**TABEL COMPARATIV PROPUNERI AMENDAMENTE**

**Propunere legislativă privind utilizarea semnăturii electronice, a mărcii temporale şi prestarea serviciilor de încredere bazate pe acestea (L524/2023)**

| **Forma iniţiatorilor** | **Modificări propuse** | **Observații / Motivare** |
| --- | --- | --- |
| **LEGE privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea** | **LEGE privind utilizarea și prestarea serviciilor de încredere** | *Având în vedere că Regulamentul (UE) nr. 910/2014 prevede toate serviciile, considerăm oportună tratarea tuturor*. |
| **Art. 1. Cadrul de reglementare al legii**   1. Prezenta lege creează cadrul juridic intern de aplicare directă 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, publicat în Jurnalul Oficial al Uniunii Europene seria L nr. 257 din 28 august 2014, denumit în continuare *Regulamentul (UE) nr. 910/2014*, și de preluare în ordinea juridică internă a măsurilor lăsate la latitudinea statelor membre. 2. Prezenta lege clarifică anumite aspecte ale utilizării semnăturii electronice, a sigiliului electronic, a mărcii temporale și a documentelor electronice cărora li s-a aplicat o semnătură electronică, o marcă temporală sau un sigiliu electronic, stabilește condițiile prestării serviciilor de încredere și atribuțiile autorităților și instituțiilor publice în domeniul prestării serviciilor de încredere. 3. Prezenta lege se completează cu dispozițiile legale privind încheierea, validitatea și efectele actelor juridice. 4. Prezenta lege reglementează cadrul juridic general în materia efectelor juridice ale semnăturilor electronice și este aplicabilă în măsura în care utilizarea și efectele unei semnături electronice nu se reglementează distinct prin acte cu putere de lege cu caracter special. | **ADR:**  **Art. 1. Cadrul de reglementare al legii**   * + 1. **Prezenta lege stabilește măsurile necesare de punere**   **în aplicare a Regulamentului (UE)** [**nr. 910/2014**](https://lege5.ro/Gratuit/gqydimjsgu/regulamentul-nr-910-2014-privind-identificarea-electronica-si-serviciile-de-incredere-pentru-tranzactiile-electronice-pe-piata-interna-si-de-abrogare-a-directivei-1999-93-ce?d=2017-08-13) **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, publicat în Jurnalul Oficial al Uniunii Europene seria L nr. 257 din 28 august 2014, denumit în continuare *Regulamentul (UE) nr. 910/2014*.**   * + 1. **Prezenta lege stabilește condițiile prestării serviciilor**   **de încredere și atribuțiile autorităților și instituțiilor publice în domeniul prestării serviciilor de încredere și clarifică anumite aspecte ale utilizării semnăturii electronice.**  **(4) ~~Prezenta lege reglementează cadrul juridic general în materia efectelor juridice ale semnăturilor electronice și este aplicabilă în măsura în care utilizarea și efectele unei semnături electronice nu se reglementează distinct prin acte cu putere de lege cu caracter special.~~** | Legea tratează și alte aspecte și servicii de încredere |
| **Art. 2. Definiții**   1. În cadrul prezentei legi sunt aplicabile definițiile relevante prevăzute la art. 3 din Regulamentul (UE) nr. 910/2014. 2. În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații: 3. *date în format electronic* - orice reprezentare digitală a unor acte, fapte sau informații și orice compilație a unor astfel de acte, fapte sau informații, inclusiv sub forma unei înregistrări audio, video sau audiovizuale; 4. *semnătura electronică simplă* - o semnătură electronică ce nu îndeplinește cel puțin una dintre condițiile pe care trebuie să le îndeplinească o semnătură electronică avansată conform art. 26 din Regulamentul (UE) nr.910/2014; 5. *sistem electronic închis -* o platformă electronică utilizată de un set definit de participanți, din cadrul aceleiași entități, ale cărei procese nu au niciun efect direct asupra terților și cu care nu se poate interacționa în mod direct din afara entității în care sistemul este implementat, utilizată pentru procedurile interne ale entității sau în orice alte scopuri similare.   ---------------------  --------------------- | **ADR:**  **Art. 2. Definiții**  (2) În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații:  **b)înscrisul  în formă electronică - *reprezintă o colecţie de date în formă electronică între care există relaţii logice şi funcţionale şi care redau litere, cifre sau orice alte caractere cu semnificaţie inteligibilă, destinate a fi citite prin intermediul unui program informatic sau al altui procedeu similar.***  ***c)semnătura electronică simplă* –o semnatură electronică ale cărei elemente nu îndeplinesc cel putin una dintre condițiile pe care trebuie să le îndeplinească o semnatură electronică avansată conform art. 26 din Regulamentul (UE) nr.910/2014;**  Se introduce o nouă literă la alin. (2) al art. (2) cu următorul cuprins:   1. ***sistem electronic închis -* sistem informatic sau sistem informatic si de comunicatii autorizat pentru functionare in baza dreptului intern sau acreditat in conformitate cu legislatia in domeniu privind informatia protejata si utilizat pentru nevoi proprii sau in baza acordurilor incheiate intre un set definit de participanți.**   **--------------------------------**  **M.A.I.**  Se introduce o nouă literă la alin. (2) al art. (2) cu următorul cuprins:  **d)înscris în formă electronică – conţinut sub formă text, creat şi stocat în formă electronică, asimilat documentului electronic.**  **--------------------------------**  **CP CONCORDIA:**  Se introduce un nou alineat la art. 2, respectiv alin. (3) cu următorul cuprins:  **(3)„Prevederile prezentei legi cu privire la semnătura electronică bazată pe un certificat digital sunt aplicabile și pentru semnătura electronică bazată pe alte tehnologii, în măsura în care prin lege nu se prevede altfel.”** | Este necesară această mențiune întrucât Codul de procedură civilă face referire la înscrisul în formă electronică, care era definit în Legea 455/2001, Lege care prin prezenta va fi abrogată.  **-------------------**  Având în vedere prevederile Regulamentului (UE) nr. 910/ 2014 care stabilesc o neutralitate a legii din punctul de vedere al tehnologiei folosite, astfel încât efectele juridice pe care le acordă să fie realizabile prin orice mijloc tehnic atât timp cât cerințele legale imperative sunt îndeplinite (a se vedea Preambul 27), considerăm necesar a exista în lege o asemenea prevedere generală care să stabilească regimul juridic general atât pentru semnăturile bazate pe certificat cât și pe cele bazate pe alte tehnologii. Acolo unde există particularități pentru un anumit tip de semnătură, proiectul de lege prevede expres acest lucru. |
| **Art. 3. Efecte juridice generale**   1. Toate tipurile de semnătură electronică prevăzute în Regulamentul (UE) nr. 910/2014 sau în prezenta lege produc efecte juridice și pot fi utilizate ca mijloace de probă în fața instanțelor de judecată. 2. Actul juridic în format electronic, semnat cu semnătura electronică având nivelul minim de încredere prevăzut de lege pentru acel tip de act juridic, produce aceleași efectele juridice ca același act juridic în format letric. 3. Valabilitatea semnăturii electronice se verifică în raport cu condițiile pe care trebuie să le îndeplinească la momentul semnării documentului electronic, iar expirarea valabilității certificatului în baza căruia a fost aplicată semnătura electronică nu afectează valabilitatea sau efectele documentului semnat. Prevederile prezentului alineat sunt valabile și în cazul semnăturilor electronice avansate care nu se bazează pe un certificat digital, ci folosesc alte tehnologii. 4. Perioada maximă de valabilitate a certificatului pentru semnătura electronică avansată se stabilește de emitentul certificatului pentru o perioadă de maxim 5 (cinci) ani. Autoritatea de supraveghere și reglementare în domeniu este responsabilă pentru stabilirea perioadelor de valabilitate în cazul semnăturilor electronice avansate care nu se bazează pe un certificat digital, ci folosesc alte tehnologii. 5. Înscrisul în formă electronică este asimilat documentului electronic.   **------------------------**  **Art. 3. Efecte juridice generale**  (1)Toate tipurile de semnătură electronică  prevăzute în Regulamentul (UE) nr. 910/2014 sau în prezenta lege produc efecte juridice și pot fi utilizate ca mijloace de probă în fața instanțelor de judecată.  (2)Actul juridic în format electronic, semnat cu semnătura electronică având nivelul minim de încredere prevăzut de lege pentru acel tip de act juridic, produce aceleași efectele juridice ca același act juridic în format letric.  (3) Valabilitatea semnăturii electronice se verifică în raport cu condițiile pe care trebuie să le îndeplinească la momentul semnării documentului electronic, iar expirarea valabilității certificatului în baza căruia a fost aplicată semnătura electronică nu afectează valabilitatea sau efectele documentului semnat. Prevederile prezentului alineat sunt valabile și în cazul semnăturilor electronice avansate care nu se bazează pe un certificat digital, ci folosesc alte tehnologii.  (5)Înscrisul în formă electronică este asimilat documentului electronic. | **ADR:**  **Art. 3. Efecte juridice generale**  **(2)Actul juridic în formă electronică semnat cu semnătura electronică impusă de lege pentru acel tip de act juridic produce efectele juridice prevăzute în legea specială.**  **(3)Semnătura electronică aplicată unui** **document electronic, potrivit art. 4, face dovada, până la proba contrară, cu privire la recunoașterea documentului electronic.**  Se introduce un nou alineat la art. 3, respectiv alin. (6) cu următorul cuprins:  **(6)Valabilitatea documentului electronic semnat cu semnătură electronică nu este afectată de valabilitatea certificatului care stă la baza semnăturii, după caz.**  **---------------------------------**  **M.A.I.**  **Art. 3. Efecte juridice generale**  **(1)Toate tipurile de semnături electronice, inclusiv semnătura electronică simplă, produc efectele juridice conform Regulamentului (UE) nr. 910/2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE.**  **(2)Actul juridic în format electronic, semnat cu tipul de semnătură electronică impus de lege sau cu semnătură electronică calificată, produce aceleaşi efecte juridice ca actul juridic în format letric.**  **(3)** Valabilitatea semnăturii electronice se verifică în raport cu condițiile pe care trebuie să le îndeplinească la momentul semnării documentului electronic, iar expirarea valabilității certificatului în baza căruia a fost aplicată semnătura electronică nu afectează valabilitatea sau efectele documentului semnat. **~~Prevederile prezentului alineat sunt valabile și în cazul semnăturilor electronice avansate care nu se bazează pe un certificat digital, ci folosesc alte tehnologii.~~**  **~~(5)Înscrisul în formă electronică este asimilat documentului electronic.~~** |  |
| **Art. 4. Efecte juridice în funcție de tipul de semnătură electronică**  (1) Documentul electronic semnat cu o semnătură electronică calificată este asimilat, în ceea ce privește condițiile și efectele sale, cu înscrisul sub semnătură privată, în condițiile art. 25 alin. (2) din Regulamentul (UE) nr. 910/2014. Semnătură electronică calificată produce aceleași efecte juridice ca semnătura olografă.  (2) Documentul electronic emis de către o autoritate sau de o instituție publică sau de către o persoană în exercitarea și în limitele atribuțiilor sale de putere publică, semnat cu o semnătură electronică calificată, sau care are aplicat un sigiliu electronic calificat este asimilat unui înscris autentic.  (3) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de validitate a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată sau cu o semnătură electronică avansată care, în condițiile prezentei legi, produce aceleași efecte ca și semnătura olografă.  (4) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de probă a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată, o semnătură electronică avansată sau cu o semnătură electronică simplă în condițiile alin. (9).  (5) Documentul electronic semnat cu o semnătură electronică avansată produce aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă în oricare dintre următoarele cazuri:   * 1. actul juridic a fost semnat cu o semnătură electronică avansată creată cu un certificat digital emis de o autoritate sau o instituție publică din România;   2. documentul electronic este recunoscut de cel căruia îi este opus, recunoașterea putând să rezulte și din faptul neechivoc al executării în tot sau în parte, de către cel care contestă semnătura electronică avansată, a obligațiilor care s-au născut din documentul electronic;   3. părțile au agreat în mod expres, printr-un înscris distinct, semnat cu semnătură olografă sau cu semnătură electronică calificată, faptul că vor conferi semnăturii electronice avansate efectele juridice ale semnăturii olografe. Părțile confirmă prin același act faptul că au înțeles riscurile și sarcina probei privind semnătura electronică avansată. În cazul raporturilor juridice în care ambele părți sunt profesioniști în sensul art. 3 alin. (2) din Legea 287/2009 privind Codul Civil, cu modificările și completările ulterioare, înscrisul distinct se poate semna și cu semnătură electronică avansată.   (6) Documentul electronic semnat cu o semnătură electronică avansată emis de o persoană juridică de drept privat și utilizată într-un sistem închis produce în acel sistem închis aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă.  (7) În interacțiunea dintre utilizatorii unui sistem electronic închis, membrii sistemului pot agrea valoarea și efectele juridice pentru orice tip de semnătură electronică.  (8) Prevederile alin. (7) sunt aplicabile pentru orice sistem electronic în care toți participanții sunt identificați cu un nivel de asigurare ridicat sau substanțial, în conformitate cu punctele 2.1.2 și 2.1.3 din Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 de stabilire a unor specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) 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. Aceste sisteme electronice sunt supuse unui proces de auditare, care va trebui repetat cel puțin o dată la doi ani și care vizează cel puțin securitatea datelor și garantarea trasabilității tuturor acțiunilor utilizatorilor din sistem ce vizează autentificarea și semnarea electronică.  (9) Documentul electronic semnat cu semnătură electronică simplă produce aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă, în cazul actelor de dispoziție evaluabile în bani cu o valoare mai mică de jumătate din salariul minim brut pe economie și dacă înscrisul semnat cu o semnătură electronică simplă este recunoscut de cel căruia îi este opus, recunoașterea putând să rezulte și din faptul neechivoc al executării în tot sau în parte, de către cel care contestă semnătura electronică simplă, a obligațiilor care s-au născut din înscrisul în formă electronică.  (10) Un document electronic semnat cu mai multe tipuri de semnătură electronică produce efectele juridice conferite de semnătura electronică cu gradul de încredere cel mai scăzut.  (11) Dacă legea impune încheierea unui act juridic prin înscris autentificat, este necesară autentificarea potrivit dispozițiilor legale aplicabile, dispozițiile prezentei legi nefiind aplicabile în aceste cazuri.  **---------------------------**  **Art. 4. Efecte juridice în funcție de tipul de semnătură electronică**  (1) Documentul electronic semnat cu o semnătură electronică calificată este asimilat, în ceea ce privește condițiile și efectele sale, cu înscrisul sub semnătură privată, în condițiile art. 25 alin. (2) din Regulamentul (UE) nr. 910/2014. Semnătură electronică calificată produce aceleași efecte juridice ca semnătura olografă.  (2) Documentul electronic emis de către o autoritate sau de o instituție publică sau de către o persoană în exercitarea și în limitele atribuțiilor sale de putere publică, semnat cu o semnătură electronică calificată, sau care are aplicat un sigiliu electronic calificat este asimilat unui înscris autentic.  (3) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de validitate a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată sau cu o semnătură electronică avansată care, în condițiile prezentei legi, produce aceleași efecte ca și semnătura olografă.  (4) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de probă a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată, o semnătură electronică avansată sau cu o semnătură electronică simplă în condițiile alin. (9).  (5) Documentul electronic semnat cu o semnătură electronică avansată produce aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă în oricare dintre următoarele cazuri:   * 1. actul juridic a fost semnat cu o semnătură electronică avansată creată cu un certificat digital emis de o autoritate sau o instituție publică din România;   2. documentul electronic este recunoscut de cel căruia îi este opus, recunoașterea putând să rezulte și din faptul neechivoc al executării în tot sau în parte, de către cel care contestă semnătura electronică avansată, a obligațiilor care s-au născut din documentul electronic;   3. părțile au agreat în mod expres, printr-un înscris distinct, semnat cu semnătură olografă sau cu semnătură electronică calificată, faptul că vor conferi semnăturii electronice avansate efectele juridice ale semnăturii olografe. Părțile confirmă prin același act faptul că au înțeles riscurile și sarcina probei privind semnătura electronică avansată. În cazul raporturilor juridice în care ambele părți sunt profesioniști în sensul art. 3 alin. (2) din Legea 287/2009 privind Codul Civil, cu modificările și completările ulterioare, înscrisul distinct se poate semna și cu semnătură electronică avansată.   (6) Documentul electronic semnat cu o semnătură electronică avansată emis de o persoană juridică de drept privat și utilizată într-un sistem închis produce în acel sistem închis aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă.  (7) În interacțiunea dintre utilizatorii unui sistem electronic închis, membrii sistemului pot agrea valoarea și efectele juridice pentru orice tip de semnătură electronică.  (8) Prevederile alin. (7) sunt aplicabile pentru orice sistem electronic în care toți participanții sunt identificați cu un nivel de asigurare ridicat sau substanțial, în conformitate cu punctele 2.1.2 și 2.1.3 din Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 de stabilire a unor specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) 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. Aceste sisteme electronice sunt supuse unui proces de auditare, care va trebui repetat cel puțin o dată la doi ani și care vizează cel puțin securitatea datelor și garantarea trasabilității tuturor acțiunilor utilizatorilor din sistem ce vizează autentificarea și semnarea electronică.  (9) Documentul electronic semnat cu semnătură electronică simplă produce aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă, în cazul actelor de dispoziție evaluabile în bani cu o valoare mai mică de jumătate din salariul minim brut pe economie și dacă înscrisul semnat cu o semnătură electronică simplă este recunoscut de cel căruia îi este opus, recunoașterea putând să rezulte și din faptul neechivoc al executării în tot sau în parte, de către cel care contestă semnătura electronică simplă, a obligațiilor care s-au născut din înscrisul în formă electronică.  (10) Un document electronic semnat cu mai multe tipuri de semnătură electronică produce efectele juridice conferite de semnătura electronică cu gradul de încredere cel mai scăzut.  (11) Dacă legea impune încheierea unui act juridic prin înscris autentificat, este necesară autentificarea potrivit dispozițiilor legale aplicabile, dispozițiile prezentei legi nefiind aplicabile în aceste cazuri.  **Art. 4 alin (3)**  (3) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de validitate a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată sau cu o semnătură electronică avansată care, în condițiile prezentei legi, produce aceleași efecte ca și semnătura olografă.  **Art. 4 alin (5)**  (5) Documentul electronic semnat cu o semnătură electronică avansată produce aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă în oricare dintre următoarele cazuri:  a) actul juridic a fost semnat cu o semnătură electronică avansată creată cu un certificat digital emis de o autoritate sau o instituție publică din România;  **Art. 4 alin (9)**  (9) Documentul electronic semnat cu semnătură electronică simplă produce aceleași efecte juridice ca și un înscris semnat cu o semnătură olografă, în cazul actelor de dispoziție evaluabile în bani cu o valoare mai mică de jumătate din salariul minim brut pe economie și dacă înscrisul semnat cu o semnătură electronică simplă este recunoscut de cel căruia îi este opus, recunoașterea putând să rezulte și din faptul neechivoc al executării în tot sau în parte, de către cel care contestă semnătura electronică simplă, a obligațiilor care s-au născut din înscrisul în formă electronică.  --------------------------  **Art. 4 alin (4)**  (4) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de probă a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată, o semnătură electronică avansată sau cu o semnătură electronică simplă în condițiile alin. (9).  **Art. 4 alin (8)**  (8) Prevederile alin. (7) sunt aplicabile pentru orice sistem electronic în care toți participanții sunt identificați cu un nivel de asigurare ridicat sau substanțial, în conformitate cu punctele 2.1.2 și 2.1.3 din Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 de stabilire a unor specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) 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. Aceste sisteme electronice sunt supuse unui proces de auditare, care va trebui repetat cel puțin o dată la doi ani și care vizează cel puțin securitatea datelor și garantarea trasabilității tuturor acțiunilor utilizatorilor din sistem ce vizează autentificarea și semnarea electronică. | **ADR:**  **Art. 4. Efecte juridice în funcție de tipul de semnătură electronică**   1. **Înscrisul în formă electronică este asimilat documentului electronic. Documentul electronic semnat cu o semnătură electronică calificată este asimilat, în ceea ce privește condițiile și efectele sale, cu înscrisul sub semnătură privată, în condițiile art. 25 din Regulamentul (UE) nr. 910/2014. Semnătură electronică calificată produce aceleași efecte juridice ca semnătura olografă.**   **(3) În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de validitate a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată sau cu o semnătură electronică avansată creată în condițiile alin. (5) lit. a și c.**  **(5)**  **c)părțile au agreat în mod expres, printr-un înscris distinct, semnat cu semnătură olografă sau cu semnătură electronică calificată, faptul că vor conferi semnăturii electronice avansate efectele juridice ale semnăturii electronice calificate. Părțile confirmă prin același act faptul că au înțeles riscurile și sarcina probei semnăturii electronice avansate. În cazul raporturilor juridice în care ambele părți sunt profesioniști în sensul art. 3 alin. (2) din Legea 287/2009 privind Codul Civil, cu modificările și completările ulterioare, înscrisul distinct se poate semna și cu semnătură electronică avansată.**  Se introduce un nou alineat la art. 4, respectiv alin. (12) cu următorul cuprins:  **(12) Documentele electronice semnate cu semnătură electronică se păstrează și se arhivează în conformitate cu Legea arhivelor Naționale și legislația privind arhivarea electronică.**  **-----------------------------------**  **M.A.I.**  Se modifică art.4 cu următorul cuprins:  **Art. 4. Efecte juridice în funcție de tipul de semnătură electronică**  **(1) Documentul electronic semnat cu o semnătură electronică simplă sau semnătură electronică avansată este socotit ca început de dovadă scrisă.**  **(2) Documentul electronic prevăzut la alin. (1) produce aceleaşi efecte ca un înscris semnat cu semnătură olografă, dacă este recunoscut de cel căruia îi este opus. Recunoaşterea poate să rezulte şi din faptul neechivoc al executării în tot sau în parte, de către cel care contestă documentul.**  **(3) Documentul electronic semnat de către cetăţean cu semnătură electronică avansată creată de către o autoritate sau instituţie publică din România este asimilat înscrisului sub semnătură privată. În relaţiile cu instituţiile publice, documentele electronice semnate cu semnătură electronică avansată creată de către o autoritate sau instituţie publică au aceeaşi valoare juridică ca documentele semnate olograf.**  **(4) Documentul electronic semnat cu o semnătură electronică calificată este asimilat cu înscrisul sub semnătură privată. Semnătura electronică calificată are efectul juridic echivalent al unei semnături olografe, conform Regulamentului (UE) nr. 910/2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE.**  **(5) Documentul electronic emis de către o autoritate sau instituţie publică sau de către o persoană în exercitarea şi în limitele atribuţiilor sale de putere publică, semnat cu o semnătură electronică calificată, semnătură electronică avansată creată de către o autoritate sau instituţie publică din România sau, după caz, documentul care are aplicat sigiliu electronic calificat este asimilat unui înscris autentic.**  **(6) Dispoziţiile prezentei legi nu sunt aplicabile procedurilor notariale de autentificare a înscrisurilor.**  **CP CONCORDIA:**  **Art. 4 alin (3)**  ”(3) în cazul în care potrivit legii, forma scrisă este cerută ca o condiţie de validitate a unui act juridic, documentul electronic îndeplineşte această cerinţă dacă a fost semnat cu o semnătură electronică calificată sau cu o semnătură electronică avansată ~~care,~~ în condiţiile **alin. 5 de mai jos** ~~prezentei legi,~~  ~~produce aceleaşi efecte ca şi semnătura olografa~~.”  **Art. 4 alin (5)**  (5) Documentul electronic **pentru care forma scrisă este cerută ca o condiție de validitate**, semnat cu o semnătură electronică avansată produce aceleaşi efecte juridice ca şi un înscris semnat cu o semnătură olografa în oricare dintre următoarele cazuri:  a) actul juridic a fost semnat cu o semnătură electronică avansată creată cu un certificat digital emis de o autoritate sau o instituţie publică din România **sau de către un prestator de servicii de încredere calificat**;  **Art. 4 alin (9)**  Se modifică alin (9) la care se introduc literele a), b) şi c) cu următorul cuprins:  **”(9) Documentul electronic semnat cu semnătură electronică simplă produce aceleaşi efecte juridice ca un înscris semnat cu o semnătură olografa în oricare dintre următoarele cazuri:**  **a) în cazul actelor patrimoniale ~~de dispoziţie~~ evaluabile în bani cu o valoare mai mică decât ~~jumătate din~~ salariul minim brut pe economie;**  **b) înscrisul semnat cu o semnătură electronică simplă este recunoscut de cel căruia îi este opus, recunoaşterea putând să rezulte şi din faptul neechivoc al executării în tot sau în parte, de către cel care contestă semnătura electronică simplă, a obligaţiilor care s-au născut din înscrisul în formă electronică;**  **c) părțile au agreat în mod expres, printr-un înscris distinct anterior, puterea doveditoare pe care o conferă semnăturii electronice simple aplicate pe un anumit înscris electronic.”