Tabel de concordanță

La proiectul de lege privind identificarea electronică și serviciile electronice de încredere

1. Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse Regulamentul (UE) NR. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE					
2. Titlul proiectului de act normativ național Legea privind identificarea electronică și serviciile electronice de încredere					
3. Gradul de compatibilitate Parțial compatibil					
Regulamentul (UE) Nr.910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE	**Legea privind identificarea electronică și serviciile electronice de încredere**	**Gradul de compatibilitate**	**Diferențele**	**Observațiile**	**Autoritatea/ persoana responsabilă**
4	5	6	7	8	9
CAPITOLUL I **DISPOZIȚII GENERALE** **Articolul 1. Obiect.** În vederea asigurării bunei funcționări a pieței interne, vizând în același timp un nivel adecvat de securitate a mijloacelor de identificare electronică și a serviciilor de încredere, prezentul regulament: (a) stabilește condițiile în care statele membre recunosc mijloacele de identificare electronică a persoanelor fizice și juridice care intră sub incidența unui sistem notificat de identificare electronică al unui alt stat membru;		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
(b) stabilește norme pentru serviciile de încredere, în special pentru tranzacțiile electronice; și (c) stabilește un cadru juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unui site internet.	**Articolul 1. Scopul legii și domeniul de aplicare** (1) Prezenta lege are drept scop asigurarea funcționării, la un nivel adecvat, a pieții naționale în domeniul de securitate a mijloacelor de identificare electronică și a serviciilor de încredere și stabilește cadrul juridic pentru semnăturile electronice, sigiliile electronice, mărcile temporale electronice, documentele electronice, serviciile de distribuție electronică înregistrate și serviciile de certificare pentru autentificarea unei pagini web.	**Compatibil**			**Serviciul de Informații și Securitate al Republicii Moldova (SIS al RM)**

	(2) Prezenta lege nu limitează modul de utilizare a documentelor.				
Articolul 2 **Domeniul de aplicare** (1) Prezentul regulament se aplică sistemelor de identificare electronică care au fost notificate de către un stat membru şi prestatorilor de servicii de încredere cu sediul în Uniune. (2) Prezentul regulament nu se aplică prestării de servicii de încredere care sunt utilizate exclusiv în sisteme închise care decurg din dreptul intern sau din acordurile încheiate între un set definit de participanţi. (3) Prezentul regulament nu aduce atingere dreptului intern sau al Uniunii privind încheierea şi valabilitatea contractelor sau a altor obligaţii juridice sau procedurale privind forma.		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE		
Articolul 3 **Definiţii** În sensul prezentului regulament, se aplică următoarele definiţii: 1.„identificare electronică" înseamnă procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;	**Articolul 2. Noţiuni principale** (1) În sensul prezentei legi, următoarele noţiuni semnifică: *identificare electronică* - procesul de utilizare a datelor de identificare a persoanelor în format electronic, reprezentând în mod unic fie o persoană fizică sau juridică, fie o persoană fizică care reprezintă o persoană juridică;	**Compatibil**			**SIS al RM**
2.„mijloace de identificare electronică" înseamnă o unitate materială şi/sau imaterială care conţine date de identificare personală şi care este folosită în scopul autentificării unui serviciu online;	*mijloace de identificare electronică* – unitate materială sau imaterială care conţine date de identificare personală şi care este folosită în scopul autentificării în cadrul unui serviciu online;	**Compatibil**			**SIS al RM**
3.„date de identificare personală" înseamnă un set de date care permit stabilirea identităţii unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;	*date de identificare personală* – set de date care permit stabilirea identităţii unei persoane fizice sau juridice sau a unei persoane fizice care reprezintă o persoană juridică;	**Compatibil**			**SIS al RM**
4.„sistem de identificare electronică" înseamnă un sistem pentru identificarea electronică în care sunt emise mijloace de identificare electronică pentru persoane fizice sau juridice sau persoane fizice reprezentând persoane juridice;	**Articolul 8. Activitatea prestatorului de servicii de încredere** (1) Prestatorul de servicii de încredere: a) creează şi eliberează certificatele cheilor publice; b) suspendă şi revocă certificatele cheilor publice, restabileşte valabilitatea certificatelor cheilor publice	**Compatibil**			**SIS al RM**

	suspendate; c) ţine registrul certificatelor cheilor publice, asigură actualizarea acestuia şi accesul public la registru; d) prestează, în bază de contract servicii de încredere.				
5.„autentificare" înseamnă un proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii şi integrităţii unor date în format electronic;	**Articolul 2. Noţiuni principale** *autentificare* – proces electronic care permite confirmarea identificării electronice a unei persoane fizice sau juridice sau a originii şi integrităţii unor date în format electronic;	**Compatibil**			**SIS al RM**
6.„beneficiar" înseamnă o persoană fizică sau juridică care beneficiază de un serviciu de identificare electronică sau de un serviciu de încredere;	*titularul certificatului cheii publice* – persoana fizică sau juridică sau persoana fizică care reprezintă persoana juridică, care utilizează serviciile de încredere;	**Compatibil**			**SIS al RM**
7.„organism din sectorul public" înseamnă un stat, o autoritate regională sau locală, un organism de drept public sau o asociaţie formată din una sau mai multe astfel de autorităţi sau din unul sau mai multe astfel de organisme de drept public; sau o entitate privată mandatată de cel puţin una dintre aceste autorităţi, organisme sau asociaţii să presteze servicii publice atunci când acţionează în temeiul unui astfel de mandat;		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE. Totodată, noţiunea este parţial definită în Codul administrativ al RM din 19.07.2018 **Articolul 7. Autorităţile publice** Autoritate publică se consideră orice structură organizatorică sau organ instituită/instituit prin lege sau printr-un alt act normativ, care acţionează în regim de putere publică în scopul realizării unui interes public.		
8.„organism de drept public" înseamnă un organism astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE a Parlamentului European şi a Consiliului;	**Legea nr.131/2015 privind achiziţiile publice.** **Articolul 13. Calitatea de autoritate contractantă** 2) Persoană juridică de drept public este orice entitate care întruneşte cumulativ următoarele condiţii: a) este constituită pentru a răspunde exclusiv unor necesităţi de interes general, fără caracter industrial sau comercial;	**Compatibil**			

	b) dispune de personalitate juridică; c) activitatea acesteia este asigurată cu bani publici sau gestiunea acesteia constituie obiectul controlului din partea autorităților publice ori a altor persoane juridice de drept public, sau consiliul ei de administrație, de conducere ori de supraveghere este format, în proporție de peste 50%, din membri numiți de către entitățile menționate.				
9. „semnatar" înseamnă o persoană fizică care creează o semnătură electronică;	**Articolul 2. Noțiuni principale** *semnatar* – persoana fizică sau persoană fizică care reprezintă o persoană juridică, care creează o semnătură electronică;	**Compatibil**			**SIS al RM**
10. „semnătură electronică" înseamnă date în format electronic, atașate la sau asociate logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna;	*semnătură electronică* – date în formă electronică, care sunt atașate la sau logic asociate cu alte date în formă electronică și care sunt utilizate ca metodă de autentificare;	**Compatibil**			**SIS al RM**
11. „semnătură electronică avansată" înseamnă o semnătură electronică ce îndeplinește cerințele prevăzute la articolul 26;	*semnătură electronică avansată* – semnătură electronică ce îndeplinește cerințele stabilite la art. 22;	**Compatibil**			**SIS al RM**
12. „semnătură electronică calificată" înseamnă o semnătură electronică avansată care este creată de un dispozitiv de creare a semnăturilor electronice calificat și care se bazează pe un certificat calificat pentru semnăturile electronice;	*semnătură electronică calificată* – semnătură electronică avansată care este creată prin intermediul unui dispozitiv de creare a semnăturilor electronice calificate și care se bazează pe un certificat calificat pentru semnături electronice.	**Compatibil**			**SIS al RM**
13. „date de creare a semnăturilor electronice" înseamnă date unice care sunt utilizate de semnatar pentru a crea o semnătură electronică;	*date de creare a semnăturilor electronice sau sigiliilor electronice* – date unice care sunt utilizate de semnatar sau de creatorul sigiliului pentru a crea o semnătură electronică sau un sigiliu electronic;	**Compatibil**			**SIS al RM**
14. „certificat pentru semnătura electronică" înseamnă o atestare electronică care face legătura între datele de validare a semnăturii electronice și o persoană fizică și care confirmă cel puțin numele sau pseudonimul persoanei respective;	*certificat pentru semnătură electronică* – atestare electronică care face legătură între datele de validare a semnăturii electronice și o persoană fizică și care confirmă cel puțin numele persoanei respective	**Compatibil**			**SIS al RM**
15. „certificat calificat pentru semnătură electronică" înseamnă un certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa I;	*certificat calificat pentru semnătură electronică* – înseamnă un certificat pentru semnătură electronică care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art. 24;	**Compatibil**			**SIS al RM**
16. „serviciu de încredere" înseamnă un serviciu	*serviciu de încredere* – serviciu electronic, prestat de	**Compatibil**			**SIS al RM**

electronic prestat în mod obişnuit în schimbul unei remuneraţii, care constă în: (a) crearea, verificarea şi validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuţie electronică înregistrată şi a certificatelor aferente serviciilor respective; sau (b) crearea, verificarea şi validarea certificatelor pentru autentificarea unui site internet; sau (c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;	obicei în schimbul unei remuneraţii, care constă în: a) crearea, verificarea şi validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuţie electronică înregistrată şi a certificatelor aferente serviciilor respective; b) crearea, verificarea şi validarea certificatelor pentru autentificarea unei pagini web; c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;				
17. „serviciu de încredere calificat" înseamnă un serviciu de încredere care îndeplineşte cerinţele aplicabile prevăzute de prezentul regulament;	*serviciu de încredere calificat* – reprezintă un serviciu de încredere care îndeplineşte cerinţele aplicabile, prevăzute de prezenta lege;	**Compatibil**			**SIS al RM**
18. „organism de evaluare a conformităţii" înseamnă un organism definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008, care este acreditat în conformitate cu regulamentul în cauză ca fiind competent să efectueze evaluarea conformităţii unui prestator de servicii de încredere calificat şi a serviciilor de încredere calificate pe care acesta le prestează;	*organul de supraveghere şi control* – autoritate publică centrală stabilită de prezenta lege cu atribuţii de supraveghere şi control în domeniul identificării electronice şi serviciilor de încredere;	**Compatibil**			**SIS al RM**
19. „prestator de servicii de încredere" înseamnă o persoană fizică sau juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;	*prestator de servicii de încredere* – întreprinzător individual sau persoană juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau necalificat;	**Compatibil**			**SIS al RM**
20. „prestator de servicii de încredere calificat" înseamnă un prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate şi căruia i se acordă statutul de calificat de către organismul de supraveghere;	*prestator de servicii de încredere calificat* – prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate şi căruia i se acordă statut de calificat de către organul de supraveghere şi control;	**Compatibil**			**SIS al RM**
21. „produs" înseamnă hardware sau software sau componente relevante de hardware sau software, destinate să fie utilizate pentru prestarea de servicii de încredere;	*produs* – hardware şi/sau software ori componente specifice ale acestora, destinate să fie utilizate pentru prestarea serviciilor de încredere;	**Compatibil**			**SIS al RM**
22. „dispozitiv de creare a semnăturilor electronice" înseamnă software sau hardware configurat, utilizat pentru a crea o semnătură electronică;	*dispozitiv de creare a semnăturii electronice sau a sigiliului electronic* – software sau harware configurat, utilizate pentru a crea o semnătură sau un sigiliu electronic;	**Compatibil**			**SIS al RM**
23. „dispozitiv de creare a semnăturilor electronice calificat" înseamnă un dispozitiv de creare a semnăturilor	*dispozitiv de creare a semnăturilor electronice sau sigiliilor electronice calificate* – dispozitiv de creare a	**Compatibil**			**SIS l RM**

electronice care îndeplineşte cerinţele prevăzute în anexa II;	semnăturii electronice sau a sigiliului electronic care îndeplineşte cerinţele prevăzute în art. 26;				
24. „creatorul unui sigiliu" înseamnă o persoană juridică care creează un sigiliu electronic;	*creatorul unui sigiliu* – persoană juridică care creează un sigiliu electronic;	**Compatibil**			**SIS al RM**
25. „sigiliu electronic" înseamnă date în format electronic ataşate la sau asociate logic cu alte date în format electronic pentru asigurarea originii şi integrităţii acestora din urmă;	*sigiliu electronic* - date în format electronic ataşate la sau asociate logic cu alte date în format electronic pentru asigurarea originii şi integrităţii acestora din urmă;	**Compatibil**			**SIS al RM**
26. „sigiliu electronic avansat" înseamnă un sigiliu electronic care îndeplineşte cerinţele prevăzute la articolul 36;	*sigiliu electronic avansat* - sigiliu electronic care îndeplineşte cerinţele prevăzute la art. 22;	**Compatibil**			**SIS al RM**
27. „sigiliu electronic calificat" înseamnă un sigiliu electronic avansat care este creat de un dispozitiv de creare a sigiliilor electronice calificat şi care se bazează pe un certificat calificat pentru sigiliile electronice;	*sigiliu electronic calificat* - sigiliu electronic avansat care este creat prin intermediul dispozitivului de creare a sigiliilor electronice calificat şi care se bazează pe un certificat calificat a sigiliilor electronice;	**Compatibil**			**SIS al RM**
28. „date de creare a sigiliilor electronice" înseamnă date unice care sunt utilizate de creatorul sigiliului electronic pentru a crea un sigiliu electronic;	*date de creare a semnăturilor electronice sau sigiliilor electronice* – date unice care sunt utilizate de semnatar sau de creatorul sigiliului pentru a crea o semnătură electronică sau un sigiliu electronic;	**Compatibil**			**SIS al RM**
29. „certificat pentru sigiliul electronic" înseamnă o atestare electronică care face legătura între datele de validare a sigiliului electronic şi o persoană juridică şi care confirmă numele persoanei respective;	*certificat pentru sigiliu electronic* – atestare electronică care face legătură între datele de validare a sigiliului electronic şi o persoană juridică şi care confirmă numele persoanei respective	**Compatibil**			**SIS al RM**
30. „certificat calificat pentru sigiliul electronic" înseamnă un certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat şi care îndeplineşte cerinţele prevăzute în anexa III;	*certificat calificat pentru sigiliu electronic* – înseamnă un certificat pentru sigiliu electronic care este emis de un prestator de servicii de încredere calificat şi care îndeplineşte cerinţele prevăzute la art. 24;	**Compatibil**			**SIS al RM**
31. „dispozitiv de creare a sigiliului electronic" înseamnă software sau hardware configurat, utilizat pentru a crea un sigiliu electronic;	*dispozitiv de creare a semnăturii electronice sau a sigiliului electronic* – software sau harware configurat, utilizate pentru a crea o semnătură sau un sigiliu electronic;	**Compatibil**			**SIS al RM**
32. „dispozitiv de creare a sigiliului electronic calificat" înseamnă un dispozitiv de creare a sigiliului electronic care îndeplineşte mutatis mutandis cerinţele prevăzute în anexa II;	*dispozitiv de creare a semnăturilor electronice sau sigiliilor electronice calificate* – dispozitiv de creare a semnăturii electronice sau a sigiliului electronic care îndeplineşte cerinţele prevăzute în art. 26;	**Compatibil**			**SIS al RM**
33. „marcă temporală electronică" înseamnă date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind dovezi că acestea din urmă au existat la acel moment;	*marcă temporală electronică* – date în format electronic care leagă alte date în format electronic de un anumit moment, stabilind dovezi că acestea din urmă au existat la acel moment;	**Compatibil**			**SIS al RM**

