea efectul juridic al semnăturii olografe

Analizând comparativ definițiile celor două noțiuni - semnătură electronică avansată și semnătura electronică calificată (prevăzute la art. 3 punctele 11 și 12 din Regulamentul eIDAS), se observă că elementele de diferență sunt, în ceea ce privește semnătura calificată:

- a) crearea acesteia printr-un dispozitiv de creare a semnăturilor electronice calificat și
- b) existența certificatului calificat.

Însă, aceste elemente de diferență (absente la semnătura avansată) nu pot conduce la refuzarea efectului juridic al semnăturii avansate, fapt menționat expres în art. 25 din Regulament. Practic, semnătura calificată este, la origini, tot o semnătură avansată, care trebuie să îndeplinească aceleași cerințe cumulative de la art. 26 din Regulament, astfel cum rezultă chiar din definiția acesteia (art. 3 pct. 12 din Regulamentul eIDAS: *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;"). Faptul că, în esență, semnătura calificată are la bază semnătura avansată, este un indiciu cu privire la potențialul de securitate suficient de ridicat al semnăturii avansate, caz în care legiuitorul român ar putea cu ușurință să elaboreze norme, în dreptul intern, prin care să reglementeze emiterea acestui tip de semnătură în condiții de securitate optime.

În primul rând, condițiile pe care trebuie să le îndeplinească semnătura avansată (menționate în art. 26 din Regulamentul eIDAS), prezintă garanții suficiente în ceea ce privește identificarea în mod unic a semnatarului, controlul asupra datelor de creare a semnăturii (acestea fiind unice, confidentiale și protejate împotriva folosirii neautorizate), precum și integritatea datelor.

În al doilea rând, este important a se avea în vedere că semnăturile avansate sunt menționate expres în Regulamentul eIDAS în legătură cu serviciile publice (art. 27 din Regulament), fapt ce denotă, pe de-o parte, posibilitatea de a fi asimilată semnăturii olografe, iar pe de altă parte, încrederea în acest tip de semnătură și, totodată, aptitudinea sa de a conferi garanții de securitate suficiente. Referitor la utilizarea semnăturii avansate în sfera serviciilor publice, e de amintit faptul că, în art. 3 din Ordonanța de Urgență nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative, se prevede că *instituțiile publice și organele de specialitate ale administrației publice centrale sunt obligate să accepte documentele eliberate de către persoanele juridice de drept public sau de drept privat în format electronic, care au o semnătură electronică calificată sau avansată, definite potrivit prevederilor art. 3 pct. 11 și 12 din Regulamentul (UE) nr. 910/2014, în scopul furnizării serviciilor publice către beneficiar.*

Din aceste prevederi, rezultă cu evidență faptul că intenția legiuitorului român nu a fost aceea de a respinge *de plano* folosirea semnăturii avansate, ci dimpotrivă, a avut în vedere să-i confere același efect juridic pe care-l are și cea calificată, respectiv de semnătură olografă. Câtă vreme înscrisurile în formă electronică, ce poartă o semnătură avansată sunt considerate ca fiind înscrisuri sub semnătură privată în fața instituțiilor publice și organelor de specialitate, firesc ar fi ca această semnătură avansată să aibă același efect (de semnătură olografă) și în raporturile dintre particulari.



PARLAMENTUL ROMÂNIEI

În al treilea rând, prin Decizia de punere în aplicare (UE) 2015/1506 a Comisiei din 8 septembrie 2015, s-au stabilit specificațiile tehnice referitoare la formatele semnăturilor electronice avansate care trebuie recunoscute de către organismele din sectorul public, semnăturile care îndeplinesc aceste specificații bucurându-se de prezumția de conformitate cu Regulamentul eIDAS. Astfel, o semnătură avansată care corespunde acestui format, este menită să producă efecte juridice, fără a exista vreun impediment în a fi asimilată semnăturii olografe.

În al patrulea rând, Regulamentul eIDAS impune și prestatorilor de servicii de încredere necalificați obligații privind luarea măsurilor tehnice și organizaționale necesare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează (art. 19 din Regulament). De asemenea, și prestatorii necalificați răspund la fel ca prestatorii calificați pentru prejudiciile cauzate în mod intenționat sau din neglijență oricărei persoane fizice sau juridice, diferența fiind doar în materie probatorie (la prestatorul calificat operează o prezumție relativă de culpă, în timp ce la prestatorul necalificat, persoana care se consideră vătămată trebuie să facă dovada culpei profesionistului).

Având în vedere aceste argumente, nu se poate considera sub nicio formă că echivalarea semnăturii avansate cu semnătura olografă reprezintă o vulnerabilizare a serviciilor publice și sistemelor care utilizează documente electronice.

Înscrisul sub semnătură privată și începutul de dovadă scrisă. Corelare cu semnătura electronică simplă, respectiv avansată

Legiuitorul român a definit înscrisul sub semnătură privată ca fiind *cel care poartă semnătura părților*, indiferent de suportul său material, arătând că *nu este supus niciunei alte formalități, în afara excepțiilor prevăzute de lege* (art. 272 din Codul de procedură civilă). Altfel spus, norma generală de drept nu impune *de plano* nicio condiție suplimentară pentru ca înscrisul sub semnătură privată să producă efecte, indiferent de suportul material pe care se află. Potrivit art. 273 alin. (1) din Codul de procedură civilă, *înscrisul sub semnătură privată, recunoscut de cel căruia îi este opus sau, după caz, socotit de lege ca recunoscut, face dovada între părți până la proba contrară*. Așadar, fie că suntem în prezența unui înscris pe suport hârtie (semnat olograf), fie că suntem în prezența unui înscris în formă electronică (semnat cu o semnătură electronică), efectul său juridic este același: face dovada între părți dacă este recunoscut de partea căreia i se opune sau dacă este socotit de lege ca recunoscut.

În ceea ce privește începutul de dovadă scrisă, acesta a fost reglementat în art. 310 din Codul de procedură civilă, potrivit căruia:

(1) *Se socotește început de dovadă scrisă orice scriere, chiar nesemnată și nedată, care provine de la o persoană căreia acea scriere i se opune ori de la cel al cărui succesori în drepturi este acea persoană, dacă scrierea face credibil faptul pretins.*

(2) *Constituie început de dovadă scrisă și înscrisul, chiar nesemnat de persoana căreia acesta i se opune, dacă a fost întocmit în fața unui funcționar competent care atestă că declarațiile cuprinse în înscris sunt conforme celor făcute de acea persoană.*

(3) *Începutul de dovadă scrisă poate face dovada între părți numai dacă este completat prin alte mijloace de probă, inclusiv prin proba cu martori ori prin prezumții.*



PARLAMENTUL ROMÂNIEI

Altfel spus, se poate considera început de dovadă scrisă orice scrieré (chiar nesemnată) care provine de la persoana căreia i se opune, dacă face credibil faptul pretins.