**  **--------------------------**  **Asociatia Furnizorilor de Servicii de Certificare**  **Art. 4 alin (4)**  În cazul în care potrivit legii, forma scrisă este cerută ca o condiție de probă a unui act juridic, documentul electronic îndeplinește această cerință dacă a fost semnat cu o semnătură electronică calificată, o semnătură electronică avansată **care, în condițiile prezentei legi, produce aceleași efecte ca și semnătura olografă**, sau cu o semnătură electronică simplă în condițiile alin. (9).  **Se elimină alin (8) al art. 4** | Este necesară această mențiune întrucât Codul de procedură civilă face referire la înscrisul în formă electronică, care era definit în Legea 455/2001, Lege care prin prezenta va fi abrogată.  Pentru claritatea normei juridice, propunem amendarea alin 3 al art. 4. Din discuțiile purtate în faza premergătoare înregistrării acestui proiect de lege, înțelegerea noastră a fost că, raportat la importanța și efectele actelor pentru care legea a cerut forma scrisă ad validitatem, se dorește impunerea unor cerințe suplimentare de siguranță pentru emiterea semnăturilor electronice avansate astfel încât să se asigure un nivel adecvat de încredere între participanții la circuitul civil și a proteja astfel raporturile juridice dar și consumatorii de servicii digitale, într-o cât mai mare măsură. Astfel, pentru rigoarea juridică este necesară clarificarea faptului că prevederile alin. (5) sunt aplicabile doar pentru semnarea electronică a actelor pentru care forma scrisă este cerută ca și condiție de validitate.  Amendamentul de la primul paragraf are în vedere corelarea cu amendamentul de la alin. (3) de mai sus.  Amendamentul de la lit. a are în vedere extinderea aplicabilității acestui alineat asupra semnăturilor avansare emise de furnizori de servicii de încredere calificate, întrucât astfel de furnizori prezintă suficiente garanții de securitate și siguranță a sistemelor și procedurilor utilizate (i.e. având in vedere cerințele la care aceștia sunt supuși conform Regulamentului (UE) nr. 910/ 2014).  Suplimentar, astfel cum rezultă și din Avizul Consiliului Legislativ, instituirea obligativității ca un certificat pentru semnătura electronică avansată să fie emis numai de o autoritate sau instituție publică din România ar putea crea un obstacol în libera circulație a serviciilor, aspect contrar dispozițiilor Tratatului privind funcționarea Uniunii Europene și, totodată, ar putea fi de natură să conducă la încălcarea principiilor liberei concurențe.  Considerăm că utilizarea semnăturii electronice simple doar în cazul în care forma scrisă este cerută ca o condiție de probă a actului juridic, nu și când forma scrisă este cerută ad validitatem, este pe deplin justificată, date fiind garanțiile reduse pe care acest tip de semnătură le prezintă. Astfel, în ceea ce privește sfera de aplicare a semnăturii simple, pentru ca o astfel de semnătură să producă efectele juridice intenționate de lege, propunem nuanțarea soluțiilor în noul Proiect de lege, în sensul în care aceasta să poată fi utilizată pentru semnarea oricăror acte juridice cu caracter patrimonial pentru care forma scrisă este solicitată ad probationem, dacă este îndeplinită una din condițiile de mai jos (caracter alternativ):  a) părțile au agreat în mod expres, printr-un înscris distinct, puterea doveditoare pe care o conferă semnăturii electronice simple.  b) înscrisul în formă electronică este recunoscut de cel căruia îi este opus (e.g. dacă există în acest sens un act de recunoaștere expresă sau implicită, ce poate fi inclusiv un act de executare în tot sau în parte a obligațiilor care s-au născut din actul juridic) sau  c) în cazul actelor patrimoniale a căror valoare totală, la data încheierii actului, nu depășește salariul minim brut pe economie.  Propunem înlocuirea actelor de dispoziție cu acte patrimoniale având în vedere faptul că astfel sfera de aplicarea se extinde și poate cuprinde și acte de conservare și administrare (e.g. contract de închiriere) în limita valorică prevăzută în textul de lege. Totodată, jumătate din valoarea salariului minim brut este o valoare destul de redusă și nu ține cont de nevoia adaptării valorii la evoluția economiei și la nevoile companiilor.  ARGUMENTELE NOASTRE ÎN SUSȚINEREA NEVOII DE FLEXIBILIZĂRII SUPLIMENTARE A TIPURILOR DE ACTE POSIBIL A FI SEMNATE CU SEMNĂTURA ELECTRONICĂ SIMPLĂ:  1. Ne dorim să NU fie îngradită libertatea părților de a conferi forță probantă semnăturii electronice simple atunci când a. cealaltă parte recunoaște semnătura sau b. părțile au convenit asupra forței probante a semnăturii utilizate (e.g., printr-o clauză din contract sau altă convenție). În ambele cazuri, ar trebui să nu conteze caracterul evaluabil în bani al actului sau valoarea acestuia.  2. Recunoașterea sau convenția părților ar trebui să fie suficiente, și în linie cu intenția proiectului de lege de eliminare a barierelor și procedeelor birocratice în special în relațiile B2B/ B2C, când legea nu impune condiții suplimentare pentru valabilitatea actului.  3. Mai mult, ar trebui să se țină cont că nu toate contractele pentru care legea solicită forma scrisă ad probationem pot fi evaluate în bani. A lăsa condiția valorii actului ca și condiție a valorii juridice a semnăturii electronice simple ar conduce la un dezavantaj în practică și o limitare excesivă a folosirii unui asemenea tip de semnătură.  4. Mai multe State Membre, dintre care și Belgia, Olanda, Spania sau Slovenia, recunosc în condiții similare cu cele propuse de noi, forța probantă echivalentă pentru documentele care poartă semnătură electronică simplă.  5. Conform preambulului din e-IDAS, pct. 48, deși un nivel ridicat de securitate este necesar pentru a asigura recunoașterea reciprocă a semnăturilor electronice, semnăturile electronice cu un nivel mai scăzut de asigurare a securității ar trebui să fie, de asemenea, acceptate. E-IDAS conferă libertatea de a reglementa si efectele juridice ale semnăturii avansate/semnăturii simple.  Prin urmare, suntem de părere că semnătura electronică simplă este o soluție eficientă pentru numeroase sectoare de activitate. De aceea, considerăm că este avantajos ca în astfel de domenii documentele semnate electronic să poată fi probate în instanța fără dificultate.  Consideram ca este important ca, pentru securitatea cicuitului juridic al documentelor, in cazul cand forma scrisa este ceruta si ca o conditie de proba a actului juridic, sa se utilizee doar o semnatura avansata care, implicit, produce aceleasi efecte ca si semnatura olografa, conform aliniatului (5). Daca nu se face aceasta precizare, deoarece nu exista o modalitate bine definita de a identifica faptul ca o semnatura este avansata, exista riscul fie ca documentele sa se semneze cu o semnatura care de fapt nu este avansata, fie ca orice semnatura sa fie contestatata pe motiv ca nu ar fi avansata, ceea ce va duce la o presiune pe sistemul judiciar.  Intelegem ca sensul acestui aliniat este ca intr-un sistem electronic (de exempu un sistem de internet banking) in care identificarea participantilor se face conform cerintelor pentru nivelul substantial sau inalt, participantii pot agrea efectul juridic pentru orice tip de semnatura….In acest caz, sunt mai multe probleme care nu sunt acoperite: 1.cum agreeaza participantii….daca este vorba despre o relatie client furnizor, de exemplu 2.identificarea participantilor pentru acces la sistem poate fi un aspect total separat de procesul de semnare electronica a documentelor - adica degeaba participantii se identifica la un nivel substantial sau inalt, daca semnarea nu se face pe baza acelor credentiale; 3. chiar si daca semnarea se face in baza acelor credentiale, nu este suficient doar faptul ca identificarea s-a facut la un astfel de nivel, pentru a avea o semnatura electronica care sa garanteze vointa semnatarului; 4. Nu este clar daca procesul de auditare mentionat este unul obligatoriu si nici care scopul acestui proces de auditare – de exemplu, cum poate clientul unei banci sa obtina dovezi cu privire la trasbilitatea actiunilor reprezentantilor bancii in sistemul informatic pe care il gestioneaza ...chiar banca? |
| **Art. 5. Recunoașterea documentului care poartă semnătura electronică**   1. În cazul nerecunoașterii sau a contestării semnăturii electronice calificate sau a sigiliului calificat, verificarea validității va fi efectuată de către instanță. Sarcina probei cu privire la încălcarea condițiilor legale și tehnice aferente semnăturii electronice calificate sau a sigiliului electronic calificat aparține celui care le contestă. 2. În cazul în care una dintre părți nu recunoaște sau contestă semnătura electronică avansată, semnătura electronică simplă ori sigiliul electronic avansat aplicate unui document, verificarea validității se realizează prin una dintre următoarele modalități: 3. prin metode de validare sau certificare disponibile public, validate de autoritatea de supraveghere și reglementare în domeniu; 4. de către emitentul semnăturii electronice avansate, în condițiile art. 11 alin (2); 5. printr-o expertiză tehnică de specialitate, dacă verificarea nu se poate realiza în condițiile lit. a) sau b).   (3) În cazul în care una dintre părți nu recunoaște sau contestă semnătura electronică simplă sau avansată, sarcina probei îndeplinirii condițiilor legale și tehnice aferente aparține celui care invocă validitatea semnăturii.  4) Un document semnat cu o semnătură electronică de orice tip, care în conformitate cu dispozițiile prezentei legi nu are valoare de semnătură olografă, va putea fi considerat început de dovadă scrisă.  **-------------------------------------------------------**  **Art. 5. Recunoașterea documentului care poartă semnătura electronică**  (1)În cazul nerecunoașterii sau a contestării semnăturii electronice calificate sau a sigiliului calificat, verificarea validității va fi efectuată de către instanță. Sarcina probei cu privire la încălcarea condițiilor legale și tehnice aferente semnăturii electronice calificate sau a sigiliului electronic calificat aparține celui care le contestă.  (3) În cazul în care una dintre părți nu recunoaște sau contestă semnătura electronică simplă sau avansată, sarcina probei îndeplinirii condițiilor legale și tehnice aferente aparține celui care invocă validitatea semnăturii.  4) Un document semnat cu o semnătură electronică de orice tip, care în conformitate cu dispozițiile prezentei legi nu are valoare de semnătură olografă, va putea fi considerat început de dovadă scrisă.  **--------------------**  **Art. 5 alin (2)**   1. În cazul în care una dintre părți nu recunoaște sau   contestă semnătura electronică avansată, semnătura electronică simplă ori sigiliul electronic avansat aplicate unui document, verificarea validității se realizează prin una dintre următoarele modalități:  a) prin metode de validare sau certificare disponibile public, validate de autoritatea de supraveghere și reglementare în domeniu;  b) de către emitentul semnăturii electronice avansate, în condițiile art. 11 alin (2);  c) printr-o expertiză tehnică de specialitate, dacă verificarea nu se poate realiza în condițiile lit. a) sau b). | **ADR:**  Se introduce un nou alineat la art. 5, respectiv alin. (5) cu următorul cuprins:  **(5) Sarcina probei încălcării condițiilor legale și tehnice aferente semnăturii electronice calificate sau a sigiliului electronic calificat aparține celui care le contestă.**  **-------------------------------------------------------**  **M.A.I.**  **Art. 5. Recunoașterea documentului care poartă semnătura electronică**  (1)**În cazul nerecunoașterii sau a contestării semnăturii electronice calificate sau a sigiliului calificat, instanța va dispune verificarea validității semnăturii electronice calificate sau a sigiliului calificat.** Sarcina probei cu privire la încălcarea condițiilor legale și tehnice aferente semnăturii electronice calificate sau a sigiliului electronic calificat aparține celui care le contestă.  **~~(3) În cazul în care una dintre părți nu recunoaște sau contestă semnătura electronică simplă sau avansată, sarcina probei îndeplinirii condițiilor legale și tehnice aferente aparține celui care invocă validitatea semnăturii.~~**  **~~4) Un document semnat cu o semnătură electronică de orice tip, care în conformitate cu dispozițiile prezentei legi nu are valoare de semnătură olografă, va putea fi considerat început de dovadă scrisă.~~**  **-------------**  **CP CONCORDIA:**  **Art. 5 alin (2)**  (2) în cazul în care una dintre părţi nu recunoaşte sau contestă semnătura electronică avansată, semnătura electronică simplă ori sigiliul electronic avansat aplicate unui document, verificarea validităţii se realizează prin una dintre următoarele modalităţi:  a) prin metode de validare sau certificare disponibile public, **~~validate de autoritatea de supraveghere şi reglementare în domeniu~~;** | Propunem acest amendament întrucât considerăm prea restrictivă această prevedere. Astfel, există tool-uri de validare a semnăturilor electronice ( ex. Adobe) in care se face inclusiv verificarea semnăturii electronice calificate, iar astfel de tool-uri internaționale nu au vreo certificare de la ADR. Prin urmare, dacă există posibilitatea de verificare a unei semnături electronice în Adobe sau alte motoare de verificare recunoscute la nivel internațional, nu înțelegem de ce am elimina o asemenea metodă de validare prin impunerea acestei limitări. |