34. „marcă temporală electronică calificată" înseamnă o marcă temporală electronică care îndeplinește cerințele prevăzute la articolul 42;	*marcă temporală electronică calificată* – reprezintă o marcă temporală electronică care îndeplinește cerințele prevăzute la art. 30;	**Compatibil**			**SIS al RM**
35. „document electronic" înseamnă orice conținut stocat în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;	*document electronic* – orice conținut în format electronic, în special sub formă de text sau de înregistrare sonoră, vizuală sau audiovizuală;	**Compatibil**			**SIS al RM**
36. „serviciu de distribuție electronică înregistrată" înseamnă un serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;	*serviciu de distribuție electronică înregistrată* – reprezintă un serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind transmiterea și recepționarea datelor și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată;	**Compatibil**			**SIS al RM**
37. „serviciu de distribuție electronică înregistrată calificat" înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la articolul 44;	*serviciu de distribuție electronică înregistrată calificat* - înseamnă un serviciu de distribuție electronică înregistrată care îndeplinește cerințele prevăzute la art.32;	**Compatibil**			**SIS al RM**
38. „certificat pentru autentificarea unui site internet" înseamnă o atestare care face posibilă autentificarea unui site internet și face legătura între site-ul internet și persoana fizică sau juridică căreia i s-a emis certificatul;	*certificat pentru autentificarea unei pagini web* - atestare care face posibilă autentificarea unei pagini web și face legătura între pagina web și persoana fizică sau juridică căreia i s-a emis certificatul;	**Compatibil**			**SIS al RM**
39. „certificat calificat pentru autentificarea unui site internet" înseamnă un certificat pentru autentificarea unui site internet care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în anexa IV;	*certificat calificat pentru autentificarea unei pagini web* – certificat pentru autentificarea unei pagini web care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute la art.33;	**Compatibil**			**SIS al RM**
40. „date de validare" înseamnă date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;	*date de validare* – date care sunt utilizate pentru a valida o semnătură electronică sau un sigiliu electronic;	**Compatibil**			**SIS al RM**
41. „validare" înseamnă procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.	*validare* - procesul prin care se verifică și se confirmă dacă o semnătură electronică sau un sigiliu electronic este validă/valid.	**Compatibil**			**SIS al RM**
Articolul 4 **Principiul pieței interne** (1) Nu există nicio restricție privind prestarea de servicii de încredere pe teritoriul unui stat membru de către un prestator de servicii de încredere stabilit în alt stat membru, din motive care se încadrează în domeniile		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

reglementate de prezentul regulament. (2) Produsele şi serviciile de încredere care sunt conforme cu prezentul regulament sunt autorizate pentru a circula liber pe piaţa internă					
Articolul 5 **Prelucrarea şi protecţia datelor** (1) Prelucrarea datelor cu caracter personal se efectuează în conformitate cu Directiva 95/46/CE. (2) Fără a aduce atingere efectului juridic aferent pseudonimelor în temeiul dreptului intern, utilizarea pseudonimelor în cadrul tranzacţiilor electronice nu este interzisă.	**Articolul 51. Protecţia datelor cu caracter personal** (1) Prestatorii de servicii de încredere vor asigura respectarea legislaţiei în domeniul protecţiei datelor cu caracter personal în procesul de prestare a serviciilor de încredere. (2) Datele cu caracter personal se colectează de către prestatorul de servicii de încredere numai în măsura în care acestea sunt necesare pentru eliberarea şi menţinerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimţământul expres al persoanei interesate.	**Compatibil**			**Centrul Naţional pentru Protecţia Datelor cu Caracter Personal**
CAPITOLUL III **IDENTIFICARE ELECTRONICĂ** **Articolul 6** **Recunoaşterea reciprocă** (1) Atunci când este necesară o identificare electronică care utilizează un mijloc de identificare electronică şi o autentificare în temeiul dreptului intern sau al practicii administrative naţionale pentru a accesa un serviciu prestat online de un organism din sectorul public într-un stat membru, mijloacele de identificare electronică emise într-un alt stat membru sunt recunoscute în primul stat membru în scopul autentificării transfrontaliere a respectivului serviciu online, cu condiţia să fie îndeplinite următoarele condiţii: (a) mijloacele de identificare electronică să fie emise în cadrul unui sistem de identificare electronică inclus în lista publicată de Comisie în temeiul articolului 9; (b) nivelul de asigurare al respectivelor mijloace de identificare electronică să corespundă unui nivel de asigurare egal sau mai ridicat decât nivelul de asigurare impus de organismul din sectorul public relevant pentru a accesa respectivul serviciu online în primul stat membru, cu condiţia ca nivelul de asigurare al mijloacelor de identificare electronică respective să corespundă nivelului		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE		

de asigurare substanțial sau ridicat; (c) organismul din sectorul public relevant utilizează nivelul de asigurare „substanțial" sau „ridicat" în legătură cu accesarea online a serviciului respectiv. Această recunoaștere trebuie să aibă loc în termen de cel mult 12 luni de la publicarea de către Comisie a listei menționate la primul paragraf litera (a). (2) Mijloacele de identificare electronică eliberate în temeiul unui sistem de identificare electronică inclus în lista publicată de Comisie în conformitate cu articolul 9 și care corespund nivelului de asigurare scăzut pot fi recunoscute de către organismele din sectorul public în scopul autentificării transfrontaliere pentru serviciul furnizat online de către organismele respective.					
Articolul 7 **Eligibilitatea pentru notificarea sistemelor de identificare electronică** Un sistem de identificare electronică este eligibil pentru notificare în temeiul articolului 9 alineatul (1) în cazul în care sunt îndeplinite toate condițiile de mai jos: (a) mijloacele de identificare electronică din cadrul sistemului de identificare electronică sunt emise: (i) de statul membru care notifică; (ii) pe baza unui mandat din partea statului membru care notifică; sau (iii) independent de statul membru care notifică și sunt recunoscute de respectivul stat membru; (b) mijloacele de identificare electronică din cadrul sistemului de identificare electronică pot fi utilizate pentru a accesa cel puțin un serviciu care este prestat de un organism din sectorul public și care necesită identificarea electronică în statul membru care notifică; (c) sistemul de identificare electronică și mijloacele de identificare electronică emise în temeiul acestuia îndeplinesc cerințele aferente cel puțin unuia dintre nivelurile de asigurare prevăzute în actul de punere în aplicare menționat la articolul 8 alineatul (3); (d) statul membru care notifică se asigură că datele de identificare personală, reprezentând în mod unic persoana		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

în cauză, sunt atribuite, în conformitate cu specificațiile, standardele și procedurile tehnice aferente nivelului de asigurare relevant prevăzut în actul de punere în aplicare menționat la articolul 8 alineatul (3), persoanei fizice sau juridice menționate la articolul 3 punctul 1 la momentul emiterii mijloacelor de identificare electronică din cadrul sistemului respectiv; (e) partea care emite mijloacele de identificare electronică din cadrul respectivului sistem se asigură că mijloacele de identificare electronică sunt atribuite persoanelor menționate la litera (d) de la prezentul articol, în conformitate cu specificațiile tehnice, standardele și procedurile aferente nivelului de asigurare corespunzător prevăzut în actul de punere în aplicare menționat la articolul 8 alineatul (3); (f) statul membru care notifică asigură disponibilitatea autentificării online, astfel încât orice beneficiar stabilit pe teritoriul altui stat membru să poată confirma datele de identificare personală primite în format electronic. În cazul altor beneficiari decât organismele din sectorul public, statul membru care notifică poate defini condițiile de acces la mijlocul respectiv de autentificare. Autentificarea transfrontalieră este furnizată gratuit atunci când este efectuată în legătură cu un serviciu online prestat de un organism din sectorul public. Statele membre nu impun nicio cerință tehnică specifică disproporționată beneficiarilor care intenționează să efectueze o astfel de autentificare, atunci când astfel de cerințe împiedică sau afectează semnificativ interoperabilitatea sistemelor de identificare electronică notificate; (g) cu cel puțin șase luni înaintea notificării în conformitate cu articolul 9 alineatul (1), statul membru care notifică furnizează celorlalte state membre, în scopul îndeplinirii obligației prevăzute la articolul 12 alineatul (5), o descriere a sistemului respectiv în conformitate cu modalitățile prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul (7); (h) sistemul de identificare electronică îndeplinește cerințele prevăzute în actul de punere în aplicare menționat la articolul 12 alineatul (8).					

Articolul 8 **Niveluri de asigurare ale mijloacelor de identificare electronică** (1) Un sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) specifică nivelurile de asigurare scăzut, substanțial și/sau ridicat pentru mijloacele de identificare electronică emise în cadrul sistemului respectiv. (2) Nivelurile de asigurare scăzut, substanțial și ridicat îndeplinesc următoarele criterii, respectiv: (a) nivelul de asigurare scăzut se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității; (b) nivelul de asigurare substanțial se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad substanțial de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a reduce substanțial riscul unei utilizări frauduloase sau al modificării frauduloase a identității; (c) nivelul de asigurare ridicat se referă la un mijloc de identificare electronică în contextul unui sistem de identificare electronică, care asigură un grad mai ridicat de încredere în legătură cu identitatea pretinsă sau declarată a unei persoane decât mijloacele de identificare electronică cu nivel de asigurare substanțial și care este caracterizat prin trimitere la specificațiile tehnice, la standardele și la procedurile corespunzătoare respectivului mijloc de identificare, inclusiv controalele tehnice, al căror scop este de a împiedica utilizarea frauduloasă sau modificarea		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

frauduloasă a identității. (3) Până la 18 septembrie 2015, ținând cont de standardele internaționale relevante și sub rezerva alineatului (2), Comisia, prin intermediul unor acte de punere în aplicare, stabilește specificații tehnice, standarde și proceduri minime, în raport cu care sunt specificate nivelurile de asigurare scăzut, substanțial și ridicat pentru mijloacele de identificare electronică în sensul alineatului (1). Aceste specificații tehnice, standarde și proceduri minime se stabilesc prin trimitere la fiabilitatea și calitatea următoarelor elemente: (a) procedura de dovedire și de verificare a identității persoanelor fizice sau juridice care solicită emiterea mijloacelor de identificare electronică; (b) procedura pentru emiterea mijloacelor de identificare electronică solicitate; (c) mecanismul de autentificare, prin care persoana fizică sau juridică utilizează mijloacele de identificare electronică pentru a confirma identitatea sa unui beneficiar; (d) entitatea care emite mijloacele de identificare electronică; (e) oricare alt organism implicat în solicitarea emiterii mijloacelor de identificare electronică; și (f) specificațiile tehnice și de securitate ale mijloacelor de identificare electronică emise. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
Articolul 9 **Notificarea** (1) Statul membru care notifică înaintează Comisiei următoarele informații și, fără întârzieri nejustificate, orice modificări ulterioare ale acestora: (a) o descriere a sistemului de identificare electronică notificat, incluzând nivelurile sale de asigurare și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului; (b) regimul de supraveghere aplicabil și informații privind		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

regimul de răspundere referitor la următoarele aspecte: (i) partea care emite mijloacele de identificare electronică; și (ii) partea care desfășoară procedura de autentificare; (c) autoritatea sau autoritățile responsabile pentru sistemul de identificare electronică; (d) informații privind entitatea sau entitățile care gestionează înregistrarea datelor unice de identificare personală; (e) o descriere a modului în care sunt îndeplinite cerințele prevăzute în actele de punere în aplicare menționate la articolul 12 alineatul(8); (f) o descriere a autentificării menționate la articolul 7 litera (f); (g) dispoziții pentru suspendarea sau revocarea sistemului de identificare electronică notificat, a autentificării sau a părților compromise în cauză. (2) La un an de la data aplicării actelor de punere în aplicare menționate la articolul 8 alineatul (3) și la articolul 12 alineatul (8), Comisia publică în Jurnalul Oficial al Uniunii Europene o listă a sistemelor de identificare electronică care au fost notificate în temeiul alineatului (1) de la prezentul articol și informațiile de bază cu privire la acestea. (3) În cazul în care Comisia primește o notificare după expirarea perioadei menționate la alineatul (2), aceasta publică în Jurnalul Oficial al Uniunii Europene modificările la lista menționată la alineatul (2) în termen de două luni de la data primirii respectivei notificări. (4) Un stat membru poate înainta Comisiei o cerere de eliminare a unui sistem de identificare electronică notificat de respectivul stat membru din lista menționată la alineatul (2). Comisia publică în Jurnalul Oficial al Uniunii Europene modificările corespunzătoare aduse listei, în termen de o lună de la primirea cererii statului membru. (5) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească circumstanțele, formatele și procedurile pentru notificările în temeiul alineatului (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la					

articolul 48 alineatul (2).					
Articolul 10 **Încălcarea securității** (1) În cazul în care fie sistemul de identificare electronică notificat în conformitate cu articolul 9 alineatul (1), fie autentificarea menționată la articolul 7 litera (f) este încălcată sau parțial compromisă într-un mod care afectează fiabilitatea autentificării transfrontaliere a sistemului respectiv, statul membru care notifică suspendă sau revocă, fără întârziere, respectiva autentificare transfrontalieră sau părțile compromise în cauză și informează celelalte state membre și Comisia. (2) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) este remediată, statul membru care notifică reinstituie autentificarea transfrontalieră și informează celelalte state membre și Comisia fără întârzieri nejustificate. (3) În cazul în care încălcarea sau compromiterea menționată la alineatul (1) nu este remediată în termen de trei luni de la suspendare sau revocare, statul membru care notifică comunică celorlalte state membre și Comisiei retragerea sistemului de identificare electronică. Comisia publică în Jurnalul Oficial al Uniunii Europene, fără întârzieri nejustificate, modificările corespunzătoare aduse listei menționate la articolul 9 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 11 **Răspunderea** (1) Statul membru care notifică este răspunzător pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligațiilor care îi revin în temeiul articolului 7 literele (d) și (f). (2) Partea care emite mijloacele de identificare electronică este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere ca urmare a nerespectării obligației menționate la articolul 7 litera (e).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