În condițiile în care legiuitorul român a înțeles, prin norme generale, să confere o anumită valoare probatorie, respectiv un efect juridic unui înscris nesemnat de partea căreia i se opune, ar fi excesiv să nu se atribuie același efect, respectiv aceeași valoare probatorie unui înscris ce poartă o semnătură electronică avansată, respectiv o semnătură electronică simplă. Într-o asemenea ipoteză, s-ar ajunge la o situație de echivalență între un înscris nesemnat deloc și un înscris ce poartă o semnătură electronică simplă sau avansată. Implicit, s-ar ajunge la situația la care s-ar ignora cu desăvârșire importanța și scopul condițiilor impuse de art. 26 din Regulament cu privire la semnătura avansată.

În plus, semnătura electronică simplă și, cu atât mai mult, cea avansată sunt create prin utilizarea de semnatar a unor date unice de creare a semnăturilor electronice, astfel cum sunt prevăzute de art. 3 pct. 13 din Regulament. Aceste date unice de creare prezintă un grad diferit de securitate, în funcție de trăsăturile acestora – sunt exclusiv sub controlul semnatarului, prezintă un grad ridicat de încredere etc. În orice caz, datele unice de creare prezintă un grad minim de securitate, capabil să asigure chiar și înscrisului în formă electronică, semnat cu o semnătură electronică simplă, o forță probatorie mai mare decât a începutului de dovadă scrisă (de esența căruia este absența cu desăvârșire a semnăturii).

Așa cum am menționat anterior, statul român are obligația de a găsi o soluție legislativă echilibrată prin care să confere efect juridic și semnăturilor electronice simple și avansate.

Tendința în spațiul Uniunii Europene

Există state europene care au reglementat deja, în dreptul intern, efectele juridice ale semnăturii electronice avansate, din dorința de a spori și eficientiza serviciile on-line, activitățile economice electronice și comerțul electronic în interiorul Uniunii Europene.

▪ **Danemarca**

- nu există limitări în ceea ce privește utilizarea semnăturii electronice, iar dacă semnătura electronică este contestată, este obligația părții care pretinde că semnătura este validă să o dovedească.
- legislația din Danemarca permite semnarea prin semnătură electronică avansată a documentelor administrative, a documentelor de înregistrare a terenurilor și a documentelor legate de activitatea de creditare.

▪ **Spania**

- prin Legea nr. 59/2003 privind semnătură electronică și Legea nr. 34/2002 privind comerțul electronic, *credențialele de internet banking sunt asimilate unei semnături olografe*.
- atât semnătura electronică avansată, cât și cea simplă, se bucură de recunoaștere juridică în Spania; valoarea probatorie a semnăturii electronice avansate este consfințită în art. 25 al Legii 59/2003, iar utilizarea acesteia devine din ce în ce mai frecventă, fiind responsabilitatea fiecărei companii de a alege instrumentul adecvat.
- în cazul în care semnătura electronică este utilizată în cadrul unor documente juridice cu valoare probatorie, este important să se utilizeze un instrument tehnologic adecvat și, în special, ca acest instrument să respecte cerințele legale ale semnăturilor electronice avansate, stabilite prin Regulamentul (UE) nr. 910/2014.



PARLAMENTUL ROMÂNIEI

▪ Polonia

- Legea bancară nr. 140/1997 și Regulamentul emis de Consiliul de Miniștrii nr. 236/2004 reglementează în mod expres posibilitatea încheierii de contracte prin mijloace electronice, *credențialele de internet banking fiind asimilate unei semnături olografe.*

▪ Ungaria

- conform legislației în vigoare în Ungaria, regula generală pentru contractele de servicii financiare, incluzând servicii financiare și servicii financiare auxiliare, este acceptarea (*cel puțin a*) semnăturii electronice avansate; excepția de la regulă o constituie contractele de credit ipotecar, care trebuie semnate olograf.
- pentru serviciile de plată sau de constituire de depozite sunt acceptate deja mijloace electronice identificate (mijloace care permit identificarea clară a persoanei și a momentului în care a fost efectuată operațiunea, respectiv recuperarea nealterată a informațiilor).
- documentele private pot fi semnate prin semnătură sau sigiliu electronic avansat, iar legislația permite semnarea electronică în cadrul unui sistem închis auditat (de exemplu, o tableta specială) prin mijloace digitale; în acest caz, un pachet conținând contractul, caracteristicile biometrice și certificatul de identificare a semnatarului se atașează la semnătura electronică avansată a furnizorului.

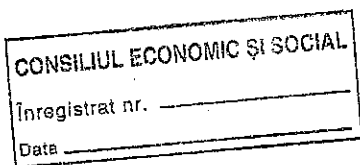
Potrivit Comisiei Europene, respectiv „*eIDAS implementation chart*”, semnătura electronică avansată a fost legiferată deja în Ungaria, Cehia, Marea Britanie, Slovacia și Suedia.

Având în cele arătate, vă rog să susțineți adoptarea prezentei propuneri legislative.

Inițiator,

senator PSD

Șerban NICOLAE



PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

SENATUL

LEGE

privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice

Parlamentul României adoptă prezenta lege

Capitolul I – Dispoziții generale

Art. 1. – Prezenta lege stabilește regimul juridic al semnăturii electronice, al sigiliului electronic și al înscrisurilor în formă electronică, precum și condițiile furnizării de servicii de certificare a semnăturilor electronice.

Art. 2. – Prezenta lege transpune în legislația internă 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, denumit în continuare „Regulamentul”, normă cu aplicare directă în statele membre ale Uniunii Europene.

Art. 3. –

- (1) Prezenta lege nu aduce atingere dispozițiilor legale privind încheierea și valabilitatea contractelor sau a altor obligații juridice sau procedurale privind forma și se completează cu dispozițiile legale privind încheierea, validitatea și efectele actelor juridice.
- (2) Nicio dispoziție a prezentei legi nu poate fi interpretată în sensul limitării autonomiei de voință și a libertății contractuale a părților. Părțile pot stabili în mod liber admisibilitatea probatorie a unui înscris în formă electronică asupra căruia s-a încorporat, atașat sau a asociat logic o semnătură electronică printr-o convenție specială în acest sens, dispozițiile art. 256 din Codul de procedură civilă fiind pe deplin aplicabile.