| **Art. 6. Sistemele închise**   1. În interiorul autorităților și instituțiilor publice sau în cadrul entităților de drept privat se pot defini sisteme închise în care utilizarea semnăturii electronice și a sigiliului electronic se face în conformitate cu legislația în vigoare și pe baza unor reglementări proprii. 2. Pentru sistemele închise gestionate de către instituțiile din domeniul apărării, ordinii publice și siguranței naționale, acestea pot emite certificate calificate care urmează a fi folosite exclusiv pentru nevoile proprii și ale căror sisteme de generare, evidență și distribuție fac parte din sisteme informatice sau sisteme informatice și de comunicații acreditate în conformitate cu legislația privind nivelul de clasificare al informației protejate. 3. Semnătura electronică și sigiliul electronic urmează regimul juridic general în cazul în care sunt utilizate în interacțiunea cu entități din exteriorul sistemului închis. 4. Schimbul de documente electronice între sistemele administrației publice, care nu implică interacțiunea cu persoanele de drept privat fizice sau juridice, face obiectul alin. (1).   **---------------------------------------------------**  **Art. 6. Sistemele închise**  2)Pentru sistemele închise gestionate de către instituțiile din domeniul apărării, ordinii publice și siguranței naționale, acestea pot emite certificate calificate care urmează a fi folosite exclusiv pentru nevoile proprii și ale căror sisteme de generare, evidență și distribuție fac parte din sisteme informatice sau sisteme informatice și de comunicații acreditate în conformitate cu legislația privind nivelul de clasificare al informației protejate. | **ADR:**  Se introduc două alineate la art. 6, respectiv alin. (5) şi alin. (6) cu următorul cuprins:  **(5) În sensul prevederilor art. 2 alin. (2) din Regulamentul (UE) nr. 910/2014, utilizarea documentelor electronice în sisteme închise se realizează conform legislației în vigoare sau în baza acordurilor încheiate între utilizatorii acestor sisteme.**  **(6) Actele administrative și documentele electronice emise de către administrația publică centrală și locală către persoanele fizice și persoanele juridice de drept privat sunt semnate cu semnătură electronică calificată.**  **---------------------------------------------------**  **M.A.I.**  **Art. 6. Sistemele închise**  2)Pentru sistemele gestionate de către instituțiile din domeniul apărării, ordinii publice și siguranței naționale, acestea pot emite certificate calificate **sau avansate** care urmează a fi folosite exclusiv pentru nevoile proprii și ale căror sisteme de generare, evidență și distribuție fac parte din sisteme informatice sau sisteme informatice și de comunicații acreditate în conformitate cu legislația privind nivelul de clasificare al informației protejate.  Se introduce un nou alineat la art. 6, respectiv alin. (5) cu următorul cuprins:  **(5) Semnătura electronică emisă de o autoritate sau instituţie publică, precum şi de către o persoană juridică de drept privat, utilizată într-un sistem închis în care toţi participanţii sunt identifcaţi în vederea emiterii semnăturii, este asimilată 7n cadrul acelui sistem cu semnătura ologafă. La fiecare 2 ani sistemele închise sunt supuse unui proces de auditare care vizează securitatea datelor şi garantarea trasabilităţii acţiunilor utilizatorilor din sistem referitoare la autentificare şi aplicarea semnăturii electronice.** |  |
| **Art. 9. Autoritatea de reglementare și supraveghere în domeniu**  (1) Responsabilitatea aplicării dispozițiilor prezentei legi și ale Regulamentului (UE) nr. 910/2014 în ceea ce privește prestatorii de marcă temporală revine autorității de reglementare și supraveghere specializată în domeniu, cu aplicarea dispozițiilor Capitolului VI din prezenta lege.  (2) În cadrul Registrului prestatorilor de servicii de încredere calificate și necalificate prevăzut la art. 21 se creează o secțiune distinctă, destinată prestatorilor de servicii de marcare temporală necalificate. Informațiile care trebuie prevăzute în acest registru sunt stabilite de către autoritatea de reglementare și supraveghere specializată în domeniu. | **ADR:**  Se introduce un nou alineat la art. 9, respectiv alin. (9) cu următorul cuprins:  **(3) În termen de 3 luni de la data publicării prezentei legi în Monitorul Oficial al României, Partea I, autoritatea desemnează furnizorul unic de bază de timp și va emite Normele tehnice și metodologice privind acreditarea prestatorilor de servicii de marcare temporală și cerințele tehnice pentru activitatea de marcare temporală.** |  |
| **Art. 10. Dobândirea și pierderea calității de prestator de servicii de încredere**   1. Prestarea serviciilor de încredere nu este supusă unei autorizări prealabile și se desfășoară în concordanță cu principiile concurenței libere și loiale, cu respectarea actelor normative în vigoare. 2. Persoanele juridice care intenționează să presteze servicii de încredere calificate si necalificate transmit, cu 30 de zile înainte de începerea activității, autorității de reglementare și supraveghere specializate în domeniu o notificare privind înregistrarea în Registrul prestatorilor de servicii de încredere calificate și necalificate prevăzut la art. 21. În plus, persoanele juridice care intenționează să presteze servicii de încredere calificate, vor înainta și un raport de evaluare a conformității, emis de un organism de evaluare a conformității și toate informațiile referitoare la procedurile de securitate și de certificare utilizate. 3. În termen de 90 zile de la data intrării în vigoare a prezentei legi, la propunerea Autorității pentru Digitalizarea României (ADR), se aprobă, prin ordin al ministrului cercetării, inovării și digitalizării procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat. Prin același ordin se detaliază și documentația menționată la alin. (2), precum și detalii privind procedurile de control și de sancționare. 4. În cazul în care prestatorul de servicii de încredere intenționează să înceteze activitățile, acesta informează cu cel puțin 30 de zile înainte de încetare autoritatea de reglementare și supraveghere specializată în domeniu. În urma verificării îndeplinirii dispozițiilor privind planurile de încetare potrivit art. 17 alin. (4) lit. (i) din Regulamentul (UE) nr. 910/2014, autoritatea de reglementare și supraveghere specializată în domeniu efectuează radierea prestatorului de servicii de încredere din Registrul prestatorilor de servicii de încredere calificate și necalificate și din Lista sigură existentă la nivel european (Trusted List). 5. Radierea se efectuează din oficiu de către autoritatea de reglementare și supraveghere specializată în domeniu, în situația în care acesta constată pe orice altă cale că prestatorul și-a încetat activitatea. | **ADR:**  **(2)Statutul de prestator de servicii de încredere calificat se dobândește în urma parcurgerii procedurii de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat acordat de către organismul de supraveghere.**  **(3) Persoanele juridice care intenționează să presteze servicii de încredere calificate si necalificate transmit, cu 30 de zile înainte de începerea activității, autorității de reglementare și supraveghere specializate în domeniu o notificare privind înregistrarea în Registrul prestatorilor de servicii de încredere calificate și necalificate prevăzut la art. 21. În plus, persoanele juridice care intenționează să presteze servicii de încredere calificate, vor înainta și un raport de evaluare a conformității, emis de un organism de evaluare a conformității și toate informațiile referitoare la procedurile de securitate și de certificare utilizate.**  **(4)În termen de 90 zile de la data intrării în vigoare a prezentei legi se aprobă, prin decizia președintelui ADR, procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat, precum și procedura de radiere din Lista sigură (Trusted List). Prin aceeași decizie se va detalia și documentația menționată la alin. (2), procedura de sancționare prevăzută la art. 36 alin. (4) și se vor detalia dispozițiile art. 28 alin. (2).**  **(5) În cazul în care prestatorul de servicii de încredere intenționează să înceteze activitățile, acesta informează cu cel puțin 30 de zile înainte de încetare autoritatea de reglementare și supraveghere specializată în domeniu. În urma verificării îndeplinirii dispozițiilor privind planurile de încetare potrivit art. 17 alin. (4) lit. (i) din Regulamentul (UE) nr. 910/2014, autoritatea de reglementare și supraveghere specializată în domeniu efectuează radierea prestatorului de servicii de încredere din Registrul prestatorilor de servicii de încredere calificate și Registrul prestatorilor de servicii de încredere necalificate și din Lista sigură existentă la nivel european (Trusted List).**  Se introduc două alineate la art. 10, respectiv alin. (6) şi alin. (7) cu următorul cuprins:   1. **Prestatorii de servicii de încredere calificați au**   **obligația de a comunica organismului de supraveghere , cu cel puțin 10 zile înainte, orice intenție de modificare a procedurilor de securitate și de certificare, cu precizarea datei și orei la care modificarea intră în vigoare, precum și obligația de a confirma în termen de 24 de ore modificarea efectuată.**   1. **Radierea se efectuează din oficiu de către**   **autoritatea de reglementare și supraveghere specializată în domeniu, în situația în care acesta constată pe orice altă cale că prestatorul și-a încetat activitatea.** | Propunem ca procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat/necalificat să fie aprobată prin decizia Președintelui ADR.  Conform HG 89/2020, de organizare și funcționare a ADR cu modificările și completările ulterioare, autoritatea exercită atribuţiile de organism de supraveghere pentru prestatorii de servicii de încredere calificaţi stabiliţi pe teritoriul României, precum şi luarea măsurilor, după caz, în legătură cu prestatorii de servicii de încredere necalificaţi stabiliţi pe teritoriul României, în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE;  În baza procedurii aprobate de către președinte, ADR acordă statutut calificat pentru prestatorii de servicii de încredere și actualizează Lista Sigură la nivelul Comisiei Europene.  Considerăm necesar să se trateze în prezenta lege faptul că ADR reglementează prin decizia președintelui modalități de recunoaştere, aprobare sau acceptare a procedurii de identificare a persoanei la distanţă. |
| **Art. 12. Obligațiile prestatorilor de servicii de încredere**   1. În vederea **emiterii certificatelor calificate,** prestatorii de servicii de încredere trebuie să îndeplinească cerințele stabilite de Regulamentul (UE) nr. 910/2014 și normele emise de către autoritatea de reglementare și supraveghere în domeniu. 2. În vederea emiterii certificatelor pentru semnătura electronică avansată, prestatorii de servicii de încredere trebuie să îndeplinească următoarele condiții: 3. să dispună de mijloace financiare și de resurse materiale, tehnice și umane corespunzătoare pentru garantarea securității, fiabilității și continuității serviciilor de certificare oferite; 4. să asigure operarea rapidă și sigură a înregistrării informațiilor prevăzute la art. 14 alin. (2), operarea rapidă și sigură a unui serviciu de suspendare și revocare a certificatelor pentru semnătura electronică avansată; 5. să asigure posibilitatea de a se determina cu precizie data și ora exactă a eliberării, a suspendării sau a revocării unui certificat pentru semnătura electronică avansată; 6. să verifice, cu mijloace corespunzătoare și conforme dispozițiilor legale, identitatea și, dacă este cazul, atributele specifice ale persoanei căreia îi este eliberat certificatul pentru semnătura electronică avansată; 7. să folosească personal cu cunoștințe de specialitate, experiență și calificare, necesare pentru furnizarea serviciilor respective, și, în special, competență în domeniul gestiunii, cunoștințe de specialitate în domeniul tehnologiei semnăturii electronice și o practică suficientă în ceea ce privește procedurile de securitate corespunzătoare; 8. să aplice procedurile administrative și de gestiune adecvate și care corespund standardelor recunoscute; 9. să utilizeze produse asociate semnăturii electronice, cu un înalt grad de fiabilitate, care sunt protejate împotriva modificărilor și care asigură securitatea tehnică și criptografică a desfășurării activităților de certificare a semnăturii electronice; 10. să adopte măsuri împotriva falsificării certificatelor și să garanteze confidențialitatea în cursul procesului de generare a datelor de creare a semnăturilor, în cazul în care prestatorii de servicii de încredere generează astfel de date; 11. să păstreze toate informațiile cu privire la un certificat pentru semnătura electronică avansată pentru o perioadă de minimum 10 ani de la data încetării valabilității certificatului și în conformitate cu dispozițiile art. 24 alin. (2) lit. h) din Regulamentul (UE) nr. 910/2014; 12. să nu stocheze, să nu reproducă și să nu dezvăluie terților datele de creare a semnăturii, cu excepția cazului în care semnatarul solicită aceasta; 13. să utilizeze sisteme fiabile pentru stocarea certificatelor pentru semnătura electronică avansată, astfel încât: numai persoanele autorizate să poată introduce și modifica informațiile din certificate; exactitatea informației să poată fi verificată; certificatele să poată fi consultate de terți doar în cazul în care există acordul titularului acestora; orice modificare tehnică, care ar putea pune în pericol aceste condiții de securitate, să poată fi identificată de persoanele autorizate; 14. să creeze un plan actualizat pentru cazul încetării serviciului, pentru a asigura continuitatea serviciului; 15. să asigure un nivel adecvat de securitate cibernetică și fizică a infrastructurii la nivelul căreia se generează și gestionează certificatele și datele cu caracter personal; 16. să creeze un plan de acțiune actualizat, în cazul unui incident de securitate cibernetică, pentru a asigura limitarea compromiterii serviciului; 17. Autoritățile și instituțiile publice care emit certificate digitale pentru crearea semnăturii electronice avansate sunt obligate să parcurgă o procedură de auditare prin care se verifică îndeplinirea tuturor condițiilor prevăzute de prezenta lege pentru emiterea semnăturii electronice avansate. 