(3) Partea care execută procedura de autentificare este răspunzătoare pentru prejudiciul cauzat în mod intenționat sau din neglijență oricărei persoane fizice sau juridice în cadrul unei tranzacții transfrontaliere pentru neasigurarea executării corecte a autentificării menționate la articolul 7 litera (f). (4) Alineatele (1), (2) și (3) se aplică în conformitate cu normele de drept intern privind răspunderea. (5) Alineatele (1), (2) și (3) nu aduc atingere răspunderii care revine, în conformitate cu dreptul intern, părților la o tranzacție în care sunt utilizate mijloace de identificare electronică care intră sub incidența sistemului de identificare electronică notificat în temeiul articolului 9 alineatul (1).					
Articolul 12 **Cooperarea și interoperabilitatea** (1) Sistemele naționale de identificare electronică notificate în temeiul articolului 9 alineatul (1) sunt interoperabile. (2) În sensul alineatului (1), se stabilește un cadru de interoperabilitate. (3) Cadrul de interoperabilitate îndeplinește următoarele criterii: (a) urmărește să fie neutru din punctul de vedere al tehnologiei și nu acordă prioritate niciuneia dintre soluțiile tehnice naționale specifice pentru identificarea electronică pe teritoriul statului membru; (b) respectă standardele europene și internaționale, atunci când este posibil; (c) facilitează punerea în aplicare a principiului luării în considerare a vieții private începând cu momentul conceperii (privacy by design); și (d) garantează că datele cu caracter personal sunt prelucrate în conformitate cu Directiva 95/46/CE. (4) Cadru de interoperabilitate este alcătuit din următoarele elemente: (a) o trimitere la cerințele tehnice minime aferente nivelurilor de asigurare menționate la articolul 8; (b) o clasificare a nivelurilor naționale de asigurare aferente sistemelor de identificare electronică notificate în		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

funcție de nivelurile de asigurare menționate la articolul 8; (c) o trimitere la cerințele tehnice minime referitoare la interoperabilitate; (d) o trimitere la un set minim de date de identificare personală, reprezentând în mod unic o persoană fizică sau juridică, care sunt disponibile din sistemele de identificare electronică; (e) regulamentul de procedură; (f) dispoziții referitoare la soluționarea litigiilor; și (g) standarde de securitate operaționale comune. (5) Statele membre cooperează cu privire la următoarele aspecte: (a) interoperabilitatea sistemelor de identificare electronică notificate în conformitate cu articolul 9 alineatul (1) și a sistemelor de identificare electronică pe care statele membre intenționează să le notifice; și (b) securitatea sistemelor de identificare electronică. (6) Cooperarea dintre statele membre constă în: (a) schimbul de informații, de experiență și de bune practici privind sistemele de identificare electronică și, în special, cerințele tehnice referitoare la interoperabilitate și la nivelurile de asigurare; (b) schimbul de informații, de experiență și de bune practici cu privire la modul de lucru cu nivelurile de asigurare ale sistemelor de identificare electronică menționate la articolul 8; (c) evaluarea inter pares privind sistemele de identificare electronică care fac obiectul prezentului regulament; și (d) analiza evoluțiilor relevante din domeniul identificării electronice. (7) Până la 18 martie 2015, Comisia stabilește, prin intermediul actelor de punere în aplicare, modalitățile procedurale necesare pentru a facilita cooperarea între statele membre menționate la alineatele (5) și (6), în vederea stimulării unui nivel ridicat de încredere și securitate corespunzător gradului de risc. (8) Până la 18 septembrie 2015, în vederea stabilirii de condiții uniforme pentru punerea în aplicare a cerinței menționate la alineatul (1), sub rezerva criteriilor stabilite la alineatul (3) și luând în considerare rezultatele					

cooperării dintre statele membre, Comisia adoptă acte de punere în aplicare privind cadrul de interoperabilitate, astfel cum este prevăzut la alineatul (4). (9) Actele de punere în aplicare menționate la alineatele (7) și (8) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
CAPITOLUL III **SERVICII DE ÎNCREDERE** **SECȚIUNEA 1** **Dispoziții generale** **Articolul 13** **Răspunderea și sarcina probei** (1) Fără a aduce atingere alineatului (2), prestatorii de servicii de încredere sunt răspunzători pentru prejudiciile cauzate în mod intenționat sau din neglijență oricărei persoane fizice sau juridice ca urmare a nerespectării obligațiilor prevăzute în prezentul regulament. Sarcina de a proba intenția sau neglijența unui prestator de servicii de încredere necalificat revine persoanei fizice sau juridice care introduce o acțiune în despăgubiri pentru prejudiciul menționat la primul paragraf. Prezumția de intenție sau de neglijență se aplică unui prestator de servicii de încredere calificat, cu excepția cazului în care acesta dovedește că prejudiciul menționat la primul paragraf nu a intervenit din intenția sau din neglijența prestatorului de servicii de încredere calificat. (2) În cazul în care prestatorii de servicii de încredere își informează clienții în prealabil în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care aceștia le prestează și în cazul în care aceste restricții pot fi recunoscute de părțile terțe, prestatorii de servicii de încredere nu sunt răspunzători pentru prejudiciile rezultate din utilizarea serviciilor care depășesc restricțiile indicate. (3) Alineatele (1) și (2) se aplică în conformitate cu normele de drept intern privind răspunderea.	**Articolul 53. Răspunderea și sarcina probei** (1) Prestatorul de servicii de încredere poartă răspundere civilă pentru prejudiciul cauzat urmare a neîndeplinirii obligațiilor prevăzute de prezenta lege, cu excepția cazurilor în care prestatorul de servicii de încredere aduce probe pertinente că nu a putut împiedica cauzarea prejudiciului. (2) Sarcina de a proba intenția sau neglijența unui prestator de servicii de încredere necalificat revine persoanei fizice sau juridice care pretinde despăgubiri pentru prejudiciul cauzat. (3) Intenția sau neglijența prestatorului de servicii de încredere calificat se prezumă, până la proba contrară. (4) Prestatorii de servicii de încredere nu poartă răspundere pentru prejudiciile rezultate din utilizarea serviciilor care depășesc restricțiile stabilite, în cazul în care prestatorii informează clienții în prealabil în mod corespunzător cu privire la restricțiile privind utilizarea serviciilor pe care aceștia le prestează.	**Compatibil**			**SIS al RM**
Articolul 14 **Aspecte internaționale** (1) Serviciile de încredere prestate de prestatori de servicii	**Articolul 3. Recunoașterea reciprocă** (1) Recunoașterea serviciilor de încredere în afara Republicii Moldova este reglementată de tratatele	**Parțial compatibil**	Transpunerea integrală este condiționată de aderarea RM la UE		**SIS al RM**

de încredere stabiliți într-o țară terță sunt recunoscute ca fiind echivalente din punct de vedere juridic cu serviciile electronice de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune dacă serviciile de încredere care provin din țara terță sunt recunoscute în temeiul unui acord încheiat între Uniune și țara terță în cauză sau o organizație internațională în conformitate cu articolul 218 din TFUE. (2) Acordurile menționate la alineatul (1) garantează, în special, că: (a) cerințele aplicabile prestatorilor de servicii de încredere calificați stabiliți în Uniune și serviciilor de încredere calificate pe care aceștia le prestează sunt îndeplinite de prestatorii de servicii de încredere din țara terță sau de organizațiile internaționale cu care a fost încheiat acordul, precum și de serviciile de încredere pe care aceștia le prestează; (b) serviciile de încredere calificate prestate de prestatori de servicii de încredere calificați stabiliți în Uniune sunt recunoscute ca echivalente din punct de vedere juridic cu serviciile de încredere prestate de prestatorii de servicii de încredere din țara terță sau de organizația internațională cu care a fost încheiat acordul.	internaţionale la care Republica Moldova este parte. În cazul în care tratatele internaţionale la care Republica Moldova este parte stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaţionale. (2) Certificatul cheii publice eliberat de către un prestator de servicii de încredere cu domiciliul sau cu sediul într-un alt stat este recunoscut ca fiind echivalent, din punctul de vedere al efectelor juridice, cu certificatul cheii publice eliberat de un prestator de servicii de încredere cu domiciliul sau cu sediul în Republica Moldova dacă este întrunită una dintre următoarele condiţii: a) prestatorul de servicii de încredere cu domiciliul sau cu sediul în alt stat a fost acreditat în cadrul regimului de acreditare în conformitate cu prevederile prezentei legi; b) un prestator de servicii de încredere calificat cu domiciliul sau cu sediul în Republica Moldova garantează recunoaşterea certificatului; c) certificatul sau prestatorul de servicii de încredere care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între Republica Moldova şi alte state sau organizaţii internaţionale, pe bază de reciprocitate. (3) Serviciile de încredere şi documentul electronic nu pot fi considerate lipsite de putere juridică doar în baza faptului că certificatul cheii publice a fost eliberat în corespundere cu normele unui stat străin , dacă acesta a fost recunoscut în condiţiile specificate la alin. (2).				
Articolul 15 **Accesibilitatea pentru persoanele cu handicap** Dacă este posibil, serviciile de încredere prestate şi produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu handicap.	**Articolul 4. Accesibilitatea pentru persoanele cu dizabilităţi** Dacă este posibil, serviciile de încredere prestate şi produsele destinate utilizatorului final utilizate pentru prestarea serviciilor respective sunt accesibile persoanelor cu dizabilităţi.	**Compatibil**	Totodată, Legea nr.60/2012 privind incluziunea socială a persoanelor cu dizabilităţi conţine norme similare. **Articolul 17.** **Politica de stat în domeniul accesibilităţii**		**Ministerul Sănătăţii, Muncii şi Protecţiei Sociale, Ministerul Economiei şi Infrastructu**

			(1) În scopul asigurării unei vieţi independente persoanelor cu dizabilităţi, autorităţile publice centrale şi locale, organizaţiile nonguvernamentale, agenţii economici, indiferent de forma de organizare juridică, în funcţie de competenţele lor funcţionale, evaluează situaţia în domeniu şi întreprind măsuri concrete pentru a facilita accesul persoanelor cu dizabilităţi, în condiţii de egalitate cu ceilalţi, la mediul fizic, la transport, la informaţie şi la mijloacele de comunicare, inclusiv la tehnologia informaţiei şi la comunicaţiile electronice, la alte utilităţi şi servicii deschise sau furnizate publicului, atît în localităţile urbane, cât şi în localităţile rurale, în conformitate cu normativele în vigoare. (2) Identificarea şi eliminarea obstacolelor/ barierelor faţă de accesul deplin al persoanelor cu dizabilităţi trebuie aplicate în special la clădiri, drumuri, mijloace		**rii, SIS al RM**

			de transport şi alte utilităţi interioare şi exterioare, inclusiv şcoli, case, instituţii publice şi locuri de muncă, la serviciile de informare şi comunicare, inclusiv serviciile electronice şi de urgenţă, de asemenea la alte utilităţi şi servicii publice.		
Articolul 16 **Sancţiuni** Statele membre stabilesc normele referitoare la sancţiunile aplicabile în cazul încălcării prezentului regulament. Sancţiunile prevăzute sunt eficace, proporţionale şi disuasive.	**Articolul 52. Răspunderea persoanelor fizice şi juridice care cad sub incidenţa prezentei legi** (1) Persoanele fizice şi juridice poartă răspundere, conform legislaţiei, pentru neîndeplinirea prevederilor prezentei legi. (2) Intermediarul în circulaţia electronică a documentelor poartă răspundere, conform legislaţiei, pentru neîndeplinirea sau îndeplinirea defectuoasă a obligaţiilor prevăzute de prezenta lege, pentru calitatea necorespunzătoare a serviciilor prestate, precum şi pentru prejudiciul cauzat de aceste acţiuni şi/sau inacţiuni. (3) Litigiile apărute în cadrul circulaţiei electronice a documentelor, precum şi cele legate de utilizarea documentelor electronice şi a serviciilor de încredere se soluţionează de către subiecţii circulaţiei electronice a documentelor în conformitate cu legislaţia şi contractele încheiate. **Articolul 54. Răspunderea titularului certificatului cheii publice** (1) Titularul certificatului cheii publice poartă răspundere civilă pentru prejudiciul cauzat de: a) neîndeplinirea sau îndeplinirea defectuoasă a obligaţiilor prevăzute de prezenta lege; b) utilizarea serviciilor de încredere, inclusiv în perioada de la solicitarea suspendării valabilităţii sau revocării certificatului cheii publice până la înscrierea, în termenul stabilit, a menţiunii respective în registrul	**Compatibil**			**SIS al RM**