Art. 4. – În vederea asigurării bunei funcționări a pieței, cu un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere, prezenta lege:

- a) stabilește condițiile de recunoaștere a mijloacelor de identificare electronică a persoanelor fizice și juridice care intră sub incidența unui sistem notificat de identificare electronică al unui stat membru al Uniunii Europene;
- b) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice;
- c) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unui site internet.

Art. 5. –

- (1) Prezenta lege se aplică sistemelor de identificare electronică care au fost notificate potrivit Regulamentului și prestatorilor de servicii de încredere cu sediul în România.



PARLAMENTUL ROMÂNIEI

(2) Prezenta lege nu se aplică prestării de servicii de încredere care sunt utilizate exclusiv în sisteme închise potrivit legii sau din acordurile încheiate între un set definit de participanți.

Art. 6. – Organismele publice și private din România au obligația de a lua măsuri pentru ca serviciile de încredere prestate și produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective să fie accesibile persoanelor cu handicap.

Art. 7. – În aplicarea prezentei legi, se aplică următoarele definiții:

- „identificare electronică” – 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;
- „mijloace de identificare electronică” – unitate materială și/sau imaterială care conține date de identificare personală și care este folosită în scopul autentificării unui serviciu online;
- „date de identificare personală” – set de date care să permită stabilirea identității unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;
- „sistem de identificare electronică” – sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice sau persoane fizice reprezentând persoane juridice;
- „autentificare” – proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii și integrității unor date în format electronic;
- „beneficiar” – persoană fizică sau juridică care beneficiază de un serviciu de identificare electronică sau de un serviciu de încredere;
- „organism din sectorul public” – autoritate regională sau locală, organism de drept public sau 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;
- „organism de drept public” – organism astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE a Parlamentului European și a Consiliului;
- „semnatar” – persoană fizică care creează o semnătură electronică;
- „semnătură electronică” – date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;
- „semnătură electronică avansată” – semnătură electronică ce îndeplinește cerințele prevăzute la articolul 26 din Regulament;
- „semnătură electronică calificată” – 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;
- „date de creare a semnăturilor electronice” – date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;



PARLAMENTUL ROMÂNIEI

- „certificat pentru semnătura electronică” – 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;
- „certificat calificat pentru semnătură electronică” – certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în Regulament;
- „serviciu de încredere” – un serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în oricare dintre următoarele:
 - 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;
 - b) crearea, verificarea și validarea certificatelor pentru autentificarea unui site internet;
 - c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;
- „serviciu de încredere calificat” – un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de Regulament;
- „organism de evaluare a conformității” – 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;
- „prestator de servicii de încredere” – persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;
- „prestator de servicii de încredere calificat” – 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;
- „produs” – hardware sau software ori componente relevante de hardware sau software, destinate să fie utilizate pentru prestarea de servicii de încredere;
- „dispozitiv de creare a semnăturilor electronice” – software sau hardware configurat, utilizat pentru a crea o semnătură electronică;
- „dispozitiv de creare a semnăturilor electronice calificat” – dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în anexa II a Regulamentului;
- „creatorul unui sigiliu” – persoană juridică care creează un sigiliu electronic;
- „sigiliu electronic” – date în format electronic atașate la sau asociate logic cu alte date în format electronic pentru asigurarea originii și integrității acestora din urmă;
- „sigiliu electronic avansat” – sigiliu electronic care îndeplinește cerințele prevăzute la articolul 36 din Regulament;
- „sigiliu electronic calificat” – sigiliu electronic avansat care este creat de un dispozitiv de creare a sigiliilor electronice calificat și care se bazează pe un certificat calificat pentru sigiliile electronice;
- „date de creare a sigiliilor electronice” – date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;



PARLAMENTUL ROMÂNIEI

- „certificat pentru sigiliul electronic” – atestare electronică care face legătura între datele de validare a sigiliului electronic și o persoană juridică și care confirmă numele persoanei respective;
- „certificat calificat pentru sigiliul electronic” – certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa III a Regulamentului;
- „dispozitiv de creare a sigiliului electronic” – software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;
- „dispozitiv de creare a sigiliului electronic calificat” înseamnă un dispozitiv de creare a sigiliului electronic care îndeplinește în mod corespunzător cerințele prevăzute în anexa II a Regulamentului;
- „marcă temporală electronică” – 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;
- „marcă temporală electronică calificată” – marcă temporală electronică care îndeplinește cerințele prevăzute la articolul 42 din Regulament;
- „document electronic” – orice conținut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală; definiția este valabilă și pentru „înscris în formă electronică”;
- „serviciu de distribuție electronică înregistrată” – serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;
- „serviciu de distribuție electronică înregistrată calificată” – serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la articolul 44 din Regulament;
- „certificat pentru autentificarea unui site internet” – atestare care face posibilă autentificarea unui site internet și face legătura între site-ul internet și persoana fizică sau juridică căreia i s-a emis certificatul;
- „certificat calificat pentru autentificarea unui site internet” – 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 a Regulamentului;
- „date de validare” – date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;
- „validare” – procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.

Art. 8. – Toate activitățile prevăzute de prezenta lege sunt supuse dispozițiilor legale privind prelucrarea datelor cu caracter personal.

Art. 9. – Un sistem de identificare electronică notificat potrivit Regulamentului specifică nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare



PARLAMENTUL ROMÂNIEI

electronică emise în cadrul sistemului respectiv, care îndeplinesc criteriile specifice după cum urmează:

- 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.

Capitolul II – Supravegherea

Art. 10. –

- (1) Guvernul desemnează prin hotărâre autoritatea publică care îndeplinește, la nivel național, potrivit Regulamentului, atribuțiile de Organism de supraveghere.
- (2) În exercitarea atribuțiilor, Organismul de supraveghere:
 - a) acordă statutul de calificat prestatorilor de servicii de încredere, precum și serviciilor pe care aceștia le prestează și/sau retrage statutul respectiv
 - b) să informeze organismul responsabil cu lista sigură națională prevăzută de Regulament cu privire la deciziile de acordare sau de retragere a statutului de calificat, cu excepția cazului în care respectivul organism este același cu Organismul de supraveghere;
 - c) prin intermediul activităților de supraveghere *ex ante* și *ex post*, se asigură că prestatorii de servicii de încredere calificați stabiliți pe teritoriul României și serviciile de încredere calificate pe care aceștia le prestează îndeplinesc cerințele stabilite prin Regulament;
 - d) verifică 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;
 - e) prin intermediul activităților de supraveghere *ex post*, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere calificați sau



PARLAMENTUL ROMÂNIEI

- serviciile de încredere pe care le prestează nu îndeplinesc cerințele stabilite prin Regulament, dispune și aplică măsuri de remediere și/sau sancțiuni eficace, proporționale și disuasive, după caz, în legătură cu prestatorii de servicii de încredere necalificați stabiliți pe teritoriul României;
- f) realizează audituri sau solicită unui organism de evaluare a conformității să efectueze o evaluare a conformității prestatorilor de servicii de încredere calificați și a serviciilor prestate de aceștia;
 - g) solicită prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute de Regulament.
 - h) cooperează 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;
 - i) cooperează cu alte organisme de supraveghere și acordă asistență acestora;
 - j) îndeplinește orice alte atribuții stabilite prin Regulament.