18. Prestatorii de servicii de încredere sunt obligați să folosească numai dispozitive securizate de creare a semnăturii electronice sau tehnologii securizate care pot fi gestionate la distanță de către aceștia pentru emiterea de certificate calificate și să respecte pe parcursul desfășurării activității procedurile de securitate și de certificare declarate. 19. Atunci când se utilizează un pseudonim, identitatea reală a titularului nu poate fi divulgată de către prestatorul de servicii de încredere decât cu consimțământul titularului sau la cererea unei autorități sau instituții publice competente. 20. Prestatorii de servicii de încredere care emit certificate calificate sunt obligați să încheie o asigurare de răspundere profesională prin subscrierea unei polițe de asigurare la o societate de asigurări pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfășurării activităților legate de prestarea serviciilor de încredere. Suma asigurată este stabilită prin ordinul prevăzut la art. 10 alin. (3). 21. Prestatorii de servicii de încredere au obligația de a facilita exercitarea atribuțiilor de control de către autoritatea de reglementare și supraveghere specializată în domeniu. 22. Prestatorii de servicii de încredere au obligația de a se integra cu Platforma Națională de interoperabilitate reglementată de Legea 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate, cu modificările și completările ulterioare, pentru a valida actele de identitate prezentate de cetățenii români care solicită certificate calificate sau certificate digitale emise de către o autoritate sau instituție publică . ------------------------------------   **Art. 12 alin. (8)**  (8) Prestatorii de servicii de încredere au obligația de a se integra cu Platforma Națională de interoperabilitate reglementată de Legea 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate, cu modificările și completările ulterioare, pentru a valida actele de identitate prezentate de cetățenii români care solicită certificate calificate sau certificate digitale emise de către o autoritate sau instituție publică. | **ADR:**  **(2)În vederea emiterii certificatelor pentru semnatura electronică avansată, prestatorii de servicii de încredere trebuie să îndeplinească următoarele condiții:**  **i) să păstreze toate informațiile cu privire la un certificat pentru semnătura electronică avansată pentru o perioadă de timp corespunzătoare, inclusiv ulterior încetării activității prestatorului de servicii de încredere,potrivit art. 24 alin. (2) lit. h) din Regulamentul (UE) nr. 910/2014;**  **l)să creeze un plan actualizat pentru cazul încetării serviciului, pentru a asigura continuitatea serviciului, plan pe care îl comunică autorității de supraveghere;**  **n)să creeze un plan de acțiune actualizat, în cazul unui incident de securitate cibernetică, pentru a asigura limitarea compromiterii serviciului, plan pe care îl comunică autorității de reglementare și supraveghere în domeniu;**  **-----------------------**  **Asociatia Furnizorilor de Servicii de Certificare**  **Art. 12 alin. (8)**  (8) Prestatorii de servicii de încredere au obligația de a se integra cu Platforma Națională de interoperabilitate reglementată de Legea 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate, cu modificările și completările ulterioare, pentru a valida actele de identitate prezentate de cetățenii români care solicită certificate calificate sau certificate digitale emise de către o autoritate sau instituție publică. **Administratorul** **Platformei Nationala de interoperabilitate va pune la dispozitie mecanismele tehnice necesare pentru validarea actelor de identitate ale cetatenilor romani.**  Se introduce un nou alineat la art. 12, respectiv alin. (9) cu următorul cuprins:  **(9) In sensul aliniatului (8), Directia Generală pentru Evidenta Persoanelor va asigura prestatorilor de servicii de incredere mecanismele tehnice necesare pentru validarea actelor prin Platforma Nationala de interoperabilitate reglementata de Legea 242/2022.** | Obligatia de integrare nu poate produce efecte daca Platforma Nationala de interoperabilitate nu asigura mecanismele de integrare sau baza de date pentru evidenta populatiei nu face parte din Platforma Nationala de interoperabilitate sau nu este accesibila. |
| **Art. 15.** **Cuprinsul certificatului**   * + 1. Certificatul calificat pentru semnătura electronică are structura prevăzută de Regulamentul (UE) nr. 910/2014 la Anexa I. Certificatele calificate vor fi emise în concordanță cu standardele ETSI specifice în vigoare sau cu ultimele versiuni ale acestora, după caz.     2. Certificatul digital pentru semnătura electronică avansată cuprinde în mod obligatoriu următoarele:   1. indicarea faptului că certificatul a fost eliberat cu titlu de certificat pentru semnătură electronică avansată;   2. informații cu privire la tipul de semnătură electronică utilizat și detalii privind cel care are sarcina probei în caz de litigiu;   c) datele de identificare ale prestatorului de servicii de încredere, precum și cetățenia acestuia, în cazul persoanelor fizice, respectiv naționalitatea acestuia, în cazul persoanelor juridice;  d) numele semnatarului sau pseudonimul acestuia, identificat ca atare, precum și alte atribute specifice ale semnatarului, dacă sunt relevante, în funcție de scopul pentru care este eliberat certificatul digital pentru semnătură electronică avansată;  e) codul personal de identificare a semnatarului;  f)datele de verificare a semnăturii, care corespund datelor de creare a semnăturii aflate sub controlul exclusiv al semnatarului;  g)indicarea începutului și sfârșitului perioadei de valabilitate a certificatului;  h)codul de identificare a certificatului digital pentru semnătura electronică avansată;  i) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere care eliberează certificatul pentru semnătura electronică avansată;  j)dacă este cazul, limitele utilizării certificatului pentru semnătura electronică avansată sau limitele valorice ale operațiunilor pentru care acesta poate fi utilizat;  k)orice alte informații stabilite de autoritatea de reglementare și supraveghere specializată în domeniu.  (3) Prestatorul de servicii de încredere atribuie beneficiarului certificatului pentru semnătura electronică avansată un cod personal care să asigure identificarea unică a semnatarului.  (4)Generarea codului personal de identificare și a codului de identificare a certificatului semnătura electronică avansată se face pe baza reglementărilor stabilite de autoritatea de reglementare și supraveghere specializată în domeniu.  (5) La solicitarea beneficiatului, prestatorul de servicii de încredere poate înscrie în certificat și alte informații decât cele menționate la alin. (1), respectiv (2) după o prealabilă verificare a exactității acestor informații.  (6) Certificatul indică în mod expres faptul că este utilizat un pseudonim, atunci când titularul se identifică printr-un pseudonim.  (7) Prestatorul de servicii de încredere poate să indice în cuprinsul unui certificat restricții ale utilizării acestuia, precum și limite ale valorii operațiunilor pentru care acesta poate fi utilizat, cu condiția ca respectivele restricții să poată fi cunoscute de către terți. Prestatorul de servicii de încredere nu este răspunzător pentru prejudiciile rezultând din utilizarea unui certificat cu încălcarea restricțiilor prevăzute în cuprinsul acestuia. | **ADR:**  ~~b) informații cu privire la tipul de semnătură electronică utilizat și detalii privind cel care are sarcina probei în caz de litigiu;~~  b) datele de identificare ale prestatorului de servicii de încredere, precum și cetățenia acestuia, în cazul persoanelor fizice, respectiv naționalitatea acestuia, în cazul persoanelor juridice;  c) numele semnatarului sau pseudonimul acestuia, identificat ca atare, precum și alte atribute specifice ale semnatarului, dacă sunt relevante, în funcție de scopul pentru care este eliberat certificatul digital pentru semnătură electronică avansată;  d) codul personal de identificare a semnatarului;  e)datele de verificare a semnăturii, care corespund datelor de creare a semnăturii aflate sub controlul exclusiv al semnatarului;  f)indicarea începutului și sfârșitului perioadei de valabilitate a certificatului calificat;  g)codul de identificare a certificatului digital pentru semnătura electronică avansată;  h) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere care eliberează certificatul pentru semnătura electronică avansată;  i)dacă este cazul, limitele utilizării certificatului pentru semnătura electronică avansată sau limitele valorice ale operațiunilor pentru care acesta poate fi utilizat;  j)orice alte informații stabilite de autoritatea de reglementare și supraveghere specializată în domeniu. | Conform art. 5 alin 1 sarcina probei revine celui care contestă semnătura |
| **Art. 16. Eliberarea certificatului calificat și necalificat**   1. Înainte de eliberarea certificatului unei persoane fizice, prestatorii de servicii de încredere au obligația de a verifica identitatea respectivei persoane.   (2) Certificatul se eliberează de către prestatorul de servicii de încredere în format digital, conform cu standardele și reglementările naționale și europene aplicabile. Prestatorul de servicii de încredere este obligat să păstreze certificatele emise pentru o perioadă de minim 10 ani.  (3) Verificarea identității unei persoane în vederea eliberării unui certificat calificat, respectiv al unui certificat pentru semnătură electronică avansată se poate face prin oricare din următoarele modalități:  a) de către prestatorul de servicii de încredere, pe baza cărții de identitate, 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 sau a unui sigiliu electronic calificat, valid la momentul identificării, emis de un prestator de servicii de încredere;  c) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului, a fost asigurată fie prezența fizică, fie prezența de la distanță echivalentă cu prezența fizică, din punct de vedere al fiabilității a persoanei fizice sau a unui reprezentant al persoanei juridice care îndeplinesc cerințele stabilite în Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”.  d) 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 emise de autoritatea de reglementare și supraveghere specializate în domeniu în 90 de zile de la intrarea în vigoare a prezentei legi. Sistemul de identificare electronică este notificat autorității de reglementare și supraveghere specializate în domeniu cu 30 de zile înainte de începerea activității, cu respectarea normelor emise de acesta.  e) prin intermediul unui terț de verificare a identității, în conformitate cu prevederile lit. a)-d).  f) 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. 16 alin (3) lit. f)**  ”(3) Verificarea identităţii unei persoane în vederea eliberării unui certificat calificat, respectiv al unui certificat pentru semnătură electronică avansată se poate face prin oricare din următoarele modalităţi:  (.......)  f) prin intermediul unui terţ de verificare a identităţii supus obligaţiilor de identificare şi verificare a identităţii în conformitate cu dispoziţiile legale privind prevenirea, combaterea şi sancţionarea spălării banilor şi a finanţării terorismului, prin aplicarea procedurilor utilizate şi comunicate autorităţilor de supraveghere din domeniile respective de activitate.”  **------------------**  **Art. 16 alin. (3)**  (3) Verificarea identităţii unei persoane în vederea eliberării unui certificat calificat, respectiv al unui certificat pentru semnătură electronică avansată se poate face prin oricare din următoarele modalităţi: | **ADR:**  **Art. 16. Eliberarea certificatului calificat și necalificat**  (**1) Înainte de eliberarea certificatului unei persoane fizice, prestatorii de servicii de încredere au obligația de a verifica identitatea respectivei persoane pe baza unui act de identitate.