	certificatelor cheilor publice, cu excepția cazurilor în care titularul certificatului va aduce probe pertinente că documentul electronic a fost semnat de o altă persoană.				
SECȚIUNEA 2 **Supravegherea** **Articolul 17** **Organismul de supraveghere** (1) Statele membre desemnează un organism de supraveghere stabilit pe teritoriul lor sau, de comun acord cu un alt stat membru, un organism de supraveghere stabilit în acel stat membru. Organismul respectiv este responsabil de sarcinile de supraveghere în statul membru care l-a desemnat. Organismelor de supraveghere li se conferă competențele necesare și resursele adecvate pentru exercitarea sarcinilor lor.	**Articolul 34. Organul de supraveghere și control** (1) Organ de supraveghere și control este Serviciul de Informații și Securitate al Republicii Moldova;	**Compatibil**			**SIS al RM**
(2) Statele membre notifică Comisiei denumirile și adresele organismelor lor de supraveghere desemnate.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
(3) Rolul organismului de supraveghere constă în: (a) supravegherea prestatorilor de servicii de încredere calificați stabiliți pe teritoriul statului membru care l-a desemnat pentru a se asigura, prin intermediul activităților de supraveghere ex ante și ex post, că respectivii prestatori de servicii de încredere calificați, precum și serviciile de încredere calificate pe care le prestează, îndeplinesc cerințele stabilite în prezentul regulament; (b) luarea de măsuri, după caz, în legătură cu prestatorii de servicii de încredere necalificați stabiliți pe teritoriul statului membru care l-a desemnat, prin intermediul activităților de supraveghere ex post, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere calificați sau serviciile de încredere pe care le prestează nu îndeplinesc cerințele stabilite în prezentul regulament. (4) În sensul alineatului (3) și sub rezerva restricțiilor prevăzute de acesta, sarcinile organismului de supraveghere includ, în special: (a) să coopereze cu alte organisme de supraveghere și să acorde asistență acestora, în conformitate cu articolul 18;	(2) Organul de supraveghere și control are următoarele atribuții: a) este responsabil de elaborarea și promovarea politicii de stat și de exercitarea controlului în domeniul serviciilor de încredere; b) efectuează acreditarea prestatorilor de servicii de încredere și retrage statutul respectiv; c) exercită funcția prestatorului de servicii de încredere calificat de nivel superior pentru prestatorii de servicii de încredere calificați; d) asigură ținerea, actualizarea și accesul public la datele Registrului de evidență a prestatorilor de servicii de încredere; e) menține și publică, în mod securizat, liste sigure, asupra cărora este aplicată semnătura electronică sau sigiliul electronic al organului de supraveghere și control, care includ informații referitoare la prestatorii de servicii de încredere calificați și informații referitoare la serviciile de încredere calificate prestate de aceștia, într-o formă pasibilă de prelucrare automată;	**Parțial compatibil**	Transpunerea integrală este condiționată de aderarea RM la UE		**SIS al RM**

(b) să efectueze analiza rapoartelor de evaluare a conformității menționate la articolul 20 alineatul (1) și la articolul 21 alineatul (1); (c) să informeze celelalte organisme de supraveghere și publicul cu privire la încălcarea securității sau la pierderea integrității, în conformitate cu articolul 19 alineatul (2); (d) să raporteze Comisiei cu privire la activitățile sale principale, în conformitate cu alineatul (6) de la prezentul articol; (e) să realizeze audituri sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității prestatorilor de servicii de încredere calificați, în conformitate cu articolul 20 alineatul (2); (f) să coopereze cu autoritățile de protecție a datelor, în special prin informarea acestora, fără întârzieri nejustificate, cu privire la rezultatele auditurilor prestatorilor de servicii de încredere calificați, în cazul în care se presupune că normele de protecție a datelor cu caracter personal au fost încălcate; (g) să acorde statutul de calificat prestatorilor de servicii de încredere, precum și serviciilor pe care aceștia le prestează și să retragă statutul respectiv, în conformitate cu articolele 20 și 21; (h) să informeze organismul responsabil cu lista sigură națională menționată la articolul 22 alineatul (3) cu privire la deciziile sale de acordare sau de retragere a statutului de calificat, cu excepția cazului în care respectivul organism este și organism de supraveghere; (i) să verifice existența și aplicarea corectă a dispozițiilor privind planurile de încetare a serviciului în cazurile în care prestatorul de servicii de încredere calificat își încetează activitățile, inclusiv modul în care informațiile sunt păstrate accesibile, în conformitate cu articolul 24 alineatul (2) litera (h); (j) să solicite prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute în prezentul regulament.	f) elaborează și aprobă, prin acte normative, cerințele în domeniul serviciilor de încredere; g) monitorizează și controlează respectarea cerințelor la prestarea serviciilor de încredere; h) participă la elaborarea și aprobarea reglementărilor tehnice și a standardelor în domeniul serviciilor de încredere; i) acordă, la solicitare, asistență metodică și practică la utilizarea serviciilor de încredere; j) supraveghează prestatoriii de servicii de încredere calificați privind calitatea și securitatea serviciilor de încredere calificate pe care le prestează precum și îndeplinirea cerințelor stabilite în prezenta lege; k) aplică măsuri, după caz, în legătură cu prestatorii de servicii de încredere, atunci când este informat că există presupunerea că respectivii prestatori de servicii de încredere pe care le prestează nu îndeplinesc cerințele stabilite în prezenta lege; l) cooperează cu autoritatea națională pentru protecția datelor cu caracter personal, în special prin informarea acesteia, fără întârzieri nejustificate, cu privire la rezultatele controalelor prestatorilor de servicii de încredere calificați, în cazul în care se presupune că normele de protecție a datelor cu caracter personal au fost încălcate; m) solicită prestatorilor de servicii de încredere să remedieze orice neîndeplinire a cerințelor prevăzute în prezenta lege;				
(5) Statele membre pot să solicite organismului de supraveghere să stabilească, să mențină și să actualizeze o		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea		

infrastructură de asigurare a încrederii în conformitate cu condițiile stabilite de dreptul intern. (6) În fiecare an, până la 31 martie, fiecare organism de supraveghere înaintează Comisiei un raport privind principalele activități desfășurate în anul calendaristic anterior, însoțit de un rezumat al notificărilor încălcărilor primit de la prestatorii de servicii de încredere, în conformitate cu articolul 19 alineatul (2). (7) Comisia pune la dispoziția statelor membre raportul anual menționat la alineatul (6). (8) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile pentru raportul menționat la alineatul (6). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).			RM la UE		
Articolul 18 **Asistență reciprocă** (1) Organismele de supraveghere cooperează cu scopul de a face schimb de bune practici. Pe baza unei solicitări justificate din partea unui alt organism de supraveghere, un organism de supraveghere acordă respectivului organism asistență astfel încât activitățile organismelor de supraveghere să poată fi desfășurate în mod coerent. Asistența reciprocă poate viza, în special, solicitările de informații și măsurile de supraveghere, cum ar fi solicitările de a desfășura inspecții legate de rapoartele de evaluare a conformității menționate la articolele 20 și 21. (2) Un organism de supraveghere căruia i se adresează o solicitare de asistență poate respinge respectiva solicitare din oricare dintre următoarele motive: (a) organismul de supraveghere nu are competența de a acorda asistența solicitată; (b) asistența solicitată nu este proporțională cu activitățile de supraveghere ale organismului de supraveghere desfășurate în conformitate cu articolul 17; (c) acordarea asistenței solicitate ar contraveni prezentului regulament. (3) După caz, statele membre pot autoriza organismele lor de supraveghere să efectueze anchete comune în care este implicat personalul din organismele de supraveghere ale		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

celorlalte state membre. Mecanismele și procedurile pentru astfel de acțiuni în comun sunt convenite și stabilite de către statele membre în cauză, în conformitate cu dreptul lor intern.					
Articolul 19 **Cerințe de securitate aplicabile prestatorilor de servicii de încredere** (1) Prestatorii de servicii de încredere calificați și necalificați iau măsurile tehnice și organizaționale corespunzătoare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează. Ținând cont de cele mai recente evoluții tehnologice, aceste măsuri garantează că nivelul securității este proporțional cu gradul de risc. În special, se iau măsuri pentru a preveni și minimiza impactul incidentelor legate de securitate și pentru a informa părțile interesate cu privire la efectele negative ale oricăror incidente de acest tip. (2) Prestatorii de servicii de încredere calificați și necalificați notifică, fără întârzieri nejustificate, însă, în orice caz, în termen de 24 de ore după ce au aflat, organismului de supraveghere competent și, dacă este cazul, altor organisme relevante, cum sunt organismul național competent pentru securitatea informațiilor sau autoritatea pentru protecția datelor, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. Atunci când încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice încălcarea securității sau pierderea integrității fără întârzieri nejustificate. După caz, în special dacă o încălcare a securității sau o pierdere a integrității se referă la două sau mai multe state membre, organismul de supraveghere notificat informează organismele de supraveghere vizate din alte state membre și ENISA.	**Articolul 38. Cerințe de securitate aplicabile prestatorilor de servicii de încredere** (1) Prestatorii de servicii de încredere calificați și necalificați aplică măsurile tehnice și organizaționale corespunzătoare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează. (2) Prestatorii de servicii de încredere calificați și necalificați notifică organului de supraveghere și control imediat, dar nu mai târziu de 24 de ore de la momentul constatării, orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de acesta. În cazul în care încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică, de asemenea, persoanei fizice sau juridice în cauză încălcarea securității sau pierderea integrității fără întârzieri nejustificate. (3) Organul de supraveghere și control notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării securității sau pierderea integrității servește interesului public.	**Compatibil**			**SIS al RM**

Organismul de supraveghere notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării securității sau pierderea integrității servește interesului public.					
(3) Organismul de supraveghere furnizează ENISA, o dată pe an, un rezumat al notificărilor privind încălcarea securității sau pierderea integrității primite de la prestatorii de servicii de încredere. (4) Prin intermediul unor acte de punere în aplicare, Comisia poate: (a) elabora specificații suplimentare referitoare la măsurile menționate la alineatul (1); și (b) defini formatele și procedurile, inclusiv termenele, aplicabile în sensul alineatului (2). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		**SIS al RM**
SECȚIUNEA 3 **Servicii de încredere calificate** **Articolul 20** **Supravegherea prestatorilor de servicii de încredere calificați** (1) Prestatorii de servicii de încredere calificați sunt auditați, pe propria cheltuială, cel puțin o dată la 24 de luni, de către un organism de evaluare a conformității. Scopul auditului este de a confirma că prestatorii de servicii de încredere calificați și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele prevăzute în prezentul regulament. Prestatorii de servicii de încredere calificați transmit raportul de evaluare a conformității care a rezultat organismului de supraveghere în termen de trei zile lucrătoare de la primirea lui. (2) Fără a aduce atingere alineatului (1), organismul de supraveghere poate, în orice moment, să efectueze un audit sau să solicite unui organism de evaluare a conformității să efectueze o evaluare a conformității privind prestatorii de servicii de încredere calificați, pe cheltuiala prestatorilor de servicii de încredere respectivi, pentru a confirma că aceștia și serviciile de încredere calificate pe care le prestează îndeplinesc cerințele	**Articolul 35. Controlul în domeniul serviciilor de încredere** (1) Controlul privind respectarea cerinţelor stabilite de prezenta lege la prestarea serviciilor de încredere şi la acordarea sau prelungirea acreditării este efectuat de către organul de supraveghere şi control. (2) Controlul se efectuează de către comisia de control în domeniul serviciilor de încredere (în continuare – Comisia) în baza regulamentului aprobat de organul de supraveghere şi control. (3) Comisia se creează în cadrul organului de supraveghere şi control în baza ordinului privind efectuarea controlului, emis de conducătorul acestui organ. (4) Componenţa nominală a Comisiei se stabileşte pentru fiecare caz în parte. (5) Comisia are dreptul: a) să beneficieze de acces liber la materialele documentare, pe suport de hârtie şi în format electronic, necesare pentru desfăşurarea lucrărilor ce ţin de prestarea serviciilor de încredere, precum şi la sistemele de distribuţie de aplicaţii soft, la aplicaţiile soft şi mijloacele hardware instalate;	**Compatibil**			**SIS al RM**

prevăzute în prezentul regulament. În cazul în care normele de protecție a datelor cu caracter personal par să fi fost încălcate, organismul de supraveghere informează autoritățile pentru protecția datelor cu privire la rezultatele auditurilor sale. (3) În cazul în care organismul de supraveghere solicită prestatorului de servicii de încredere calificat să remedieze neîndeplinirea obligațiilor care îi revin în temeiul prezentului regulament, iar respectivul prestator nu acționează în consecință și, după caz, într-un termen stabilit de organismul de supraveghere, organismul de supraveghere, ținând seama în special de amploarea, de durata și de consecințele respectivei neîndepliniri, poate retrage statutul de calificat al respectivului prestator sau al serviciului prestat de acesta care este afectat și informează organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1). Organismul de supraveghere informează prestatorul de servicii de încredere calificat cu privire la retragerea statutului de calificat, al său sau al serviciului în cauză.	b) să obțină informații complete despre condițiile și modul de exploatare a mijloacelor hardware și software; c) să obțină de la persoanele responsabile și de la personalul prestatorului de servicii de încredere informațiile privind prestarea serviciilor de încredere ce țin de obiectul controlului; d) să beneficieze de acces, în decursul zilei lucrătoare (în perioada efectuării controlului), în încăperile prestatorului de servicii de încredere. (6) Comisia nu are dreptul să efectueze controlul fără prezentarea ordinului privind efectuarea controlului și fără prezentarea actelor de identitate ale membrilor Comisiei. (7) La efectuarea controlului privind respectarea condițiilor prevăzute de prezenta lege, Comisia va ține cont de următoarele reguli: a) legalitatea și respectarea competenței stabilite de lege; b) neadmiterea aplicării sancțiunilor care nu sunt stabilite de lege; c) tratarea dubiilor, apărute la aplicarea legislației, în favoarea prestatorului de servicii de încredere; d) efectuarea controlului pe cheltuiala statului; e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului; f) dreptul prestatorului de servicii de încredere de a contesta acțiunile organului de supraveghere și control, inclusiv în instanța judecătorească. (8) Controalele planificate privind respectarea de către prestatorul de servicii de încredere calificați a obligațiilor prevăzute de prezenta lege se efectuează de către organul de supraveghere și control cel mult o dată în decursul anului calendaristic, cu cooptarea, după caz, a reprezentanților instituțiilor cu funcții de reglementare și de control, conform competenței. (9) Planurile controalelor, elaborate de organul de supraveghere și control și aprobate în modul stabilit, se coordonează, în privința termenelor de efectuare, cu conducerea prestatorului de servicii de încredere, cu cel				