Art. 11. –

- (1) Cerințele și procedura de acordare/retragere a statutului de prestator de servicii de încredere calificat, precum și răspunderea acestora sunt cele stabilite prin Regulament.
- (2) Prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează se auditează, pe propria cheltuială, cel puțin o dată la 24 de luni, de către un organism de evaluare a conformității, pentru a asigura că îndeplinesc cerințele prevăzute de Regulament. Raportul de evaluare a conformității fiind transmis organismului de supraveghere în termen de trei zile lucrătoare de la primirea lui.
- (3) Din oficiu, pentru motive temeinice, organismul de supraveghere poate oricând să efectueze un audit sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității privind prestatorii de servicii de încredere calificați, pe cheltuiala prestatorilor de servicii de încredere respectivi, pentru a confirma că aceștia și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute de Regulament.

Capitolul III – Instrumente specifice

Semnătura electronică și documentul electronic

Art. 12. –

- (1) Semnătura electronică constă în folosirea unui procedeu eficient de identificare a unei persoane ce garantează legătura acesteia cu înscrisul în formă electronică astfel semnat și care certifică, până la proba contrară, existența consimțământului semnatarului cu privire la conținutul actului, integritatea acestuia fiind garantată.
- (2) Eficiența procedurii este prezumată, până la proba contrară, în cazul semnăturii electronice avansate și a semnăturii electronice calificate.
- (3) O semnătură electronică avansată îndeplinește cumulativ următoarele cerințe:
 - a) face trimitere exclusiv la semnatar;



PARLAMENTUL ROMÂNIEI

- 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;
 - d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.
- (4) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe.
 - (5) O semnătură electronică calificată bazată pe un certificat calificat eliberat de un stat membru al Uniunii Europene este recunoscută drept semnătură electronică calificată în România.
 - (6) 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.
 - (7) Înscrisul în formă electronică, căruia i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică calificată, este asimilat, în ceea ce privește condițiile și efectele sale, cu înscrisul sub semnătura privată.

Art. 13. –

- (1) Orice înscris în formă electronică poate fi acceptat ca mijloc de probă dacă este inteligibil și, prin circumstanțele creării și stocării sale, prezintă garanții suficiente în privința conținutului său și a identității persoanei de la care emană.
- (2) Valoarea probatorie a înscrisului în formă electronică este apreciată de instanța competentă în funcție, între altele, de tipul și natura înscrisului, de circumstanțele creării și stocării și garanțiile la care acestea dau naștere privind identitatea persoanei de la care emană și integritatea conținutului său, împrejurări ce pot fi dovedite și prin alte mijloace de probă.
- (3) În sensul prezentului articol, dispozițiile art. 282-284 din Codul de procedură civilă sunt pe deplin aplicabile.

Art. 14. –

- (1) În cazul în care, potrivit legii, forma scrisă este cerută ca o condiție de validitate a unui act juridic, un înscris în formă electronică îndeplinește această cerință dacă este îndeplinită una din următoarele cerințe:
 - a) i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică calificată.
 - b) i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică avansată emisă de o autoritate publică din România;
- (2) În cazul în care, potrivit legii, forma scrisă este cerută ca o condiție de probă a unui act juridic, un înscris în formă electronică îndeplinește această cerință dacă este îndeplinită una din următoarele cerințe:
 - a) este recunoscut de cel căruia îi este opus;
 - b) i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică calificată sau avansată;
 - c) i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică, alta decât una calificată sau avansată și are la bază o convenție referitoare la admisibilitatea probatorie a respectivului înscris, încheiată între aceleași părți ori înscrisul consfințește încheierea



PARLAMENTUL ROMÂNIEI

unor acte juridice care constituie acte de dispoziție neevaluabile în bani, acte de dispoziție evaluabile în bani cu o valoare mai mică de 1000 lei, acte de conservare sau acte de administrare.

- (3) Înscrisurile în formă electronică prevăzute la alineatul precedent fac dovada până la proba contrară.

Art. 15. –

- (1) În cazul în care una dintre părți contestă înscrisul în formă electronică sau semnătura electronică, instanța va proceda la verificarea înscrisului în formă electronică, prin modalitățile prevăzute de lege.
- (2) În situația în care se dispune efectuarea unei expertize tehnice de specialitate, expertul trebuie să solicite certificatele pentru semnătura electronică, în cazul în care acestea există, precum și orice alte documente necesare, potrivit legii, pentru identificarea autorului înscrisului, a semnatarului ori a titularului de certificat pentru semnătura electronică.
- (3) Sarcina probei că o semnătură electronică avansată îndeplinește condițiile prevăzute de art. 26 din Regulament revine celui ce o invocă.

Art. 16. – 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.

Art. 17. – Pentru semnăturile electronice utilizate în cadrul serviciilor publice se aplică dispozițiile corespunzătoare organismelor publice din statele membre ale Uniunii Europene astfel cum sunt dispuse prin Regulament.

Crearea, certificarea, validarea și păstrarea semnăturii electronice

Art. 18. – Dispozitivelor de creare a semnăturilor electronice calificate le sunt aplicabile cerințele și procedura de certificare prevăzute de Regulament.

Art. 19. –

- (1) Certificatele calificate pentru semnăturile electronice trebuie să îndeplinească cerințele obligatorii prevăzute de anexa I a Regulamentului.
- (2) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative, dar care nu afectează interoperabilitatea și recunoașterea semnăturilor electronice calificate.
- (3) În cazul în care un certificat calificat pentru semnăturile electronice a fost revocat după activarea inițială, acesta își pierde valabilitatea din momentul în care a fost revocat, fără a putea reveni la statutul său anterior.
- (4) Certificatele calificate pentru semnăturile electronice pot fi suspendate, cu aplicarea următoarelor cerințe:
- a) certificatul își pierde valabilitatea pe parcursul perioadei de suspendare;
 - b) serviciul care oferă informații privind statutul certificatului indică clar suspendarea și durata acesteia.