**  **(3) Verificarea identității unei persoane în vederea eliberării unui certificat calificat, respectiv al unui certificat pentru semnătură electronică avansată se poate face prin oricare din următoarele modalități:**  **c) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului, a fost asigurată fie prezența fizică, fie prezența de la distanță echivalentă cu prezența fizică, din punct de vedere al fiabilității, a persoanei fizice sau a unui reprezentant al persoanei juridice care îndeplinesc cerințele stabilite în Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei din 8 septembrie 2015 în ceea ce privește nivelurile de asigurare „substanțial” sau „ridicat”.**  ~~f) 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.~~  **---------------------**  **CP CONCORDIA:**  **Art. 16 alin (3) lit. f)**  ”(3) Verificarea identităţii unei persoane în vederea eliberării unui certificat calificat, respectiv al unui certificat pentru semnătură electronică avansată se poate face prin oricare din următoarele modalităţi:  (.......)  f) prin intermediul unui terţ de verificare a identităţii **sau de către prestatorul de servicii de încredere supuși** obligaţiilor de identificare şi verificare a identităţii în conformitate cu dispoziţiile legale privind prevenirea, combaterea şi sancţionarea spălării banilor şi a finanţării terorismului, prin aplicarea procedurilor utilizate şi comunicate autorităţilor de supraveghere din domeniile respective de activitate.”  **------------------**  **Asociatia Furnizorilor de Servicii de Certificare**  **Art. 16 alin. (3)**  (3) Verificarea identităţii unei persoane în vederea eliberării unui certificat calificat, respectiv al unui certificat pentru semnătură electronică avansată se poate face **numai** prin oricare din următoarele modalităţi:  Se introduce un nou alineat, respectiv alin. (4) cu următorul cuprins:  **(4)Prevederile alineatului sunt valabile și pentru identificarea semnatarilor in cazul semnăturilor electronice avansate care nu se bazează pe un certificat digital, ci folosesc alte tehnologii.** | Conform Regulamentului 910/2014, prestatorii de servicii verifică prin mijloace corespunzătoare și în conformitate cu legislația națională identitatea persoanei, în acest context este necesară verificarea unui act de identitate in vederea identificării unei persoane la distanță  Considerăm necesar a se completa ipoteza de la lit. f cu posibilitatea prestatorului de servicii de încredere de a face identificarea conform procedurilor utilizate şi comunicate autorităţilor de supraveghere, dacă un astfel de prestator este supus obligaţiilor de identificare şi verificare a identităţii în conformitate cu dispoziţiile legale privind prevenirea, combaterea şi sancţionarea spălării banilor şi a finanţării terorismului. Mai exact, dacă un terț de verificare a identității ar avea acest drept dacă este supus legislației AML, pentru identitate de rațiune si prestatorul de servicii de încredere ar trebuie sa aibă acest drept.  Este necesara adaugarea particulei „numai” pentru a rezulta obligativitatea utilizarii uneia dintre modalitatile de la punctele a-f.  Deoarece propunerea legislativa are in vedere faptul ca o semnatura avansata poate fi creata si pe baza altor tehnologii decat cea bazata pe certificate digitale, este important de precizat ca, si in aceste situatii, identificarea semnatarilor trebuie facuta tot in acelasi mod. |
| **Art. 18. Recunoașterea certificatelor eliberate de prestatorii de servicii de încredere** **străini**   1. Certificatul calificat eliberat de către un prestator de servicii de încredere cu domiciliul sau cu sediul într-un alt stat membru al Uniunii Europene 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 cu sediul în România. 2. Prestatorii de servicii de încredere calificate, înființați într-un stat membru al Uniunii Europene, și care sunt înscriși în Lista Sigură la nivelul UE vor putea presta servicii de încredere în România. | **ADR:**  Se introduce un nou alineat, respectiv alin. (3) cu următorul cuprins:  **(3) Certificatul calificat emis de un prestator de servicii de încredere, stabilit într-o țară terță din afara Uniunii Europene, este recunoscut în temeiul unui acord încheiat între Uniunea Europeană și țara terță în cauză, sau o organizație internațională, conform art. 218 din TFUE.** |  |
| **Art. 20. Atribuțiile autorității de reglementare și supraveghere specializată**   * + 1. În calitate de autoritate de reglementare și supraveghere specializată în domeniu, ADR exercită atribuții de control prin personalul anume împuternicit în acest sens.     2. În realizarea atribuțiilor prevăzute de prezenta lege, ADR se asigură că personalul încadrat păstrează confidențialitatea surselor și a informațiilor în legătură cu sesizările sau plângerile primite și nu dezvăluie datele de care a luat cunoștință cu ocazia exercitării atribuțiilor.     3. În îndeplinirea rolului prevăzut la art. 19, ADR:  1. acordă sau retrage calitatea de prestator calificat de servicii de încredere, respectiv calitatea de prestator necalificat de servicii de încredere; 2. asigură că prestatorii de servicii de încredere calificate stabiliți pe teritoriul României și serviciile de încredere calificate pe care aceștia le prestează îndeplinesc cerințele stabilite de Regulamentul (UE) nr. 910/2014; 3. realizează demersuri de verificare regulată a prestatorilor de servicii de încredere calificate și necalificate și a serviciilor prestate de aceștia; 4. solicită prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute de Regulamentul (UE) nr. 910/2014 sau de prezenta lege; 5. poate, din oficiu sau la solicitarea oricărei persoane interesate, să verifice sau să dispună verificarea conformității activităților unui prestator de servicii de încredere cu dispozițiile prezentei legi sau Regulamentul (UE) nr. 910/2014; 6. cooperează cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, dacă din demersurile de verificare reies încălcări ale normelor de protecție a datelor cu caracter personal; 7. îndeplinește orice alte atribuții stabilite prin Regulamentul (UE) nr. 910/2014 în sarcina organismului de supraveghere; 8. aplică măsuri de remediere și sancțiuni în conformitate cu prezenta lege. 9. Pentru realizarea atribuțiilor prevăzute de prezenta lege, ADR are dreptul: 10. să aibă acces liber, permanent, în orice loc în care se află echipamentele necesare prestării serviciilor de încredere; 11. să solicite orice document sau informație necesară în vederea realizării controlului; 12. să verifice punerea în aplicare a oricăror proceduri de securitate sau de certificare utilizate prestatorii de servicii de încredere; 13. să sigileze orice echipamente necesare prestării serviciilor de încredere sau să rețină orice document ce are legătură cu această activitate, pe o perioadă care nu poate depăși 15 zile, dacă această măsură se impune; 14. ADR are obligația de a crea, menține și actualiza Registrul prestatorilor de servicii de încredere calificate și necalificate, care constituie evidența oficială a prestatorilor de servicii de încredere. Registrul este public, actualizat în mod permanent și este disponibil pe pagina de internet a ADR. 15. ADR are obligația de a defini și de a detalia mijloacele de identificare recunoscute pentru emiterea certificatelor calificate și a certificatelor pentru semnătura electronică avansată, printre care introducerea posibilității identificării prin mijloace electronice de identificare și prin mijloace de identificare de la distanță echivalente cu prezența fizică a titularului certificatului calificat. 16. ADR are obligația de a stabili modalitățile de certificare a dispozitivelor de creare a semnăturilor electronice și a sigiliilor electronice de către organisme de certificare din România. 17. ADR are obligația de a elabora normele tehnice și metodologice de aplicare dispozițiilor privind marca temporală.   **...............................**  **Art. 20 alin (3)**  ”(3) în îndeplinirea rolului prevăzut la art. 19, ADR:  a) acordă sau retrage calitatea de prestator calificat de servicii de încredere, respectiv calitatea de prestator necalificat de servicii de încredere;” | **ADR:**  **Art. 20. Atribuțiile autorității de reglementare și supraveghere specializată**  **~~(2) În realizarea atribuțiilor prevăzute de prezenta lege, ADR se asigură că personalul încadrat păstrează confidențialitatea surselor și a informațiilor în legătură cu sesizările sau plângerile primite și nu dezvăluie datele de care a luat cunoștință cu ocazia exercitării atribuțiilor.~~**  **(2)În îndeplinirea rolului prevăzut la art. 15, ADR**:  **c)realizează demersuri de verificare și poate solicita, în orice moment, prestatorilor de servicii de încredere calificați să efectueze un audit conform normelor emise de către autoritatea de reglementare și supraveghere în domeniu sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității privind serviciile prestate de aceștia pentru a confirma că serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute de Regulamentul (UE) nr. 910/2014 și de prezenta Lege;**  **d) realizează demersuri de verificare și poate solicita, în orice moment, prestatorilor de servicii de încredere necalificați să efectueze un audit, conform normelor emise de către autoritatea de reglementare și supraveghere în domeniu pentru a confirma că serviciile de încredere pe care le prestează îndeplinesc cerințele prevăzute de prezenta Lege;**  **e)solicită prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute de Regulamentul (UE) nr. 910/2014 sau de prezenta lege;**  **f)poate, din oficiu sau la solicitarea oricărei persoane interesate, să verifice sau să dispună verificarea conformității activităților unui prestator de servicii de încredere cu dispozițiile prezentei legi sau Regulamentul (UE) nr. 910/2014;**  **g)cooperează cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal dacă din demersurile de verificare și audit reies încălcări ale normelor de protecție a datelor cu caracter personal;**  **h)îndeplinește orice alte atribuții stabilite prin Regulamentul (UE) nr. 910/2014 în sarcina organismului de supraveghere;**   1. **aplică măsuri de remediere și sancțiuni în conformitate cu prezenta lege.** 2. **să verifice punerea în aplicare a oricăror proceduri de securitate sau de certificare utilizate de prestatorii de servicii de încredere**;   **(4) ADR instituie, menține și publică liste care includ informații referitoare la prestatorii de servicii de încredere calificați pentru care este responsabilă, împreună cu informații referitoare la serviciile de încredere calificate prestate de aceștia, în conformitate cu Regulamentul (UE) nr. 910/2014. ADR reglementează prin decizia președintelui modalități de recunoaştere, aprobare sau acceptare a procedurii de identificare a persoanei la distanţă utilizând mijloace video în vederea emiterii de certificate calificate.**  **............................**  **CP CONCORDIA:**  **Art. 20 alin (3)**  ”(3) în îndeplinirea rolului prevăzut la art. 19, ADR:  a) acordă sau retrage calitatea de prestator calificat de servicii de încredere **calificate, ~~respectiv calitatea de prestator necalificat de servicii de încredere;”~~** | Obligația de a păstra confidențialitatea surselor și informațiilor rezultă deja din natura statutului de funcționar public.  Propunem amendarea acestui articol pentru corelare cu prevederile art. 10 alin 2 din Proiect. Conform Preambul (36) din Regulamentul (UE) 910 *” Prestatorii de servicii de încredere necalificați ar trebui să facă obiectul unor activități de supraveghere ex post lejere și bazate pe reacție, justificate de natura serviciilor și a operațiunilor lor.”.* Astfel, înțelegem rațiunea notificării de către aceștia a ADR asupra îndeplinirii condițiilor din legislație pentru prestarea serviciilor de încredere, însă credem că este excesiv ca ei să fie supuși unui proces de autorizare. |
| **Art. 21. Registrul prestatorilor de servicii de încredere calificate și necalificate**  (1) Registrul prestatorilor de servicii de încredere stabilit la nivel național cuprinde:  a) Registrul prestatorilor de servicii de încredere calificate (numit Lista Sigură / Trusted List) și  b) Registrul prestatorilor de servicii de încredere necalificate;  (2) Conținutul și structura Registrului prestatorilor de servicii de încredere calificate și necalificate se stabilesc de către ADR în termen de 30 de zile de la intrarea în vigoare a prezentei legi, în conformitate cu prevederile art. 22 din Regulamentul (UE) nr. 910/2014 și cu Decizia de punere în aplicare (UE) 2015/1505 a Comisiei din 8 septembrie 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;  (3) Registrul constituie evidența oficială a:  a) prestatorilor de servicii de încredere calificate care au sediul în România;  b) prestatorilor de servicii de încredere necalificate care au sediul în Romania și care emit certificate pentru semnătura electronică avansată sau care furnizează alte tehnologii pentru crearea unei semnături electronice avansate care nu se bazează pe un certificat digital;  c) prestatorilor de servicii de încredere necalificate care au sediul în România, auditați, care emit certificate pentru semnătura electronică avansată;  d) prestatorilor de servicii de încredere necalificate, altele decât emiterea de certificate;  e) prestatorilor de servicii de încredere cu sediul sau domiciliul în alt stat care nu este membru UE, ale căror certificate calificate sunt recunoscute la nivel național;  (4) Înregistrarea în Registrul prestatorilor de servicii de încredere calificate și necalificate, conținutul cererii și documentația necesară prevăzută la art. 10 alin. (2) se stabilesc prin Ordinul prevăzut la art. 10 alin. (3). | **ADR:**  **Art. 21. Registrul prestatorilor de servicii de încredere calificați și necalificați**  Se introduce o nouă litera la alin. (1) art.21, cu următorul cuprins:  **c) Registrul prestatorilor de servicii de marcare temporală necalificați;**    **(3) Registrul constituie evidența oficială a:**  **~~e) prestatorilor de servicii de încredere cu sediul sau domiciliul în alt stat care nu este membru UE, ale căror certificate calificate sunt recunoscute la nivel național;~~** |  |