	puţin 5 zile lucrătoare înainte de începerea acestor controale. (10) Controalele inopinate se efectuează la decizia organului de supraveghere şi control, numai în temeiul: a) depistării şi confirmării, de către organul supraveghere şi control, a faptelor de încălcare a prezentei legi; şi/sau b) recepţionării cererilor şi reclamaţiilor argumentate adresate în formă scrisă organului supraveghere şi control referitoare la încălcările sau la îndeplinirea necorespunzătoare a obligaţiilor prevăzute de prezenta lege de către prestatorul de servicii de încredere. (11) Prestatorul de servicii de încredere este informat despre efectuarea controlului inopinat în ziua demarării controlului. (12) Controalele repetate se efectuează numai în scopul verificării executării prescripţiei privind lichidarea încălcărilor prezentei legi, indicate în actul de control precedent (planificat sau inopinat). Controlul repetat se consideră parte componentă a controlului precedent. (13) Controlul se efectuează strict în termenele stabilite în ordinul privind efectuarea controlului. (14) Termenul de efectuare a controlului planificat şi a controlului inopinat nu poate depăşi 10 zile lucrătoare, iar a celui repetat – 5 zile lucrătoare. În cazul controalelor inopinate, termenul de 10 zile poate fi prelungit cu încă 10 zile de către conducătorul organului supraveghere şi control în baza unei decizii motivate, adusă la cunoştinţa prestatorului de servicii de încredere supus controlului, care poate fi contestată de către prestatorul de servicii de încredere. (15) La efectuarea controlului privind respectarea obligaţiilor prevăzute de prezenta lege, prestatorul de servicii de încredere prezintă informaţia şi documentele relevante scopului controlului şi nu împiedică efectuarea acestuia. (16) În baza rezultatelor controlului se întocmeşte un act în 2 exemplare, unul dintre care se expediază/înmânează, în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat,				

	prestatorului de servicii de încredere, iar al doilea se păstrează la organul de supraveghere şi control. În cazul în care nu este de acord cu rezultatele controlului efectuat, prestatorul de servicii de încredere, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexând documentele de rigoare. (17) În cazul în care se depistează încălcări ale obligaţiilor prevăzute de prezenta lege, organul supraveghere şi control emite, în baza actului de control, prescripţia privind lichidarea acestor încălcări, ce cuprinde recomandările privind modul de remediere a tuturor încălcărilor depistate, precum şi avertizarea despre posibila suspendare sau retragere a acreditării dacă acestea nu vor fi lichidate în termenul stabilit. (18) Termenul pentru lichidarea încălcărilor depistate constituie 15 zile lucrătoare, calculat din ziua următoare celei în care a fost primită prescripţia expediată/înmânată împreună cu actul de control. (19) Dacă în termenul stabilit prestatorul de servicii de încredere nu a lichidat toate încălcările depistate, la solicitarea oficială a acestuia, termenul pentru lichidarea încălcărilor este prelungit cu termenul solicitat de prestatorul de servicii de încredere, dar care nu poate depăşi 20 de zile lucrătoare.. (20) Prestatorul de servicii de încredere calificat care a primit prescripţia privind lichidarea încălcărilor obligaţiilor prevăzute de prezenta lege este obligat, în termenul indicat în prescripţie, să comunice organului de supraveghere şi control informaţia privind lichidarea încălcărilor. (21) Informaţiile despre rezultatele efectuării controlului se publică de către organul de supraveghere şi control pe pagina sa web oficială. (22) Prestatorul de servicii de încredere are dreptul să depună la organul de supraveghere şi control reclamaţii în scris privind încălcările prevederilor prezentei legi admise de Comisie sau să conteste acţiunile acesteia în instanţa judecătorească.				

	Articolul 36. Suspendarea şi reluarea valabilităţii acreditării (1) Acreditarea este suspendată în conformitate cu legislaţia în domeniul reglementării activităţii de întreprinzător. (2) Drept temei pentru realizarea acţiunilor prevăzute de lege pentru suspendarea acreditării servesc: a) cererea prestatorului de servicii de încredere calificat privind suspendarea acreditării; b) încălcarea de către prestatorul de servicii de încredere a obligaţiilor stabilite de prezenta lege; c) depistarea unor date neautentice în documentele prezentate organului de supraveghere şi control; d) nevalabilitatea garanţiei bancare sau a poliţei de asigurare; e) nerespectarea de către prestatorul de servicii de încredere a prescripţiei privind lichidarea încălcărilor prevăzute de prezenta lege, depistate în urma controlului efectuat de Comisie. (3) Decizia privind suspendarea acreditării se aduce la cunoştinţă prestatorului de servicii de încredere calificat în termen de 3 zile lucrătoare de la data adoptării acesteia. Termenul de suspendare a acreditării nu poate depăşi 2 luni. (4) Prestatorul de servicii de încredere calificat este obligat să înştiinţeze în scris organul de supraveghere şi control despre înlăturarea circumstanţelor care au dus la suspendarea acreditării. (5) Decizia privind reluarea valabilităţii acreditării se adoptă de către organul de supraveghere şi control în temeiul hotărârii instanţei de judecată care a emis hotărârea de suspendare a acreditării sau a instanţei de judecată ierarhic superioare, în termen de 3 zile lucrătoare de la data primirii înştiinţării. Decizia se aduce la cunoştinţă prestatorului de servicii de încredere în termen de 3 zile lucrătoare de la data adoptării acesteia. (6) Termenul de valabilitate a acreditării nu se prelungeşte pe perioada de suspendare a acesteia.				

	Articolul 37. Retragerea acreditării (1) Acreditarea este retrasă în conformitate cu legislaţia în domeniul reglementării activităţii de întreprinzător. (2) Drept temei pentru realizarea acţiunilor prevăzute de lege în vederea retragerii acreditării servesc: a) cererea prestatorului de servicii de încredere calificat privind încetarea activităţii, depusă cu 30 de zile înainte de încetarea planificată; b) decizia cu privire la anularea înregistrării de stat a întreprinzătorului individual sau a persoanei juridice în cadrul căreia activează prestatorul de servicii de încredere; c) constatarea faptului de transmitere a certificatului de acreditare sau a copiei de pe acesta altei persoane în scopul desfăşurării genului de activitate acreditat; d) neînlăturarea, în termenul stabilit, a circumstanţelor care au dus la suspendarea acreditării; e) nerespectarea repetată a prescripţiilor privind lichidarea încălcărilor obligaţiilor stabilite de prezenta lege. (3) Menţiunea referitoare la data şi numărul deciziei privind retragerea acreditării se înscrie în Registrul de evidenţă a prestatorilor de servicii de încredere nu mai târziu de ziua lucrătoare imediat următoare zilei adoptării deciziei. (4) Toate certificatele cheilor publice emise de către prestatorul de servicii de încredere calificat care şi-a încetat activitatea se revocă şi se transmit spre păstrare altui prestator de servicii de încredere calificat, în modul stabilit de organul de supraveghere şi control, pe cheltuiala prestatorului de servicii de încredere care îşi încetează activitatea. (5) Prestatorul de servicii de încredere calificat este obligat, în decurs de 10 zile lucrătoare de la data adoptării deciziei de retragere a acreditării, să depună la organul de supraveghere şi control certificatul de acreditare retras.				
(4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referinţă ale		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea		

următoarelor standarde: (a) pentru acreditarea organismelor de evaluare a conformității și pentru raportul de evaluare a conformității menționat la alineatul (1); (b) privind normele de audit în temeiul cărora organismele de evaluare a conformității își vor desfășura evaluarea conformității prestatorilor de servicii de încredere calificați, astfel cum se menționează la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).			RM la UE		
Articolul 21 **Inițierea unui serviciu de încredere calificat** (1) În cazul în care prestatorii de servicii de încredere care nu au statutul de calificat intenționează să înceapă să presteze servicii de încredere calificate, aceștia transmit organismului de supraveghere o notificare a intenției lor, împreună cu un raport de evaluare a conformității emis de un organism de evaluare a conformității. (2) Organismul de supraveghere verifică dacă prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele prevăzute în prezentul regulament și, în special, cerințele pentru prestatorii de servicii de încredere calificați și pentru serviciile de încredere calificate prestate de aceștia. În cazul în care organismul de supraveghere ajunge la concluzia că prestatorul de servicii de încredere și serviciile de încredere prestate de acesta respectă cerințele menționate în primul paragraf, organismul de supraveghere acordă statutul de calificat prestatorului de servicii de încredere și serviciilor de încredere prestate de acesta și informează organismul menționat la articolul 22 alineatul (3) în scopul actualizării listelor sigure menționate la articolul 22 alineatul (1), în termen de maximum trei luni de la notificare în conformitate cu alineatul (1) de la prezentul articol. În cazul în care verificarea nu este încheiată în termen de trei luni de la notificare, organismul de supraveghere informează prestatorul de servicii de încredere, specificând motivele întârzierii și termenul în care se	**Articolul 7. Acreditarea prestatorului de servicii de încredere** (1) Prestatorul de servicii de încredere obține statutul de calificat în urma procedurii de acreditare. (2) Prestatorii de servicii de încredere calificați se supun acreditării în conformitate cu prevederile prezentei legi. (3) Acreditarea prestatorului de servicii de încredere se efectuează de către organul de supraveghere și control în baza cererii depuse. Acreditarea prestatorului de servicii de încredere este gratuită și se acordă pentru un termen de 5 ani, dacă în cererea de acreditare nu este indicat un termen mai mic. (4) Organul de supraveghere și control, în baza documentelor prezentate, în termen de 30 de zile, adoptă decizia privind acreditarea prestatorului de servicii de încredere sau privind refuzul de acreditare. (5) Prestatorul de servicii de încredere se consideră calificat din ziua emiterii certificatului de acreditare. (6) Modul de solicitare, acordare, suspendare și retragere a certificatului de acreditare a prestatorului de servicii de încredere calificat se stabilește prin act normativ al organului de supraveghere și control. (7) Modul de solicitare, acordare, suspendare și retragere a certificatului de acreditare a prestatorului de servicii de încredere calificat se stabileşte de Legea nr. 160/2011 privind reglementarea prin autorizare a activității de întreprinzător, în partea în care nu este reglementat de prezenta lege.	**Compatibil**			**SIS al RM**

încheie verificarea.	(8) Informaţia despre prestatorii de servicii de încredere calificaţi acreditaţi, precum şi despre cei cu acreditarea retrasă se publică de către organul de supraveghere şi control pe pagina sa web oficială. (9) Prestatorii de servicii de încredere calificaţi sunt obligaţi, pe parcursul întregului termen de acreditare, să asigure respectarea cerinţelor în conformitate cu care a fost acreditat. În cazul apariţiei circumstanţelor care fac imposibilă asigurarea respectării acestor cerinţe, prestatorul de servicii de încredere calificat urmează să notifice organul de supraveghere şi control despre acest fapt în decurs de 24 de ore. (10) Prestatorii de servicii de încredere necalificaţi sunt obligaţi să comunice organului de supraveghere şi control, cel târziu în termen de 10 zile, orice modificare a procedurilor de securitate şi de certificare, cu precizarea datei şi orei la care modificarea a intrat sau va intra în vigoare. (11) Prestatorul de servicii de încredere calificat de nivel superior nu este supus acreditării în conformitate cu prevederile prezentei legi.				
(3) Prestatorii de servicii de încredere calificaţi pot începe furnizarea serviciului de încredere calificat după ce statutul de calificat a fost indicat în listele sigure menţionate la articolul 22 alineatul (1). (4) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele şi procedurile în sensul alineatelor (1) şi (2). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE		
Articolul 22 **Listele sigure** (1) Fiecare stat membru instituie, menţine şi publică liste care includ informaţii referitoare la prestatorii de servicii de încredere calificaţi pentru care este responsabil, împreună cu informaţii referitoare la serviciile de încredere calificate prestate de aceştia. (2) Statele membre instituie, menţin şi publică, în mod securizat, listele sigure semnate sau sigilate electronic		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE		

menționate la alineatul (1), într-o formă adecvată pentru prelucrarea automată. (3) Statele membre notifică Comisiei, fără întârzieri nejustificate, informații cu privire la organismul responsabil pentru instituirea, menținerea și publicarea listelor sigure naționale și detalii despre locul unde sunt publicate aceste liste, certificatele utilizate pentru semnarea sau sigilarea listelor sigure și orice modificări ale acestora. (4) Comisia pune la dispoziția publicului, printr-un canal sigur, informațiile menționate la alineatul (3) într-o formă purtând o semnătură electronică sau un sigiliu electronic adecvate pentru prelucrarea automată. (5) Până la 18 septembrie 2015, Comisia specifică, prin intermediul unor acte de punere în aplicare, informațiile menționate la alineatul (1) și definește specificațiile tehnice și formatele pentru listele sigure aplicabile în sensul alineatelor (1)-(4). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).RO 28.8.2014 Jurnalul Oficial al Uniunii Europene L 257/97					
Articolul 23 **Marca de încredere a UE pentru serviciile de încredere calificate** (1) După indicarea statutului de calificat menționat la articolul 21 alineatul (2) al doilea paragraf pe lista sigură menționată la articolul 22 alineatul (1), prestatorii de servicii de încredere calificați pot utiliza o marcă de încredere a UE pentru a indica într-un mod simplu, ușor de recunoscut și clar serviciile de încredere calificate pe care le prestează. (2) În cazul utilizării mărcii de încredere a UE pentru serviciile de încredere calificate menționate la alineatul (1), prestatorii de servicii de încredere calificați se asigură că pe site-ul lor internet este disponibil un link către lista sigură relevantă. (3) Până la 1 iulie 2015, Comisia, prin intermediul unor acte de punere în aplicare, stabilește specificațiile referitoare la forma și, în special, prezentarea,		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