PARLAMENTUL ROMÂNIEI

Art. 20. –

- (1) Dispozitivele de creare a semnăturilor electronice calificate care îndeplinesc cerințele prevăzute în anexa II a Regulamentului se certifică de un organism autorizat potrivit legii.
- (2) 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 legale pentru evaluarea securității produselor din domeniul tehnologiei informației;
 - b) un proces de evaluare efectuat în conformitate cu standardele pentru evaluarea securității stabilite potrivit Regulamentului, în ipoteza absenței standardelor menționate la lit. a);
 - c) un proces de evaluare efectuat în conformitate cu standarde comparabile stabilite potrivit Regulamentului, în cazul în care un proces de evaluare de securitate declanșat potrivit procedurii prevăzute la lit. a) este în curs de desfășurare.

Art. 21. –

- (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 a Regulamentului;
 - 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 unui 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;
 - g) integritatea datelor semnate nu a fost compromisă;
 - h) cerințele prevăzute la articolul 26 din Regulament 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.

Art. 22. – Un serviciu de validare calificat pentru semnături electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care îndeplinește cumulativ următoarele:

- a) realizează validarea în condițiile prevăzute la art. 18 alin. (1) din prezenta lege;
- 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.



PARLAMENTUL ROMÂNIEI

Art. 23. – 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.

Crearea, certificarea, validarea și păstrarea sigiliului electronic

Art. 24. – Dispozitivelor de creare a sigiliilor electronice le sunt aplicabile cerințele și procedura de certificare prevăzute de Regulament.

Art. 25. –

- (1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute în anexa III a Regulamentului.
- (2) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative, dar care nu afectează interoperabilitatea și recunoașterea sigiliilor electronice calificate.
- (3) 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, fără a putea reveni la statutul său anterior.

Art. 26. – Dispozițiile art. 20, 21 și 22 se aplică în mod corespunzător dispozitivelor de creare a sigiliilor electronice calificate, certificării acestora, sigiliilor electronice, sigiliilor electronice calificate și sigiliilor electronice avansate cu respectarea dispozițiilor corespunzătoare ale Regulamentului.

Art. 27. –

- (1) Unui sigiliu electronic nu i se refuză efectul juridic ori 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 al Uniunii Europene este recunoscut drept sigiliu electronic calificat în România.

Art. 28. –

Sigiliul electronic avansat îndeplinește cumulativ următoarele cerințe:

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



PARLAMENTUL ROMÂNIEI

Art. 29. – Pentru sigiliile electronice utilizate în cadrul serviciilor publice se aplică dispozițiile corespunzătoare organismelor publice din statele membre ale Uniunii Europene astfel cum sunt dispuse prin Regulament.

Mărcile temporale electronice

Art. 30. – 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) se bazează pe o sursă de timp precisă, legată de ora universală coordonată;
- 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.

Art. 31. –

- (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 al Uniunii Europene este recunoscută drept marcă temporală electronică calificată în România.

Serviciile de distribuție electronică înregistrată

Art. 32. –

- (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.
- (2) În cazul datelor transferate între doi sau mai mulți prestatori de servicii de încredere, cerințele de la alin. (1) se aplică tuturor prestatorilor de servicii de încredere calificați.

Art. 33. –



PARLAMENTUL ROMÂNIEI

- (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.

Autentificarea unui site internet

Art. 34. – Pentru autentificarea unui site internet, certificatele calificate îndeplinesc cerințele prevăzute în anexa IV a Regulamentului.

Capitolul IV – Prestarea serviciilor de încredere de către prestatorii de servicii cu sediul sau domiciliul în România

Dispoziții comune

Art. 35. – Prestarea serviciilor de încredere nu este supusă nici unei autorizări prealabile și se desfășoară în concordanță cu principiile concurenței libere și loiale, cu respectarea actelor normative în vigoare.

Art. 36. –

- (1) Prestatorii de servicii de încredere vor asigura accesul la toate informațiile necesare utilizării corecte și în condiții de siguranță a serviciilor sale, inclusiv prin publicarea on-line a ofertei de servicii, a modului de utilizare a acestora și a restricțiilor privind utilizarea, într-un limbaj accesibil.
- (2) Prestatorii de servicii de încredere sunt obligați să specifice clienților în oferta disponibilă on-line și în contract dacă serviciile de încredere pe care le furnizează sunt calificate sau necalificate.
- (3) Informațiile prevăzute la alin (1) vor face referire cel puțin la:
 - a) procedura ce trebuie urmată în scopul creării și verificării semnăturii electronice;
 - b) tarifele percepute;
 - c) modalitățile și condițiile concrete de utilizare a certificatelor, inclusiv limitele impuse utilizării acestora;
 - d) obligațiile care incumbă, potrivit prezentei legi, titularului certificatului, respectiv prestatorului de servicii de încredere;
 - e) căile de soluționare a litigiilor;
 - f) condițiile contractuale de eliberare a certificatului, inclusiv eventualele limitări ale răspunderii prestatorului de servicii de încredere;
 - g) orice alte informații stabilite de organismul de supraveghere.



PARLAMENTUL ROMÂNIEI

Art. 37. -

- (1) Prestatorii de servicii de încredere, precum și personalul angajat sau subcontractanții prestatorului de servicii de încredere, persoană fizică sau juridică, sunt obligați să păstreze secretul informațiilor încredințate în cadrul activității lor profesionale, cu excepția celor în legătură cu care titularul certificatului acceptă să fie publicate sau comunicate terților și a celor solicitate de autoritățile competente, potrivit legii.
- (2) Încălcarea obligației prevăzute la alin. (1) constituie infracțiune de divulgare a secretului profesional, prevăzută și sancționată de Codul Penal.

Art. 38. -

- (1) Prestatorii de servicii de încredere care emit certificate au obligația de a crea și de a menține un registru electronic de evidență a certificatelor eliberate.
- (2) Registrul electronic de evidență a certificatelor eliberate trebuie să facă mențiuni despre:
 - a) data și ora exactă la care certificatul a fost eliberat;
 - b) data și ora exactă la care expiră certificatul;
 - c) dacă este cazul, data și ora exactă la care certificatul a fost suspendat sau revocat, inclusiv cauzele care au condus la suspendare sau la revocare.
- (3) Registrul electronic de evidență a certificatelor eliberate trebuie să fie disponibil permanent pentru consultare, în regim on-line.