| **Art. 22. Activitatea de control efectuată de autoritatea de reglementare și supraveghere specializată în domeniu**   * + 1. Dacă în urma controlului efectuat se constată nerespectarea dispozițiilor prezentei legi, a Regulamentului (UE) nr. 910/2014 ori a reglementărilor emise de autoritatea de reglementare și supraveghere specializată în domeniu, aceasta solicită prestatorului de servicii de încredere să se conformeze, în termenul pe care îl stabilește. În aceste cazuri, autoritatea de reglementare și supraveghere specializată în domeniu aplică sancțiunile prevăzute în Capitolul VIII.   (2)În cazul în care dispune încetarea activității unui prestator de servicii de încredere care emite certificate digitale, autoritatea de reglementare și supraveghere specializată în domeniu asigură fie revocarea certificatelor emise de prestatorul de servicii de încredere, fie preluarea activității și a registrului electronic de evidență a certificatelor eliberate și a serviciului de revocare a acestora de către un alt prestator de servicii de încredere, cu acordul acestuia. Oricare din aceste măsuri sunt comunicate de îndată titularilor certificatelor.  (3)În cazul în care activitatea prestatorului de servicii de încredere nu este preluată de către un alt prestator, prestatorul de servicii de încredere este obligat să asigure revocarea tuturor certificatelor eliberate de el. În caz contrar, acestea sunt revocate pe cheltuiala sa de către a autoritatea de reglementare și supraveghere specializată în domeniu.  (4)Autoritatea de reglementare și supraveghere specializată în domeniu va prelua și va păstra arhivele și registrul electronic de evidență a certificatelor eliberate de prestatorul de servicii de încredere a cărui activitate nu a fost preluată de către un alt prestator de servicii de încredere. | **ADR:**  **Art. 22. Activitatea de control efectuată de autoritatea de reglementare și supraveghere specializată în domeniu**  **(1)Dacă în urma controlului efectuat se constată nerespectarea dispozițiilor prezentei legi, a Regulamentului (UE) nr. 910/2014 ori a reglementărilor emise de autoritatea de reglementare și supraveghere specializată în domeniu, aceasta solicită prestatorului de servicii de încredere să se conformeze, în termenul pe care îl stabilește, dispozițiilor legale. În aceste cazuri, autoritatea de reglementare și supraveghere specializată în domeniu aplică sancțiunile principale și complementare prevăzute în Capitolul VIII, putând dispune inclusiv suspendarea sau încetarea activității prestatorului de servicii de încredere și radierea acestuia din Registrul prestatorilor de servicii calificați și necalificați.** |  |
| **Art. 23. Semnăturile electronice create cu certificate emise de autorități și instituții publice**   1. Autoritățile și instituțiile publice care emit certificate pentru semnături electronice vor respecta normele privind identificarea și autentificarea, emise de autoritatea de supraveghere și reglementare în domeniu și de către MCID. 2. În cazul în care autoritățile și instituțiile publice care furnizează certificate digitale nu au posibilitatea onorării unei solicitări în vederea furnizării acestora, autoritățile sau instituțiile publice solicitante pot achiziționa servicii de încredere furnizate de prestatori de servicii de încredere privați, cu respectarea dispozițiilor legale aplicabile achizițiilor publice.   **----------------------------------------------------**  **Art. 23. Semnăturile electronice create cu certificate emise de autorități și instituții publice**   1. Autoritățile și instituțiile publice care emit certificate pentru semnături electronice vor respecta normele privind identificarea și autentificarea, emise de autoritatea de supraveghere și reglementare în domeniu și de către MCID.   **------------------- ---------------------------**  **Art. 23. Semnăturile electronice create cu certificate emise de autorități și instituții publice**  (l) Autoritățile și instituțiile publice care emit certificate pentru semnături electronice vor respecta normele privind identificarea și autentificarea, emise de autoritatea de supraveghere și reglementare în domeniu și de către MCID. | **ADR:**  **Art. 23. Semnăturile electronice create cu certificate emise de autorități și instituții publice**   1. **Autoritățile și instituțiile publice care emit certificate pentru semnături electronice vor respecta normele privind identificarea și autentificarea, emise de autoritatea de supraveghere și reglementare în domeniu.**   **----------------------------------------------------**  **M.A.I.**  **Art. 23. Semnăturile electronice create cu certificate emise de autorități și instituții publice**   1. Autoritățile și instituțiile publice care emit certificate **calificate** pentru semnături electronice vor respecta normele privind identificarea și autentificarea, emise de autoritatea de supraveghere și reglementare în domeniu și de către MCID.   **---------------------------------------------**  **Asociatia Furnizorilor de Servicii de Certificare**  **Art. 23. Semnăturile electronice create cu certificate emise de autorități și instituții publice**  (l) Autoritățile și instituțiile publice care emit certificate pentru semnături electronice vor respecta normele privind identificarea și autentificarea, emise de autoritatea de supraveghere și reglementare în domeniu și de către MCID **Autoritățile și instituțiile publice vor putea emite certificate doar daca sunt abilitate de lege pentru acest scop și numai autorităților și instituțiilor publice sau pentru propriile sisteme inchise.**  (2) În cazul în care autoritățile și instituțiile publice care furnizează certificate digitale nu au posibilitatea onorării unei solicitări în vederea furnizării acestora, autoritățile sau instituțiile publice solicitante pot achiziționa servicii de încredere furnizate de prestatori de servicii de încredere privați, cu respectarea dispozițiilor legale aplicabile achizițiilor publice.  Se introduce un nou alineat, respectiv alin. (3) cu următorul cuprins:  (3) **Pentru respectarea principiilor concurenței libere și loiale, furnizarea de catre autoritatile si institutiile publice de certificate digitale pentru semnatura avansata sau calificata catre persoane juridice de drept privat sau catre cetateni se face contra-cost la un pret care sa reflecte corect toate costurile aferente furnizarii de certificate digitale, incluzand, fara a se limita la acestea, costurile cu dezvoltarea sau achizitia si mentenanta produselor software necesare pentru emiterea certificatelor, costul cu achizitia si mentenanta infrastructurii hardware necesare, costurile cu resursele umane necesare pentru operarea infrastructurii, pentru identificare, pentru acordare suport catre cetateni, costurile cu auditurile, precum si orice alte costuri necesare pentru indeplinirea tuturor cerintelor Regulamentului 910 si ale prezentei legi**. | Furnizarea gratuita de certificate pentru cetateni de catre institutiile publice incalca principiile unei piete concurentialale, asa cum este piata serviciilor de incredere, conform prevederilor Regulamentului 910/2014 |
| **Art. 24. Utilizarea semnăturii electronice de către autoritățile și instituțiile publice**   1. Actele emise în format electronic de autoritățile și instituțiile publice sunt semnate cu o **semnătură electronică calificată sau** cu o semnătură electronică **avansată** creată cu un certificat digital emis de o autoritate sau o instituție publică din România. 2. În cadrul procedurilor de elaborare, avizare și prezentare a proiectelor de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, inițiate în vederea adoptării sau aprobării de către Guvern, actele și documentele autorităților și ale instituțiilor publice semnate cu semnătura electronică calificată au forța juridică a înscrisurilor autentice. 3. În aplicarea prevederilor alin. (2), măsurile metodologice, organizatorice, termenele și circulația proiectelor de acte normative se stabilesc prin hotărâre a Guvernului la propunerea Secretariatului General al Guvernului. 4. Serviciul de Telecomunicații Speciale, în calitate de prestator de servicii de încredere calificate acreditat conform Regulamentului (UE) nr. 910/2014, furnizează servicii de încredere calificate, cu titlu gratuit, în scopul îndeplinirii atribuțiilor funcționale, exclusiv personalului autorizat din cadrul autorităților și instituțiilor publice beneficiare, în conformitate cu prevederile Legii nr. 92/1996 privind organizarea și funcționarea Serviciului de Telecomunicații Speciale, cu modificările și completările ulterioare. 5. Organele de stat cu atribuţii în domeniul siguranţei   naţionale furnizează servicii de încredere calificate pentru sistemele închise gestionate de acesta, certificatele calificate emise de aceste organe fiind recunoscute şi folosite pentru nevoi proprii şi un set definit de participanţi în baza acordurilor încheiate, pentru realizarea schimbului de date intern, sau între acesta şi instituţiile din domeniul apărării, ordinii publice şi securităţii naţionale, precum şi pentru semnarea corespondenţei digitale şi realizarea schimbului de corespondenţă digitală.  ------------------------------------------------------------- | **ADR:**  **Art. 24. Utilizarea semnăturii electronice de către autoritățile și instituțiile publice**  **(4)Guvernul poate stabili prin Hotărâre, la propunerea Secretariatului General, prestatorii de servicii de încredere calificați din Lista Sigură, care prestează servicii de încredere calificate pentru administrația publică.**  ------------------ - -----------------------------  **Asociatia Furnizorilor de Servicii de Certificare**  Se introduc trei alineate, respectiv alin. (6), alin. (7) şi alin. (8) la art. 24 cu următorul cuprins:  **(6) Anual, Serviciul de Telecomunicatii Speciale va publica costul pentru un certificat calificat impreuna cu dispozitivul calificat de creare de semnatura calificata furnizate in scopul prevazut la alin. (4).**  **(7) Costul certificatului calificat prevazut la alin (6) il reprezinta raportul dintre toate costurile STS aferente furnizarii de certificate calificate si numarul de certificate emise de STS din respectivul an. Costurile aferente furnizarii de certificate calificate includ, fara a se limita la acestea, costurile cu dezvoltarea sau achizitia si mentenanta produselor software necesare pentru emiterea certificatelor, costul cu achizitia si mentenanta infrastructurii hardware necesare, costurile cu resursele umane necesare pentru operarea infrastructurii, pentru identificare, pentru acordare suport catre cetateni, costurile cu auditurile, precum si orice alte costuri necesare pentru indeplinirea tuturor cerintelor Regulamentului 910 si ale prezentei legi.**  **(8) Institutiile si autoritatile publice mentionate la alin. (4) pot achizitiona certificate digitale calificate de la prestatori calificati de servicii de incredere, daca pretul de achizitie fara TVA este mai mic decat costul publicat de STS.** | Nu se pot desemna prin lege prestatorii de servicii de încredere calificați, întrucât statutul de calificat se acordă de către organismul de supraveghere în baza unui raport de evaluare a conformității. Mai mult decât atât, prestatorii de servicii de încredere pot obține acest statut în urma îndeplinirii condițiilor prevăzute de Regulamentul 910/2014 și standardele ETSI din domeniu. Totodată, conform art. 21 din Regulamentul 910/2014 Prestatorii de servicii de încredere calificați pot începe furnizarea serviciului de încredere calificat după ce statutul de calificat a fost indicat în listele sigure. **Astfel, acordarea statutului de prestator de servicii de încredere calificat prin lege constituie caz de infringement.**  Guvernul poate stabili, prestatorii de servicii de încredere calificați din Lista Sigură (care au fost deja acreditați), care prestează servicii de încredere calificate pentru administrația publică, cu condiția ca pe perioada cât prestează servicii de încredere calificate sa fie acreditați și publicați în Lista Sigură  Furnizarea gratuita de catre STS de certificate calificate pentru institutiile publice reprezinta o limitare a accesului prestorilor privati de servicii de incredere la piata institutiilor publice pentru certificate digitale calificare. Propunerile au scopul de defini un anumit prag valoric de la care institutiile publice pot totusi achizitiona certificate calificate de si de la prestatori privati, in situatii diverse, in care, din motive operationale, utilizarea de certificate calificate de la alti prestatori este o optiune mai buna pentru o institutie publica. |