componența, mărimea și designul mărcii de încredere a UE pentru serviciile de încredere calificate. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
Articolul 24 **Cerințe pentru prestatorii de servicii de încredere calificați** (1) Atunci când emite un certificat calificat pentru un serviciu de încredere, un prestator de servicii de încredere calificat verifică, prin mijloace corespunzătoare și în conformitate cu legislația națională, identitatea și, atunci când este cazul, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat. Informațiile menționate la primul paragraf sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părți terțe, în conformitate cu dreptul intern: (a) de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau (b) de la distanță, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului calificat, a fost asigurată prezența fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice și care îndeplinesc cerințele stabilite la articolul 8 în ceea ce privește nivelurile de asigurare „substanțial" sau „ridicat"; sau (c) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat emis în conformitate cu dispozițiile de la litera (a) sau (b); sau (d) prin utilizarea altor metode de identificare recunoscute la nivel național, care oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică. Nivelul de asigurare echivalent este confirmat de un organism de evaluare a conformității. (2) Un prestator de servicii de încredere calificat care prestează servicii de încredere calificate: (a) informează organismul de supraveghere cu privire la	**Articolul 9. Obligaţiile prestatorului de servicii de încredere** (1) Prestatorul de servicii de încredere este obligat: a) să verifice autenticitatea datelor indicate în cererea de certificare a cheii publice în baza documentelor ce confirmă datele în cauză; b) să asigure corespunderea informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice; c) să introducă certificatul cheii publice în registrul certificatelor cheilor publice nu mai târziu de data şi ora la care începe să curgă termenul de valabilitate a certificatului; d) să asigure accesul la registrul certificatelor cheilor publice, cu respectarea prevederilor art. 51; e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege şi să facă menţiunea respectivă în registrul certificatelor cheilor publice în termenele stabilite; f) să acopere prejudiciile aduse oricărei entităţi sau persoane fizice, care se încrede în mod rezonabil în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de încredere, prin faptul că a omis să înregistreze revocarea certificatului; g) să înştiinţeze titularul certificatului cheii publice despre faptele care au devenit cunoscute prestatorului de servicii de încredere şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice; h) să prezinte informaţiile necesare pentru autentificarea serviciilor de încredere; i) să îndeplinească alte obligaţii stabilite de legislaţie. (2) Prestatorul de servicii de încredere calificat este obligat, suplimentar celor stipulate la alin. (1):	**Compatibil**			**SIS al RM**

orice schimbare survenită în prestarea sa de servicii de încredere calificate şi cu privire la vreo intenţie de a îşi înceta activitatea respectivă; (b) angajează personal şi, după caz, subcontractanţi care deţin cunoştinţele, credibilitatea, experienţa şi calificările necesare şi care au beneficiat de formare adecvată în ceea ce priveşte normele de siguranţă şi protecţie a datelor cu caracter personal şi aplică proceduri administrative şi de gestiune care corespund standardelor europene sau internaţionale; (c) în ceea ce priveşte riscul de răspundere pentru daune în conformitate cu articolul 13, menţine suficiente resurse financiare şi/sau obţine o asigurare de răspundere adecvată, în conformitate cu dreptul intern; (d) înainte de stabilirea unei relaţii contractuale, informează, în mod clar şi cuprinzător, orice persoană care doreşte să utilizeze un serviciu de încredere calificat de clauzele şi condiţiile exacte privind utilizarea acelui serviciu, inclusiv orice restricţie privind utilizarea acestuia; (e) utilizează sisteme şi produse demne de încredere care sunt protejate împotriva modificărilor şi asigură siguranţa tehnică şi fiabilitatea proceselor susţinute de acestea; (f) utilizează sisteme demne de încredere pentru a stoca datele care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât: (i) acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obţinut consimţământul persoanei la care se referă datele; (ii) numai persoanele autorizate să poată introduce şi modifica datele stocate; (iii) autenticitatea datelor să poată fi controlată; (g) ia măsuri adecvate împotriva falsificării şi furtului de date; (h) înregistrează şi menţine accesibile pentru o perioadă de timp corespunzătoare, inclusiv ulterior încetării activităţii prestatorului de servicii de încredere calificat, toate informaţiile relevante referitoare la datele emise şi primite de către prestatorul de servicii de încredere calificat, în special în scopul de a furniza dovezi în procedurile judiciare şi în scopul asigurării continuităţii serviciului.	1) să certifice, în modul stabilit de legislaţie, cheia sa publică destinată certificării cheilor publice; 2) să informeze organul de supraveghere şi control cu privire la orice schimbare survenită în prestarea de servicii de încredere calificate şi cu privire la intenţia de a îşi înceta activitatea respectivă; 3) să utilizeze sisteme sigure pentru stocarea datelor care îi sunt furnizate, într-o formă care poate fi verificată, astfel încât: a) acestea să fie disponibile publicului pentru cercetări numai în cazul în care a fost obţinut consimţământul subiectului la care se referă datele; b) numai persoanele autorizate să poată introduce şi/sau modifica datele stocate; c) autenticitatea datelor să poată fi controlată; 4) să verifice, prin mijloace corespunzătoare şi în conformitate cu legislaţia, identitatea şi, după caz, atributele specifice ale persoanei fizice sau juridice căreia i s-a emis un certificat calificat. Informaţiile menţionate sunt verificate de prestatorul de servicii de încredere calificat, fie direct, fie prin intermediul unei părţi terţe: a) de către persoana fizică sau de către un reprezentant autorizat al persoanei juridice, în persoană; sau b) de la distanţă, utilizând mijloace de identificare electronică pentru care, înainte de eliberarea certificatului calificat, a fost asigurată prezenţa fizică a persoanei fizice sau a unui reprezentant autorizat al persoanei juridice; c) prin intermediul unui certificat, al unei semnături electronice calificate sau al unui sigiliu electronic calificat; d) prin utilizarea altor metode de identificare recunoscute la nivel naţional, care oferă un nivel de asigurare echivalent, din perspectiva fiabilităţii, cu prezenţa fizică. Metodele alternative de identificare de la distanţă a persoanei sunt stabilite de către Guvern. 5) să ia măsuri adecvate împotriva falsificării şi furtului de date;				

Aceste înregistrări pot fi efectuate în mod electronic; (i) are un plan actualizat, în cazul încetării serviciului, pentru a asigura continuitatea serviciului conform dispoziţiilor verificate de către organismul de supraveghere, în conformitate cu articolul 17 alineatul (4) litera (i); (j) asigură prelucrarea legală a datelor cu caracter personal în conformitate cu Directiva 95/46/CE; (k) în cazul prestatorilor de servicii de încredere calificaţi care eliberează certificate calificate, instituie şi actualizează permanent o bază de date a certificatelor. (3) Dacă un prestator de servicii de încredere calificat care eliberează certificate calificate decide să revoce un certificat, acesta înregistrează respectiva revocare în baza sa de date privind certificatele şi publică statutul de revocat al certificatului în timp util şi în orice caz în termen de 24 de ore de la primirea cererii. Revocarea intră în vigoare imediat după publicare. (4) Cu privire la alineatul (3), prestatorii de servicii de încredere calificaţi care emit certificate calificate furnizează oricărui beneficiar informaţii cu privire la valabilitatea sau revocarea statutului de certificate calificate emise de aceştia. Aceste informaţii sunt puse la dispoziţie cel puţin pentru fiecare certificat în parte, în orice moment şi după expirarea perioadei de valabilitate a certificatului, în mod automat, fiabil, gratuit şi eficient.	6) să înregistreze, pe o perioadă stabilită de timp, în conformitate cu art. 12, toate informaţiile pertinente referitoare la un certificat calificat al cheii publice, în special pentru a putea furniza dovezi privind certificarea în justiţie. Înregistrările pot fi efectuate prin mijloace electronice; 7) înainte să stabilească o relaţie contractuală cu o persoană care solicită un certificat în sprijinul serviciului său de încredere, să informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele şi condiţiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării acestui certificat, la existenţa unui sistem de acreditare şi la procedurile de contestare şi soluţionare a litigiilor. Informaţiile transmise pe cale electronică, trebuie comunicate în scris, într-un limbaj accesibil. Elementele pertinente ale informaţiilor trebuie puse, de asemenea, la cerere, la dispoziţia părţilor terţe care beneficiază de certificat; 8) să solicite eliberarea duplicatului certificatului de acreditare în cazul pierderii sau deteriorării acestuia; 9) să înregistreze şi menţină accesibile pentru o perioadă de 15 ani, inclusiv ulterior încetării activităţii, toate informaţiile relevante referitoare la datele emise şi primite, în special în scopul de a furniza dovezi în procedurile judiciare şi în scopul asigurării continuităţii serviciului. Aceste înregistrări pot fi efectuate în mod electronic.				
(5) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numerele de referinţă ale standardelor pentru sisteme şi produse demne de încredere, care respectă cerinţele prevăzute la alineatul (2) literele (e) şi (f) de la prezentul articol. În cazul în care sistemele şi produsele demne de încredere respectă standardele respective, se presupune că acestea respectă cerinţele prevăzute la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE		

SECȚIUNEA 4 **Semnătura electronică** **Articolul 25** **Efectele juridice ale semnăturilor electronice** (1) Unei semnături electronice nu i se refuză efectul juridic şi posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este în format electronic sau că nu îndeplineşte cerinţele pentru semnăturile electronice calificate. (2) O semnătură electronică calificată are efectul juridic echivalent al unei semnături olografe. (3) O semnătură electronică calificată bazată pe un certificat calificat eliberat de un stat membru este recunoscută drept semnătură electronică calificată în toate celelalte state membre.	**Articolul 18. Principiile de utilizare a semnăturii electronice şi sigiliului electronic** Principiile de utilizare a semnăturii electronice şi sigiliului electronic sunt: a) libertatea alegerii şi utilizării oricărui tip de semnătură electronică sau sigiliului electronic, dacă actele normative sau acordul părţilor nu prevăd cerinţa de utilizare a unui tip concret de semnătură electronică sau sigiliu electronic, în corespundere cu obiectivele de utilizare a acesteia; b) posibilitatea alegerii oricăror tehnologii şi/sau mijloace tehnice care permit utilizarea tipurilor concrete de semnături electronice sau sigiliului electronic în conformitate cu prevederile prezentei legi; c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice sau a sigiliului electronic şi/sau a documentului electronic pe care acestea sunt aplicate doar în baza faptului că semnătura electronică sau sigiliul electronic a fost creat prin intermediul dispozitivului de creare a semnăturii electronice sau a sigiliului electronic şi/sau al produsului. **Articolul 20. Regimul juridic de utilizare a semnăturii electronice şi sigiliului electronic** (1) Semnătura electronică şi sigiliul electronic, indiferent de gradul de protecţie de care dispune, produce efecte juridice şi este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă: a) se prezintă în formă electronică; sau b) nu se bazează pe un certificat eliberat de un prestator servicii de încredere; sau c) nu se bazează pe un certificat calificat al cheii publice; sau d) nu este creată prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic. (2) Semnătura electronică calificată are aceeaşi valoare juridică ca şi semnătura olografă. (3) Semnătura electronică calificată şi sigiliu electronic calificat beneficiază de prezumţia integrităţii datelor şi a corectitudinii originii respectivelor date la care se	**Parţial compatibil**	Transpunerea integrală este condiţionată de aderarea RM la UE		

	referă semnătura electronică sau sigiliul electronic calificat. (4) Modalitatea în care se asigură gradul de protecţie a semnăturii electronice calificate pentru echivalarea acesteia cu semnătura olografă aplicată pe hârtie se stabileşte de organul de supraveghere şi control, conform atribuţiilor prevăzute la art. 34 alin. (2). (5) Modalitatea de aplicare a semnăturilor electronice de către funcţionarii persoanelor juridice de drept public se stabileşte de Guvern. Persoanele juridice de drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanţii acestora. (6) Semnătura electronică şi sigiliul electronic nu constituie mijloace de criptare a informaţiei.				
Articolul 26 **Cerințe pentru semnături electronice avansate** O semnătura electronică avansată îndeplinește următoarele cerințe: (a) face trimitere exclusiv la semnatar; (b) permite identificarea semnatarului; (c) este creată utilizând date de creare a semnăturilor electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său; și (d) este legată de datele utilizate la semnare astfel încât orice modificare ulterioară a datelor poate fi detectată.	**Articolul 22. Cerințe pentru semnăturile electronice și sigiliile electronice avansate** Semnăturile electronice sau sigiliile electronice avansate îndeplinesc cumulativ următoarele cerinţe: a) fac trimitere exclusiv la titular; b) permit identificarea titularului; c) sunt create utilizând date de creare a semnăturilor electronice, sau a sigiliilor electronice, pe care semnatarul, sau creatorul sigiliului, le poate utiliza cu un nivel ridicat de încredere, exclusiv sub controlul său; d) sunt legate de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.	**Compatibil**			**SIS al RM**
Articolul 27 **Semnăturile electronice în cadrul serviciilor publice** (1) În cazul în care un stat membru solicită o semnătură electronică avansată pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaşte semnăturile electronice avansate, semnăturile electronice avansate bazate pe un certificat calificat pentru semnături electronice şi semnăturile electronice calificate care întrebuinţează cel puţin formatele sau metodele		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