Prestarea serviciilor de încredere calificate

Art. 39. - Dacă titularul certificatului utilizează un pseudonim, acest lucru se indică clar beneficiarului, iar identitatea titularului poate fi divulgată doar la solicitarea autorităților competente, potrivit legii sau cu consimțământul titularului.

Art. 40. - Cu 30 de zile înainte de începerea activității, persoanele care intenționează să presteze servicii de încredere calificate au obligația de a notifica Organismului de supraveghere intenția de începere a activității, înaintând totodată un raport de evaluare a conformității, emis de un organism de evaluare a conformității.

Art. 41. - Procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat se stabilește prin ordin al ministrului comunicațiilor și societății informaționale.

Art. 42. -

- (1) La eliberarea certificatelor calificate, în cazul în care solicitantul este o persoană fizică, prestatorii de servicii de încredere au obligația de a verifica identitatea respectivei persoane.
- (2) La eliberarea certificatelor calificate, în cazul în care solicitantul este o persoană juridică, prestatorii de servicii de încredere au obligația de a verifica identitatea persoanei fizice care este reprezentant al respectivei persoane juridice, inclusiv calitatea de reprezentant și de asemenea, de a verifica datele respectivei persoane juridice, în baza de date oficiale



PARLAMENTUL ROMÂNIEI

obținute de la Registrele naționale de înregistrare a persoanelor juridice emise în țara de care aparține respectiva persoană juridică.

- (3) Verificarea identității unui solicitant în vederea eliberării unui certificat calificat se poate face prin oricare din următoarele modalități:
- a) de către prestatorul de servicii de încredere, pe baza actului de identitate, inclusiv cel electronic, a pașaportului sau a permisului de ședere emis de autoritățile competente, în original, al solicitantului și prin prezența fizică a solicitantului în fața unui reprezentant al prestatorului de servicii de încredere calificate, reprezentant care trebuie să aibă un contract cu prestatorul de servicii de încredere, să fie desemnat și pregătit de respectivul prestator de servicii de încredere calificat să efectueze activități de identificare a persoanei;
 - b) de către prestatorul de servicii de încredere, pe baza unui certificat calificat valid la momentul identificării, emis de un prestator de servicii de încredere sau al unei semnături electronice calificate sau al unui sigiliu electronic calificat bazate pe un certificat calificat, valid, emis de același prestator de servicii de încredere;
 - c) de către prestator de servicii de încredere calificate, pe baza unei declarații emise de un notar public, care confirmă identitatea solicitantului, în baza prezenței fizice a solicitantului la respectivul notar public;
 - d) 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 al persoanei juridice și care îndeplinesc cerințele stabilite la articolul 8 din Regulamentul nr. 910/2014, în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”;
 - e) de la distanță, prin orice tehnici și mijloace de identificare electronică care asigură securitatea, certitudinea, integritatea și confidențialitatea datelor de identificare, dacă nivelul de asigurare este echivalent cu prezența fizică, din punct de vedere al fiabilității, conform normelor minimale emise de Organismul de supraveghere în 90 de zile de la intrarea în vigoare a prezentei legi; sistemul de identificare electronică este notificat Organismului de supraveghere cu 45 de zile înainte de începerea activității, cu respectarea normelor minimale emise de acesta;
 - f) prin intermediul unui terț de verificare a identității, în conformitate cu prevederile lit. a)-e);
 - g) prin intermediul unui terț de verificare a identității supus obligațiilor de identificare și verificare a identității în conformitate cu dispozițiile legale privind prevenirea, combaterea și sancționarea spălării banilor și a finanțării terorismului, prin aplicarea procedurilor utilizate și comunicate autorităților de supraveghere din domeniile respective de activitate.

Art. 43. – Prestatorii de servicii de încredere calificați trebuie să păstreze toate informațiile cu privire la un certificat calificat pentru o perioadă de minimum 10 ani de la data încetării valabilității certificatului, potrivit art. 24, alineatul (2) litera h) din Regulament.

Art. 44. –



PARLAMENTUL ROMÂNIEI

- (1) Prestatorii de servicii de încredere calificați trebuie să dispună de resurse financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfășurării activităților legate de certificarea semnăturilor electronice.
- (2) Asigurarea se realizează fie prin subscrierea unei polițe de asigurare la o societate de asigurări, fie prin intermediul unei scrisori de garanție din partea unei instituții financiare de specialitate, fie printr-o altă modalitate stabilită prin decizia Organismului de supraveghere.
- (3) Suma asigurată și suma acoperită prin scrisoarea de garanție sunt stabilite de Organismul de supraveghere.

Contractarea terților de verificare a identității

Art. 45. –

- (1) Dacă prestatorul de servicii de încredere calificat decide să se folosească de un terț de verificare a identității, va încheia în acest sens un contract cu terțul de verificare a identității.
- (2) În contractul încheiat cu terții de verificare a identității, prestatorii de servicii de încredere au obligația de a include clauze privind procedurile de securitate, pregătirea personalului, auditarea periodică, asigurarea terțului de verificare a identității și alte clauze care să diminueze riscul și să asigure repararea în caz de prejudicii.

Art. 46. – Prestatorii de servicii de încredere calificați vor răspunde pentru prejudiciile cauzate oricărei persoane fizice sau juridice ca urmare a nerespectării Regulamentului, respectiv a prezentei legi, de către terții de verificare a identității care îi deservesc.

Revocarea, suspendarea, și încetarea valabilității certificatelor

Art. 47. –

- (1) Orice prestator de servicii de încredere are obligația de a suspenda certificatul în termen de 24 de ore din momentul la care a luat la cunoștință sau trebuia să ia la cunoștință despre apariția oricărui dintre următoarele cazuri:
 - a) la cererea semnatarului, după o prealabilă verificare a identității acestuia;
 - b) în cazul în care o hotărâre judecătorească definitivă dispune suspendarea certificatului;
 - c) în cazul în care informațiile conținute în certificat nu mai corespund realității, dacă nu se impune revocarea certificatului;
 - d) în orice alte situații care constituie cazuri de suspendare a certificatelor eliberate, potrivit procedurilor de securitate și de certificare declarate de prestator potrivit Regulamentului.
- (2) Orice prestator de servicii de încredere care emite certificate are obligația de a revoca certificatul în termen de 24 de ore din momentul în care a luat cunoștință sau trebuia și putea să ia cunoștință despre apariția oricărui dintre următoarele cazuri:
 - a) la cererea semnatarului, după o prealabilă verificare a identității acestuia;
 - b) la decesul sau punerea sub interdicție a semnatarului;
 - c) în cazul în care o hotărâre judecătorească definitivă dispune revocarea;