| **Art. 25 Activitatea și obligațiile autorităților și instituțiilor publice**   1. Autoritățile și instituțiile publice sunt obligate să accepte documente electronice semnate cu o semnătură electronică, aplicată în conformitate cu dispozițiile prezentei legi și ale Regulamentului (UE) 910/2014. 2. În vederea primirii documentelor electronice, autoritățile și instituțiile publice pun la dispoziție portaluri proprii sau utilizează astfel de instrumente puse la dispoziție de către terți. 3. În situația în care primirea unui document electronic nu se poate realiza în conformitate cu dispozițiile alin. (2), autoritățile și instituțiile publice utilizează în acest sens poșta electronică. 4. Documentele emise de către autoritățile și instituțiile publice ca urmare a primirii unor documente în conformitate cu prevederile prezentului articol se comunică în format electronic, cu excepția situației în care există o cerere contrară. 5. Autoritățile și instituțiile publice au obligația să publice în mediul online informații privindmodalitatea de primire a documentelor electronice. 6. Autoritățile și instituțiile publice care oferă servicii publice au obligația de a se integra cu Platforma PSCID (ROeID), sistemul informatic dezvoltat de ADR pentru identificarea electronică a cetățenilor. 7. Persoanele juridice de drept privat au posibilitatea de a-și integra sistemele informatice private cu Platforma PSCID (ROeID), cu aprobarea prealabila a Autorității pentru Digitalizarea României. | **Asociatia Furnizorilor de Servicii de Certificare**  **Art. 25 Activitatea și obligațiile autorităților și instituțiilor publice**  (1) Autoritățile și instituțiile publice sunt obligate să accepte documente electronice semnate cu o semnătură electronică, aplicată în conformitate cu dispozițiile prezentei legi și ale Regulamentului (UE) 910/2014 **si sunt obligate sa accepte cel putin documente electronice semnate cu semnatura electronica calificata**.  (6)Autoritățile și instituțiile publice care oferă servicii publice **pentru semnatura electronica** au obligația de a se integra cu Platforma PSCID (ROeID), sistemul informatic dezvoltat de ADR pentru identificarea electronică a cetătenilor.  **~~(7) Persoanele juridice de drept privat au posibilitatea de a-și integra sistemele informatice private cu Platforma PSCID (ROeID), cu aprobarea prealabila a Autorității pentru Digitalizarea României.~~** | In conformitate cu cerintele articolului 27 din Regulament, in situatia in care o institutie publica accepta o semnatura electronica, alta decat cea calificata, este obligata sa accepte si semnatura electronica calificata.  Precizarea este necesara pentru ca daca serviciile nu sunt pentru semnatura electronica, aliniatul (6) nu are nici o relevanta in contextul acestei propuneri legislative. In plus, nu exista nici un act legislativ care sa reglementeze platforma PSCID (ROeID), ceea ce poate aduce incertitudini la nivelul acestei propuneri legislative.  Aliniatul (7) nu are legatura cu titlul art. 25 care se refera la activitatea și obligațiile autorităților și instituțiilor publice. |
| **Art. 26. Obligațiile titularilor de certificate pentru semnătură electronică**   1. Titularii de certificate calificate sau de certificate pentru semnătura electronică avansată sunt obligați să păstreze datele de autentificare utilizate pentru aplicarea semnăturii electronice calificate, respectiv avansate, în mod securizat și să nu le divulge altor persoane. 2. Titularii de certificate calificate sau de certificate pentru semnătura electronică avansată sunt obligați să solicite în termen de 24 de ore revocarea certificatelor, în următoarele cazuri:   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. | **ADR:**  **Art. 26 bis. Alte servicii de încredere:**  **(1) Serviciile de încredere prevăzute în Regulament respectă atât prevederile prezentei legi, cât și normele emise de către Autoritatea de Reglementare și Supraveghere.**  **(2)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.**  **(3) 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**  **(4) Statutul de prestator de servicii de încredere calificat pentru prestarea serviciilor de încredere de la alin (1) se dobândește în urma parcurgerii procedurii de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat acordat de către organismul de supraveghere.** |  |
| **Art. 28 Contravenții în legătură cu prestarea serviciilor de încredere**  (2) Constituie contravenție, dacă, potrivit legii nu constituie infracțiune și se sancționează cu amendă de la 75.000 lei la 750.000 lei fapta prestatorului de servicii de încredere care:  ....  e) eliberează certificate calificate, respectiv certificate pentru semnătura avansată, fără a verifica identitatea solicitantului în condițiile prezentei legi și a altor reglementări aplicabile;  ...  w)nu respectă obligația prevăzută la art. 12 alin. (8) de a se integra cu Platforma Națională de interoperabilitate reglementată de Legea 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate sau cu altă bază de date are ca obiect evidența populației pentru a valida actele de identitate prezentate de cetățenii români care solicită certificate calificate; | **Asociatia Furnizorilor de Servicii de Certificare**  **Art. 28 Contravenții în legătură cu prestarea serviciilor de încredere**  (2) Constituie contravenție, dacă, potrivit legii nu constituie infracțiune și se sancționează cu amendă de la 75.000 lei la 750.000 lei fapta prestatorului de servicii de încredere care:  ...  e) eliberează certificate calificate, respectiv certificate pentru semnătura avansată, fără a verifica identitatea solicitantului, în condițiile prezentei legi și a altor reglementări aplicabile **sau nu respecta cerintele prezentei legi si a altor reglementari aplicabile la verificarea identitatii semnatarului in situatia semnaturilor avansate care nu se bazează pe un certificat digital, ci folosesc alte tehnologii**;  ...  w)nu respectă obligația prevăzută la art. 12 alin. (8) de a se integra cu Platforma Națională de interoperabilitate reglementată de Legea 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate **~~sau cu altă bază de date are ca obiect evidența populației pentru a valida actele de identitate prezentate de cetățenii români care solicită certificate calificate~~;** | Sanctiunea trebuie aplicata in aceeasi masura si prestatorilor de servicii de incredere ca furnizeaza servicii de semnatura avansata bazate pe alte tehnologii decat cea bazata pe certificate digitale.  Nu exista in cadrul propunerii legislative nici o prevedere cu privire la vreo obligatie de integrare cu „o alta baza de date are ca obiect evidenta populatiei pentru a valida actele de identitate prezentate de cetatenii romani”. In consecinta nu se pot stabili contraventii pentru neindeplinirea unei obligatii care nu este reglementata clar in cadrul propunerii legislative. In plus, articolul 12 alin (8) se refera si la certificatele pentru semnatura avansata, nu doar la certificatele calificate. |
| **Art. 34. Dispoziții tranzitorii**   1. Prezenta lege intră în vigoare în termen de 3 luni de la data publicării ei în Monitorul Oficial al României. 2. Ordinul Ministerului 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 prin ordin comun al Președintelui ADR și al Ministerului Cercetării, Inovării și Digitalizării în termen de 90 de zile de la intrarea în vigoare a legii. 3. În termen de 3 luni de la data publicării prezentei legi în Monitorul Oficial al României, Partea I, ADR desemnează furnizorul unic de bază de timp și propune Guvernului revizuirea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, aprobate prin Hotărârea Guvernului nr. 1259/2001. Noile norme tehnice și metodologice pentru aplicarea legii vor face obiectul unei noi Hotărâri de Guvern. 4. Dispozițiile legale în vigoare care cuprind sintagma *semnătură electronică extinsă* sunt interpretate în sensul utilizării semnăturii electronice avansate. Dispozițiile legale în vigoare care cuprind sintagma *semnătură electronică extinsă bazată pe un certificat calificat* sunt interpretate în sensul utilizării semnăturii electronice calificate. 5. Prevederile legale din alte acte normative referitoare la semnarea unui document electronic de către personalul din administrația publică cu o semnătură electronică calificată sunt considerate a fi îndeplinite și dacă semnarea se face cu o semnătură electronică avansată creată cu un certificat digital emis de către o autoritate sau instituție publică din România. 6. Orice referire din legislația în vigoare la termenul „*furnizor de servicii de certificare”* sunt considerate ca făcând referire la „prestator de servicii de încredere”. 7. Prestatorii de servicii de încredere și prestatorii de servicii de marcare temporală care au dobândit acest statut înainte de intrarea în vigoare a prezentei legi își mențin acest statut. 8. Certificatele emise în conformitate cu cerințele Legii nr. 455/2001, până la data intrării în vigoare a prezentei legi, își păstrează statutul conferit de această lege până la expirarea sau revocarea lor. Mărcile temporale emise în conformitate cu cerințele Legii nr. 451/2004, până la data intrării în vigoare a prezentei legi, sunt considerate mărci temporale electronice în sensul prezentei legi si a Regulamentului (UE) nr.910/2014. 9. În cazul în care acte normative naționale de tipul Ordin, Instrucțiune, Regulament, Circulară, Precizare, Normă, Normă metodologică, Normă tehnică, Îndrumare metodologică, Decizie, Reglementări, Reguli sau orice act normativ cu forță juridică inferioară Ordonanței de Guvern conțin dispoziții contrare prezentei legi, în special în ceea ce privește utilizarea semnăturii electronice potrivit art. 4, emitenții acestor acte le modifică pentru aliniere cu prezenta lege în termen de 3 luni de la intrarea în vigoare a legii. Până la data intrării în vigoare a actelor normative subsecvente, emise în executarea prezentei legi, se aplică prevederile actelor normative în vigoare, în măsura în care nu contravin acesteia. | **ADR:**  **Art. 34. Dispoziții tranzitorii**  **(2)Ordinul Ministerului 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 abrogat în termen de 90 de zile de la intrarea în vigoare a legii.**  Se introduce un nou alineat, respectiv alin. (10) la art.34 cu următorul cuprins:   1. **În termen de 90 de zile de la data publicării în**   **Monitorul Oficial al României, ADR va emite norme privind recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanta utilizând mijloace video.** |  |
| **Art. 35 Abrogarea sau amendarea dispozițiilor legale contradictorii**  (12) La articolul 7 din Legea nr.135/2007 privind arhivarea documentelor în formă electronică,  publicată în Monitorul Oficial al României, Partea I, nr. 138 din 25 februarie 2014, cu modificările și completările ulterioare, alineatul (7), litera (a) se modifică și va avea următorul cuprins:  „a) semnarea documentelor în formă electronică, semnătură electronică calificată sau semnătură electronică avansată aparținând titularului dreptului de dispoziție asupra documentului, denumită în continuare semnătură electronică.  **------------------------------ -----------------------**  **Art. 35** **Abrogarea sau amendarea dispozițiilor legale contradictorii**  (14) La articolul 50 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, publicată în Monitorul Oficial al României, Partea I, nr. 925 din 27 decembrie 2011, aprobată cu modificări şi completări prin Legea nr. 140/2012, cu modificările şi completările ulterioare, alineatul (3), litera b) se modifică şi va avea următorul cuprins:  „b) dacă utilizatorul final este de acord, ca înscris în formă electronică, semnat cu semnătură electronică calificată sau, prin excepţie de la prevederile legale speciale care reglementează semnătura electronică, cu semnătură electronică avansată, în ambele cazuri aplicarea semnăturii electronice îndeplinind condiţiile de validitate ale contractului.” | **ADR:**  **Art. 35 Abrogarea sau amendarea dispozițiilor legale contradictorii**   1. La articolul 7 din Legea nr.135/2007 privind arhivarea documentelor în formă electronică,   publicată în Monitorul Oficial al României, Partea I, nr. 138 din 25 februarie 2014, cu modificările și completările ulterioare, alineatul (7), litera (a) se modifică și va avea următorul cuprins:  „a) **semnarea documentelor în formă electronică, semnătură electronică calificată sau aparținând titularului dreptului de dispoziție asupra documentului, denumită în continuare semnătură electronică.**  ----------------------------------------  **ASOCIAŢIA OPERATORILOR MOBILI DIN ROMÂNIA**  **Art. 35** **Abrogarea sau amendarea dispozițiilor legale contradictorii**  (14) La articolul 50 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, publicată în Monitorul Oficial al României, Partea I, nr. 925 din 27 decembrie 2011, aprobată cu modificări şi completări prin Legea nr. 140/2012, cu modificările şi completările ulterioare, alineatul (3), litera b) se modifică şi va avea următorul cuprins:  „b) dacă utilizatorul final este de acord, ca înscris în formă electronică, semnat cu semnătură electronică calificată sau, prin excepţie de la prevederile legale speciale care reglementează semnătura electronică, cu semnătură electronică avansată, în ambele cazuri aplicarea semnăturii electronice îndeplinind condiţiile de validitate ale contractului.” **Prin excepţie de la orice prevedere contrară, în situaţiile prevăzute de acest paragraf semnătura electronică avansată va fi asimilată unei semnături olografe.”** |  |