definite în actele de punere în aplicare menționate la alineatul (5). (2) În cazul în care un stat membru solicită o semnătură electronică avansată bazată pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaşte semnăturile electronice avansate bazate pe un certificat calificat şi semnăturile electronice calificate care întrebuinţează cel puţin formatele sau metodele definite în actele de punere în aplicare menţionate la alineatul (5). (3) Statele membre nu solicită o semnătură electronică la un nivel de securitate mai ridicat decât cel al semnăturii electronice calificate pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public. (4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referinţă ale standardelor pentru semnături electronice avansate. În cazul în care o semnătură electronică avansată îndeplineşte respectivele standarde, se presupune că aceasta respectă cerinţele referitoare la semnăturile electronice avansate menţionate în prezentul articol alineatele (1) şi (2) şi la articolul 26. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2). 5) Până la 18 septembrie 2015 şi ţinând cont de practicile, standardele şi actele juridice ale Uniunii existente, Comisia defineşte, prin intermediul unor acte de punere în aplicare, formate de referinţă ale semnăturilor electronice avansate sau metode de referinţă, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).					
Articolul 28 **Certificate calificate pentru semnăturile electronice** (1) Certificatele calificate pentru semnăturile electronice îndeplinesc cerinţele prevăzute în anexa I. (2) Certificatele calificate pentru semnăturile electronice	**Articolul 24. Cerinţe pentru certificatele calificate pentru semnături electronice sau pentru sigilii electronice** Certificatele calificate pentru semnături electronice sau pentru sigilii electronice conţin:	**Parţial compatibil**	Transpunerea integrală este condiţionată de aderarea RM la UE		

nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa I. (3) Certificatele calificate pentru semnăturile electronice pot include atribute specifice suplimentare facultative. Aceste atribute nu afectează interoperabilitatea și recunoașterea semnăturilor electronice calificate. (4) În cazul în care un certificat calificat pentru semnăturile electronice a fost revocat după activarea inițială, acesta își pierde valabilitatea din momentul în care a fost revocat și nu se revine în niciun caz la statutul său anterior. (5) Sub rezerva următoarelor condiții, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a unui certificat calificat pentru semnătura electronică: (a) în cazul în care un certificat calificat pentru semnătura electronică a fost suspendat temporar, acest certificat își pierde valabilitatea pe parcursul perioadei de suspendare; (b) perioada de suspendare este clar indicată în baza de date privind certificatele și statutul de suspendat este vizibil, pe perioada suspendării, din serviciul care oferă informații privind statutul certificatului. (6) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru semnătura electronică. În cazul în care un certificat calificat pentru semnătura electronică îndeplinește standardele respective, se presupune că acesta respectă cerințele prevăzute în anexa I. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale semnatarului sau creatorului sigiliului electronic; d) datele de validare a semnăturilor electronice sau sigiliilor electronice care corespund datelor de creare a acestora; e) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează; f) numărul unic de înregistrare a certificatului; g) date de verificare a certificatului calificat pentru semnătura electronică sau sigiliul electronic care corespund datelor de creare a acestora; h) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent, sau; i) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice recunoscute conform art. 3, sau; j) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere de nivel superior, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice ale prestatorilor de servicii de întredere acreditați.				
Articolul 29 **Cerințe pentru dispozitivele de creare a semnăturilor electronice calificate** (1) Dispozitivele de creare a semnăturilor electronice calificate îndeplinesc cerințele prevăzute în anexa II. (2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale	**Articolul 26. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice** (1) Dispozitivele de creare a semnăturilor electronice sau sigiilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice și proceduri corespunzătoare, cel puțin că: a) datele de creare a semnăturii sau a sigiliului	**Parțial compatibil**	Transpunerea integrală este condiționată de aderarea RM la UE		

standardelor pentru dispozitivele de creare a semnăturilor electronice calificate. În cazul în care un dispozitiv de creare a semnăturilor electronice calificat îndeplinește standardele respective, se presupune că acesta respectă cerințele prevăzute în anexa II. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	electronic nu pot apărea decât o singură dată, iar confidenţialitatea acestora este asigurată în conformitate cu prezenta lege; b) datele de creare a semnăturii electronice sau a sigiliului electronic nu pot fi deduse prin calcul şi semnătura electronică sau sigiliul electronic sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată; c) datele de creare a semnăturii electronice sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane; d) oferă posibilitatea afişării conţinutului documentului electronic pe care se aplică semnătura electronică sau sigiliul electronic sau face referinţa irevocabilă la documentul dat; e) semnătura electronică sau sigiliul electronic este creat numai după confirmarea de către semnatar sau creatorul unui sigiliu a operaţiunii de creare a semnăturii electronice sau a sigiliului electronic; f) confirmă în mod univoc crearea semnăturii sau a sigiliului electronic. (2) Dispozitivele de creare a semnăturii electronice sau a sigiliului electronic avansate sau calificate nu trebuie să modifice datele asupra cărora se aplică semnătura electronică sau sigiliul electronic avansat sau calificat, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.				
Articolul 30 **Certificarea dispozitivelor de creare a semnăturilor electronice calificate** (1) Conformitatea dispozitivelor de creare a semnăturii electronice calificate cu cerințele prevăzute în anexa II este certificată de organisme publice sau private adecvate desemnate de statele membre.		**Parțial compatibil**	Prevederile art. 30 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii. Astfel, prevederile menționate vor fi transpuse prin modificarea ordinului directorului SIS al RM nr. 25/2017 și ordinului	În termen de 12 luni de la data publică rii legii	**SIS al RM**

			directorului SIS al RM nr. 69/2016.		
(2) Statele membre notifică Comisiei denumirile și adresele organismului public sau privat menționat la alineatul (1). Comisia pune informațiile respective la dispoziția statelor membre. (3) Certificarea menționată la alineatul (1) se bazează pe unul dintre următoarele elemente: (a) un proces de evaluare de securitate efectuat în conformitate cu unul dintre standardele pentru evaluarea securității produselor din domeniul tehnologiei informației incluse în lista instituită în conformitate cu al doilea paragraf; sau (b) un alt proces decât procesul prevăzut la litera (a), cu condiția ca acest proces să utilizeze niveluri de securitate comparabile și ca organismul public sau privat menționat la alineatul (1) să notifice Comisiei respectivul proces. Procesul respectiv poate fi utilizat numai în absența standardelor menționate la litera (a) sau dacă un proces de evaluare de securitate menționat la litera (a) este în curs de desfășurare. Comisia stabilește, prin intermediul unor acte de punere în aplicare, lista standardelor pentru evaluarea de securitate a produselor din domeniul tehnologiei informației menționate la litera (a). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).(4) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 47 privind stabilirea de criterii specifice care urmează să fie îndeplinite de către organismele desemnate menționate la alineatul (1) de la prezentul articol.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 31 **Publicarea unei liste a dispozitivelor de creare a semnăturilor electronice certificate și calificate** (1) Statele membre notifică Comisiei, fără întârzieri nejustificate și în termen de maximum o lună de la încheierea certificării, informații cu privire la dispozitivele de creare a semnăturilor electronice calificate care au fost certificate de către organismele menționate la articolul 30 alineatul (1). De asemenea, statele membre notifică		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

Comisiei, fără întârziere și în termen de maximum o lună de la anularea certificării, informații cu privire la dispozitivele de creare a semnăturii electronice care nu mai sunt certificate. (2) Pe baza informațiilor primite, Comisia stabilește, publică și menține o listă a dispozitivelor de creare a semnăturilor electronice certificate și calificate. (3) Comisia poate, prin intermediul unor acte de punere în aplicare, să definească formatele și procedurile aplicabile în sensul alineatului (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
Articolul 32 **Cerințe pentru validarea semnăturilor electronice calificate** (1) Procesul de validare a unei semnături electronice calificate confirmă validitatea unei semnături electronice calificate cu următoarele condiții: (a) certificatul care stă la baza semnăturii a fost, la momentul semnării, un certificat calificat pentru semnătura electronică în conformitate cu anexa I; (b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul semnării; (c) datele de validare a semnăturilor corespund datelor furnizate de beneficiar; (d) setul unic de date care reprezintă semnatarul în certificat este furnizat corect beneficiarului; (e) utilizarea vreunui pseudonim este indicată clar beneficiarului în cazul în care la momentul semnării s-a folosit un pseudonim; (f) semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat; (g) integritatea datelor semnate nu a fost compromisă;(h) cerințele prevăzute la articolul 26 au fost îndeplinite la momentul semnării. (2) Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului	**Articolul 28. Cerințe pentru validarea semnăturii și sigiliului electronic calificate** Procesul de validare a unei semnături electronice sau sigiliu electronic calificat confirmă validitatea acestora cu următoarele condiții: a) certificatul care stă la baza semnăturii electronice sau sigiliului electronic a fost, la momentul semnării sau sigilării, un certificat calificat pentru semnătura electronică sau sigiliu electronic, în conformitate cu articolul 25; b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat și a fost valabil în momentul aplicării semnăturii electronice sau sigiliului electronic; c) datele de validare a semnăturilor electronice sau sigiliilor electronice corespund datelor furnizate de titularul certificatului cheii publice; d) setul unic de date care reprezintă semnatarul sau creatorul sigiliului electronic în certificat este furnizat corect titularului certificatului cheii publice; e) utilizarea vreunui pseudonim este indicată clar titularului certificatului cheii publice în cazul în care la momentul semnării s-a folosit un pseudonim; f) semnătura electronică sau sigiliul electronic a fost creat printr-un dispozitiv de creare a semnăturilor sau sigiliilor electronice calificate; g) integritatea datelor asupra cărora a fost aplicată	**Compatibil**			**SIS al RM**

să detecteze orice aspect relevant pentru securitate.	semnătura electronică sau sigiliul electronic nu a fost compromisă; h) cerințele prevăzute la art. 22 au fost îndeplinite la momentul semnării.				
(3) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru validarea semnăturilor electronice calificate. În cazul în care validarea semnăturilor electronice calificate îndeplineşte standardele respective, se presupune că aceasta respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 33 **Serviciul calificat de păstrare a semnăturilor electronice calificate** (1) Un serviciu de validare calificat pentru semnături electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care: (a) realizează validarea în conformitate cu articolul 32 alineatul (1); şi (b) permite beneficiarilor să primească rezultatul procesului de validare în mod automat, fiabil, eficient şi care poartă semnătura electronică avansată sau sigiliul electronic avansat al prestatorului care oferă serviciul de validare calificat.		**Parțial compatibil**	Prevederile art. 33 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii. Astfel, prevederile menționate vor fi transpuse prin modificarea ordinului directorului SIS al RM nr. 69/2016.		**SIS al RM**
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință pentru standardele referitoare la serviciul de validare calificat menționat la alineatul (1). În cazul în care serviciul de validare a semnăturilor electronice calificate îndeplineşte standardele respective, se prezumă că acesta respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 34 **Serviciul calificat de păstrare a semnăturilor electronice calificate** (1) Un serviciu calificat de păstrare a semnăturilor		**Parțial compatibil**	Prevederile art. 34 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele		**SIS al RM**

electronice calificate poate fi prestat numai de către un prestator de servicii de încredere calificat care utilizează proceduri și tehnologii capabile să extindă fiabilitatea semnăturilor electronice calificate dincolo de perioada de validitate tehnologică.			normative subordonate legii. Astfel, prevederile menționate vor fi transpuse prin modificarea ordinului directorului SIS al RM nr. 69/2016.		
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru serviciul calificat de păstrare a semnăturilor electronice calificate. În cazul în care dispozițiile privind serviciul calificat de păstrare a semnăturilor electronice calificate îndeplinesc standardele respective, se presupune că acestea respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
SECȚIUNEA 5 **Sigiliile electronice** **Articolul 35** **Efectele juridice ale sigiliilor electronice** (1) Unui sigiliu electronic nu i se refuză efectul juridic și posibilitatea de a fi acceptat ca probă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru sigiliile electronice calificate. (2) Un sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă sigiliul electronic calificat.	**Articolul 20. Regimul juridic de utilizare a semnăturii electronice și sigiliului electronic** (1) Semnătura electronică și sigiliul electronic, indiferent de gradul de protecție de care dispune, produce efecte juridice și este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă: a) se prezintă în formă electronică; sau b) nu se bazează pe un certificat eliberat de un prestator servicii de încredere; sau c) nu se bazează pe un certificat calificat al cheii publice; sau d) nu este creată prin intermediul dispozitivului de creare a semnăturii electronice sau sigiliului electronic. (2) Semnătura electronică calificată are aceeași valoare juridică ca și semnătura olografă. (3) Semnătura electronică calificată și sigiliu electronic calificat beneficiază de prezumția integrității datelor și a corectitudinii originii respectivelor date la care se referă semnătura electronică sau sigiliul electronic calificat. (4) Modalitatea în care se asigură gradul de protecție a semnăturii electronice calificate pentru echivalarea	**Compatibil**			**SIS al RM**

	acesteia cu semnătura olografă aplicată pe hârtie se stabileşte de organul de supraveghere şi control, conform atribuţiilor prevăzute la art. 34 alin. (2). (5) Modalitatea de aplicare a semnăturilor electronice de către funcţionarii persoanelor juridice de drept public se stabileşte de Guvern. Persoanele juridice de drept privat stabilesc de sine stătător modalitatea de aplicare a semnăturilor electronice de către reprezentanţii acestora. (6) Semnătura electronică şi sigiliul electronic nu constituie mijloace de criptare a informaţiei.				
(3) Un sigiliu electronic calificat bazat pe un certificat calificat eliberat de un stat membru este recunoscut drept sigiliu electronic calificat în toate celelalte state membre.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 36 **Cerințele pentru sigiliile electronice avansate** Un sigiliu electronic avansat îndeplinește următoarele cerințele: (a) face trimitere exclusiv la creatorul sigiliului; (b) permite identificarea creatorului sigiliului; (c) este creat cu ajutorul datelor de creare a sigiliilor electronice pe care creatorul sigiliului le poate utiliza sub controlul său, cu un nivel ridicat de încredere, pentru crearea sigiliilor electronice; și (d) este legat de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată.	**Articolul 22. Cerințe pentru semnăturile electronice și sigiliile electronice avansate** Semnăturile electronice sau sigiliile electronice avansate îndeplinesc cumulativ următoarele cerințe: a) fac trimitere exclusiv la titular; b) permit identificarea titularului; c) sunt create utilizând date de creare a semnăturilor electronice, sau a sigiliilor electronice, pe care semnatarul, sau creatorul sigiliului, le poate utiliza cu un nivel ridicat de încredere, exclusiv sub controlul său; d) sunt legate de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată	**Compatibil**			**SIS al RM**
Articolul 37 **Sigiliile electronice în cadrul serviciilor publice** (1) În cazul în care un stat membru solicită un sigiliu electronic avansat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate, sigiliile electronice avansate bazate pe un certificat calificat pentru sigilii electronice și sigiliile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