PARLAMENTUL ROMÂNIEI

- d) dacă se dovedește în mod neîndoielnic că certificatul a fost emis în baza unor informații eronate sau false;
 - e) în cazul în care informațiile esențiale conținute în certificat nu mai corespund realității;
 - f) atunci când confidențialitatea datelor de creare a semnăturii a fost încălcată;
 - g) în cazul în care certificatul a fost utilizat în mod fraudulos;
 - h) în orice alte situații care constituie cazuri de revocare a certificatelor eliberate, potrivit procedurilor de securitate și de certificare declarate de prestator potrivit Regulamentului.
- (3) Prestatorul de servicii de încredere îl va informa de urgență pe titular despre suspendarea sau revocarea certificatului, împreună cu motivele care au stat la baza deciziei sale.
 - (4) Prestatorul de servicii de încredere va înscrie mențiunea de suspendare sau de revocare a certificatului în registrul electronic de evidență a certificatelor eliberate prevăzut la art. 38, în termen de 24 de ore de la data la care a fost adoptată decizia respectivă.
 - (5) Suspendarea sau revocarea va deveni opozabilă terților de la data înscrierii sale în lista de certificate suspendate, respectiv revocate gestionată de prestatorul de servicii de încredere calificat, în conformitate cu standardele tehnice în vigoare și în registrul prevăzut la art. 38.

Art. 48. –

- (1) În cazul în care prestatorul de servicii de încredere intenționează să înceteze activitățile, acesta va informa cu cel puțin 30 de zile înainte de încetare Organismul de supraveghere.
- (2) Organismul de supraveghere trebuie să verifice existența și aplicarea corectă a dispozițiilor privind planurile de încetare potrivit art. 17 alin (4) lit. (i) din Regulament.

Registrul prestatorilor de servicii de încredere calificați

Art. 49. –

- (1) Organismul de supraveghere are obligația de a menține și de a actualiza Registrul prestatorilor de servicii de încredere calificați, denumit în continuare Registru.
- (2) Registrul constituie evidența oficială a prestatorilor de servicii de încredere calificați de care este responsabil Organismul de supraveghere.
- (3) Registrul are rolul de a asigura, prin efectuarea înregistrărilor prevăzute de prezenta lege, stocarea datelor de identificare și a unor informații legate de activitatea prestatorilor de servicii de încredere calificați, precum și informarea publicului cu privire la datele și informațiile stocate.
- (4) Conținutul și structura Registrului se stabilesc de către Organismul de supraveghere, în termen de 30 de zile de la intrarea în vigoare a prezentei legi, în conformitate cu articolul 22 din Regulament și cu Decizia de punere în aplicare nr. 1505/2015 de stabilire a specificațiilor tehnice și a formatelor pentru listele sigure în temeiul articolului 22 alineatul (5) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.



PARLAMENTUL ROMÂNIEI

Art. 50. – Înregistrarea în Registrul prevăzut la art. 49 a datelor de identificare și a informațiilor necesare cu privire la activitatea prestatorilor de servicii de încredere calificați, se efectuează pe bază de cerere individuală, care trebuie transmisă la Organismul de supraveghere, cel târziu la data începerii activității prestatorului.

Art. 51. –

- (1) Registrul este public și se actualizează permanent de către Organismul de supraveghere.
- (2) Condițiile gestionării Registrului, accesul efectiv la informațiile pe care le conține, informațiile care pot fi oferite solicitanților și modul de actualizare a acestuia se stabilesc prin normele tehnice și metodologice emise de Organismul de supraveghere, în termen de 30 de zile de la data intrării în vigoare a prezentei legi.

Art. 52. –

- (1) Radierea prestatorilor de servicii de încredere calificați din Registor se efectuează pe baza comunicării făcute de către prestator Organismului de supraveghere cu cel puțin 30 de zile înainte de data încetării activității sale.
- (2) Radierea se poate efectua și din oficiu de către Organismul de supraveghere, în situația în care acesta constată pe orice altă cale că prestatorul și-a încetat activitatea.

Capitolul V – Recunoașterea certificatelor eliberate de prestatori de încredere calificați străini și a dispozitivelor calificate de creare a semnăturilor electronice calificate în cadrul altor state

Art. 53. –

- (1) Un prestator de servicii de încredere calificat, care a obținut acest statut într-un stat membru al Uniunii Europene, în conformitate cu dispozițiile Regulamentului, are dreptul de a-și desfășura activitatea pe teritoriul României fără a fi necesară parcurgerea vreunei proceduri de autorizare sau notificare, cu respectarea regulilor privind prestarea de servicii de încredere impuse de statul în care prestatorul își are domiciliul sau sediul.
- (2) Certificatul calificat eliberat de către un prestator de servicii de încredere cu domiciliul sau cu sediul într-un stat membru al Uniunii Europene, potrivit Regulamentului, este recunoscut ca fiind echivalent din punct de vedere al efectelor juridice cu certificatul calificat eliberat de un prestator de servicii de încredere cu domiciliul sau sediul în România.

Art. 54. – Certificatul calificat eliberat de către un prestator de servicii de încredere cu domiciliul sau cu sediul într-un stat terț, care nu este membru al Uniunii Europene, pentru un cetățean al respectivului stat este recunoscut ca fiind echivalent din punct de vedere al efectelor juridice cu certificatul calificat eliberat de un prestator de servicii de încredere cu domiciliul sau sediul în România, dacă certificatul sau prestatorul de servicii de încredere care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între România sau Uniunea Europeană și alte state sau organizații internaționale, pe bază de reciprocitate și în conformitate cu prevederile Regulamentului.



PARLAMENTUL ROMÂNIEI

Art. 55. – Dispozitivele calificate de creare a semnăturilor și sigiliilor electronice calificate în cadrul unui alt stat membru al Uniunii Europene, în conformitate cu prevederile Regulamentului sunt recunoscute ca atare și în România.

Obligațiile titularilor de certificate

Art. 56. – Titularii de certificate sunt obligați să solicite, de îndată, revocarea certificatelor, în cazul în care:

- a) au pierdut datele de creare a semnăturii electronice;
- b) au motive să creadă că datele de creare a semnăturii electronice au ajuns la cunoștința unui terț neautorizat;
- c) informațiile esențiale cuprinse în certificat nu mai corespund realității.

Capitolul VI – Accesarea serviciilor publice on-line și păstrarea documentelor în format electronic

Art. 57. –

- (1) În scopul accesării serviciilor publice on-line, fiecare autoritate sau instituție publică își definește prin ordin al conducătorului instituției metodele de autentificare, identificare și autorizare.
- (2) Aceste metode se stabilesc în funcție de nivelul de încredere necesar accesării sau utilizării fiecărui serviciu public, în urma efectuării unei analize interne de risc și a unei analize de impact asupra protecției datelor cu caracter personal, la propunerea administratorului de sistem.
- (3) Nivelul de încredere solicitat pentru utilizarea serviciilor publice on-line respectă principiile proporționalității și necesității.
- (4) Metodologia de analiză a riscului și de analiză a impactului asupra protecției datelor cu caracter personal se aprobă prin decizie a președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, care se publică în Monitorul Oficial al României, Partea I, în termen de 30 de zile de la data intrării în vigoare a prezentei legi.
- (5) Orice prelucrare a datelor cu caracter personal, prin mijloace automate, inclusiv analiza impactului asupra protecției datelor cu caracter personal, se poate face numai în condițiile prevăzute de Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 și de Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general de protecție a datelor).

Art. 58. – Prin ordin al conducătorului autorității sau instituției publice se stabilesc condițiile de păstrare a documentelor interne în format electronic.

Art. 59. – Condițiile de păstrare trebuie să asigure:

- a) protecția datelor cu caracter personal



PARLAMENTUL ROMÂNIEI

- b) accesul la documentele electronice
- c) realizarea de copii de siguranță
- d) măsuri de securitate, tehnice și organizatorice.

Art. 60. – Prestatorii de servicii de încredere calificați trebuie să se asigure că îndeplinirea condițiilor și măsurilor prevăzute la art. 59 sunt respectate și de furnizorii lor de servicii, respectiv de terțele părți care au acces la documentele electronice sau la datele cu caracter personal ale semnatarilor.

Capitolul VII – Sancțiuni

Art. 61. – Constituie contravenție, dacă potrivit legii nu constituie infracțiune, și se anționează cu amendă de la 15.000 lei la 75.000 lei fapta prestatorului serviciilor de încredere care:

- a) omite să efectueze notificarea prevăzută la art. 40;
- b) împiedică exercitarea atribuțiilor de control de către Organismul de supraveghere prin personalul desemnat în acest sens;
- c) omite să efectueze notificarea prevăzută la art. 48.

Art. 62. – Constituie contravenție, dacă potrivit legii nu constituie infracțiune, și se anționează cu amendă de la 75.000 lei la 750.000 lei fapta prestatorului serviciilor de încredere care:

- a) nu respectă prevederile art. 11, prin nefurnizarea informațiilor prevăzute la art. 36 alin. (2) și (3), respectiv în condițiile prevăzute la alin. (1) sau prin furnizarea lor inexactă
- b) nu respectă dispozițiile art. 38;
- c) eliberează certificate prezentate titularilor ca fiind calificate, care nu conțin mențiunile prevăzute la Anexa I a Regulamentului;
- d) eliberează certificate care conțin informații inexacte, informații care sunt contrare legii, bunelor moravuri sau ordinii publice, ori informații a căror exactitate nu a fost verificată
- e) eliberează certificate calificate fără a verifica identitatea solicitantului în condițiile prezentei legi;
- f) nu respectă prevederile art. 43;
- g) nu ia măsuri pentru asigurarea confidențialității în cursul procesului de generare a datelor pentru crearea semnăturilor electronice, în situația în care sunt generate astfel de date;
- h) stochează, reproduce sau dezvăluie terților datele de creare a semnăturilor electronice, fără consimțământul expres al semnatarului;
- i) utilizează dispozitive de creare a semnăturilor electronice care nu respectă cerințele prevăzute în Anexa II a Regulamentului;
- j) nu suspendă sau nu revocă certificatele eliberate în termenul legal, dacă suspendarea sau revocarea este obligatorie;
- k) continuă să desfășoare activități legate de certificarea semnăturilor electronice în situația în care Organismul de supraveghere a dispus suspendarea sau încetarea activității prestatorului de servicii de încredere;



PARLAMENTUL ROMÂNIEI

- l) desfășoară activități legate de certificarea semnăturilor electronice, folosindu-se fără a avea dreptul de calitate de prestator de servicii de încredere calificat.

Art. 63. –

- (1) Constatarea contravențiilor și aplicarea sancțiunilor prevăzute în prezentul capitol se face de către personalul cu atribuții de control din cadrul Organismului de supraveghere.
- (2) Prin excepție de la prevederile art. 28 alin. (1) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare și ale art. 22 alin. (2) din Legea nr. 203/2018 privind măsuri de eficientizare a achitării amenzilor contravenționale, în cazul sancțiunilor aplicate pentru săvârșirea contravențiilor prevăzute la art. 36 și 37, contravenientul poate achita, în termen de cel mult 15 zile de la data înmânării sau comunicării procesului-verbal de constatare a contravenției și de aplicare a sancțiunii, jumătate din cuantumul amenzii aplicate, despre această posibilitate făcându-se mențiune în procesul verbal.

Capitolul VIII – Dispoziții finale

Art. 64. –

- (1) În termen de 30 de zile de la data intrării în vigoare a prezentei legi, guvernul aprobă prin hotărâre, la propunerea Organismului de supraveghere, norme de aplicare a legii.
- (2) Ordinul ministrului Comunicațiilor și Societății Informaționale nr. 449/2017 privind procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014, va fi actualizat în termen de 30 de zile de la intrarea în vigoare a prezentei legi, prin ordin al conducătorului Organismului de supraveghere.

Art. 65. – Dispozițiile prezentei legi se completează, în mod corespunzător, cu prevederile Regulamentului (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.

Art. 66. –

- (1) La data intrării în vigoare a prezentei legi, Legea nr. 455/2001 privind semnătura electronică, republicată în Monitorul Oficial al României, Partea I, nr. 316 din 30 aprilie 2014, cu modificările ulterioare, precum și orice dispoziții contrare se abrogă.
- (2) Orice referire la Legea nr. 455/2001 privind semnătura electronică, va fi considerată o referire la prezenta lege și la 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.



PARLAMENTUL ROMÂNIEI

Art. 65. – Prezenta lege intră în vigoare în termen de 30 de zile de la data publicării în Monitorul Oficial al României, Partea I.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (1) din Constituția României, republicată.

PREȘEDINTELE CAMEREI DEPUTAȚILOR

MARCEL CIOLACU

PREȘEDINTELE SENATULUI

CĂLIN POPESCU TĂRICEANU