(2) În cazul în care un stat membru solicită un sigiliu electronic bazat pe un certificat calificat pentru utilizarea în cadrul unui serviciu online prestat de către un organism din sectorul public sau în numele acestuia, respectivul stat membru recunoaște sigiliile electronice avansate bazate pe un certificat calificat și sigiliile electronice calificate care întrebuințează cel puțin formatele sau metodele definite în actele de punere în aplicare menționate la alineatul (5). (3) Statele membre nu solicită un sigiliu electronic la un nivel de securitate mai ridicat decât cel al sigiliului electronic calificat pentru utilizarea transfrontalieră a unui serviciu online prestat de un organism din sectorul public. (4) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru sigilii electronice avansate. În cazul în care un sigiliu electronic avansat îndeplinește standardele respective, se presupune că acesta respectă cerințele referitoare la sigiliile electronice avansate menționate la alineatele (1) și (2) de la prezentul articol și la articolul 36. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2). (5) Până la 18 septembrie 2015 și ținând cont de practicile, standardele și actele juridice ale Uniunii existente, Comisia definește, prin intermediul unor acte de punere în aplicare, formate de referință ale sigiliilor electronice avansate sau metode de referință, în cazul în care sunt utilizate formate alternative. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).					
Articolul 38 **Certificate calificate pentru sigiliul electronic** (1) Certificatele calificate pentru sigiliile electronice îndeplinesc cerințele prevăzute în anexa III. (2) Certificatele calificate pentru sigiliile electronice nu fac obiectul niciunei cerințe obligatorii în plus față de cerințele prevăzute în anexa III. (3) Certificatele calificate pentru sigiliile electronice pot include atribute specifice suplimentare facultative. Aceste	**Articolul 24. Cerințe pentru certificatele calificate pentru semnături electronice sau pentru sigilii electronice** Certificatele calificate pentru semnături electronice sau pentru sigilii electronice conțin: a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii electronice;	**Parțial compatibil**	Transpunerea integrală este condiționată de aderarea RM la UE		**SIS al RM**

atribute nu afectează interoperabilitatea şi recunoaşterea sigiliilor electronice calificate. (4) În cazul în care un certificat calificat pentru un sigiliu electronic a fost revocat după activarea iniţială, acesta îşi pierde valabilitatea din momentul în care a fost revocat şi nu se revine în niciun caz la statutul său anterior. (5) Sub rezerva următoarelor condiţii, statele membre pot să stabilească norme interne cu privire la suspendarea temporară a certificatelor calificate pentru sigiliile electronice: (a) în cazul în care un certificat calificat pentru sigilii electronice a fost suspendat temporar, respectivul certificat îşi pierde valabilitatea pe parcursul perioadei de suspendare; (b) perioada de suspendare este clar indicată în baza de date privind certificatele şi statutul de suspendat este vizibil, pe perioada suspendării, din serviciul care oferă informaţii privind statutul certificatului. (6) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referinţă ale standardelor pentru certificatele calificate pentru sigiliile electronice. În cazul în care un certificat calificat pentru sigiliul electronic îndeplineşte standardele respective, se presupune că acesta respectă cerinţele prevăzute în anexa III. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).	b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare şi alte date ale semnatarului sau creatorului sigiliului electronic; d) datele de validare a semnăturilor electronice sau sigiliilor electronice care corespund datelor de creare a acestora; e) data şi ora la care începe să curgă termenul de valabilitate a certificatului şi data şi ora la care acest termen încetează; f) numărul unic de înregistrare a certificatului; g) date de verificare a certificatului calificat pentru semnătura electronică sau sigiliul electronic care corespund datelor de creare a acestora; gh semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent, sau; i) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice recunoscute conform art. 3, sau; j) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere de nivel superior, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice ale prestatorilor de servicii de întredere acreditaţi.				
Articolul 39 **Dispozitive de creare a sigiliilor electronice calificate** (1) Articolul 29 se aplică mutatis mutandis cerinţelor pentru dispozitivele de creare a sigiliilor electronice calificate. (2) Articolul 30 se aplică mutatis mutandis certificării dispozitivelor de creare a sigiliilor electronice calificate. (3) Articolul 31 se aplică mutatis mutandis publicării unei liste a dispozitivelor de creare a sigiliilor electronice certificate şi calificate.	**Articolul 26. Cerinţe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice** (1) Dispozitivele de creare a semnăturilor electronice sau sigiilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice şi proceduri corespunzătoare, cel puţin că: a) datele de creare a semnăturii sau a sigiliului electronic nu pot apărea decât o singură dată, iar confidenţialitatea acestora este asigurată în conformitate cu prezenta lege;	**Parţial compatibil**	Transpunerea integrală este condiţionată de aderarea RM la UE. Totodată, prevederile art.30 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.		**SIS al RM**

	b) datele de creare a semnăturii electronice sau a sigiliului electronic nu pot fi deduse prin calcul şi semnătura electronică sau sigiliul electronic sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată; c) datele de creare a semnăturii electronice sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane; d) oferă posibilitatea afişării conţinutului documentului electronic pe care se aplică semnătura electronică sau sigiliul electronic sau face referinţa irevocabilă la documentul dat; e) semnătura electronică sau sigiliul electronic este creat numai după confirmarea de către semnatar sau creatorul unui sigiliu a operaţiunii de creare a semnăturii electronice sau a sigiliului electronic; f) confirmă în mod univoc crearea semnăturii sau a sigiliului electronic. (2) Dispozitivele de creare a semnăturii electronice sau a sigiliului electronic avansate sau calificate nu trebuie să modifice datele asupra cărora se aplică semnătura electronică sau sigiliul electronic avansat sau calificat, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.				
Articolul 40 **Validarea şi păstrarea sigiliilor electronice calificate** Articolele 32, 33 şi 34 se aplică mutatis mutandis validării şi păstrării sigiliilor electronice calificate.	**Articolul 28. Cerinţe pentru validarea semnăturii şi sigiliului electronic calificate** Procesul de validare a unei semnături electronice sau sigiliu electronic calificat confirmă validitatea acestora cu următoarele condiţii: a) certificatul care stă la baza semnăturii electronice sau sigiliului electronic a fost, la momentul semnării sau sigilării, un certificat calificat pentru semnătura electronică sau sigiliu electronic, în conformitate cu articolul 25; b) certificatul calificat a fost emis de un prestator de servicii de încredere calificat şi a fost valabil în momentul aplicării semnăturii electronice sau sigiliului electronic;	**Parţial compatibil**	Transpunerea integrală este condiţionată de aderarea RM la UE Totodată, prevederile art.33 alin.(1) şi 34 alin.(1) nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.		**SIS al RM**

	c) datele de validare a semnăturilor electronice sau sigiliilor electronice corespund datelor furnizate de titularul certificatului cheii publice; d) setul unic de date care reprezintă semnatarul sau creatorul sigiliului electronic în certificat este furnizat corect titularului certificatului cheii publice; e) utilizarea vreunui pseudonim este indicată clar titularului certificatului cheii publice în cazul în care la momentul semnării s-a folosit un pseudonim; f) semnătura electronică sau sigiliul electronic a fost creat printr-un dispozitiv de creare a semnăturilor sau sigiliilor electronice calificate; g) integritatea datelor asupra cărora a fost aplicată semnătura electronică sau sigiliul electronic nu a fost compromisă; h) cerințele prevăzute la art. 22 au fost îndeplinite la momentul semnării.				
SECȚIUNEA 6 **Mărcile temporale electronice** **Articolul 41** **Efectul juridic al mărcilor temporale electronice** (1) Unei mărci temporale electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru marca temporală electronică calificată. (2) O marcă temporală electronică calificată beneficiază de prezumția corectitudinii datei și orei pe care le indică și a integrității datelor la care se raportează data și ora indicate.	**Articolul 29. Efectul juridic al mărcilor temporale electronice** (1) Unei mărci temporale electronice nu i se refuză efectul juridic și posibilitatea de a fi acceptată ca probă în procedurile judiciare doar din motiv că aceasta este sub formă electronică sau că nu îndeplinește cerințele pentru marca temporală electronică calificată. (2) O marcă temporală electronică calificată beneficiază de prezumția corectitudinii datei și orei pe care le indică și a integrității datelor la care se raportează data și ora indicate	**Compatibil**			**SIS al RM**
(3) O marcă temporală electronică calificată emisă într-un stat membru este recunoscută drept marcă temporală electronică calificată în toate statele membre.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 42 **Cerințe pentru mărcile temporale electronice calificate** (1) O marcă temporală electronică calificată îndeplinește următoarele cerințe: (a) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie	**Articolul 30. Cerințe pentru mărcile temporale electronice** (1) Cerințele pentru mărcile temporale electronice avansate sunt stabilite de către prestatorii de servicii de încredere. (2) O marcă temporală electronică calificată, se	**Compatibil**			**SIS al RM**

schimbate fără ca acest lucru să fie detectat; (b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată; și (c) este semnată utilizând o semnătură electronică avansată sau sigilată cu un sigiliu electronic avansat al prestatorului de servicii de încredere calificat sau printr-o metodă echivalentă.	elibrează de către prestatorul de servicii de încredere calificat și îndeplinește următoarele cerințe: a) asigură o legătură între dată și oră și date astfel încât să excludă în mod rezonabil posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat; b) se bazează pe o sursă de timp precisă, legată de ora universală coordonată; c) asupra acesteia este aplicată o semnătură electronică calificată sau un sigiliu electronic calificat al prestatorului de servicii de încredere calificat sau o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul mărcilor temporale recunoscute conform art. 3.				
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru legătura între dată și oră și date și pentru exactitatea surselor orei indicate. În cazul în care legătura între dată și oră și date și exactitatea surselor orei indicate îndeplinesc standardele respective, se presupune că se respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
SECȚIUNEA 7 **Serviciul de distribuție electronică înregistrată** **Articolul 43** **Efectul juridic al unui serviciu de distribuție electronică înregistrată** (1) Datelor trimise și primite prin utilizarea unui serviciu de distribuție electronică înregistrată nu li se refuză efectul juridic și posibilitatea de a fi acceptate ca dovadă în procedurile judiciare doar din motiv că acesta este sub formă electronică sau că nu îndeplinește cerințele pentru serviciul de distribuție electronică înregistrată. (2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată beneficiază de prezumția integrității datelor, a trimiterii datelor respective de către expeditorul identificat și a primirii acestora de	**Articolul 31. Efectul juridic al unui serviciu de distribuție electronică înregistrată** (1) Datelor transmise 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 calificat. (2) Datele trimise și primite utilizând un serviciu de distribuție electronică înregistrată calificat 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	**Compatibil**			**SIS al RM**

către destinatarul identificat şi a preciziei datei şi orei trimiterii şi primirii datelor indicate de serviciul de distribuţie electronică înregistrată.	serviciul de distribuţie electronică înregistrată.				
Articolul 44 **Cerinţe pentru serviciile de distribuţie electronică înregistrată calificate** (1) Serviciile de distribuţie electronică înregistrată calificate îndeplinesc următoarele cerinţe: (a) sunt prestate de către unul sau mai mulţi prestatori de servicii de încredere calificaţi; (b) asigură identificarea expeditorului cu un nivel de încredere ridicat; (c) asigură identificarea destinatarului înainte de furnizarea datelor; (d) trimiterea şi primirea datelor este securizată printr-o semnătură electronică avansată sau un sigiliu electronic avansat al prestatorului de servicii de încredere calificat astfel încât să se excludă posibilitatea ca datele să fie schimbate fără ca acest lucru să fie detectat; (e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului şi destinatarului datelor; (f) data şi ora trimiterii, primirii şi ale oricărei modificări a datelor este indicată printr-o marcă temporală electronică calificată. În cazul datelor transferate între doi sau mai mulţi prestatori de servicii de încredere, cerinţele de la literele (a)-(f) se aplică tuturor prestatorilor de servicii de încredere calificaţi.	**Articolul 32. Cerinţe pentru serviciile de distribuţie electronică înregistrată calificate** Serviciile de distribuţie electronică înregistrată calificate îndeplinesc următoarele cerinţe: a) sunt prestate de către unul sau mai mulţi prestatori de servicii de încredere calificaţi; b) asigură identificarea expeditorului; c) asigură identificarea destinatarului înainte de furnizarea datelor; d) trimiterea şi primirea datelor este securizată printr-o semnătură electronică sau un sigiliu electronic al prestatorului de servicii de încredere calificat astfel încât să se excludă posibilitatea că datele să fie schimbate fără ca acest lucru să fie detectat; e) orice modificare a datelor necesare în scopul de a trimite sau primi datele este clar indicată expeditorului şi destinatarului datelor; f) data şi ora trimiterii, primirii şi ale oricărei modificări a datelor este indicată printr-o marcă temporală electronică calificată.	**Compatibil**			**SIS al RM**
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referinţă ale standardelor pentru procesele de trimitere şi primire de date. În cazul în care procesul de trimitere şi primire de date îndeplineşte standardele respective, se presupune că se respectă cerinţele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiţionată de aderarea RM la UE		
SECŢIUNEA 8 **Autentificarea unui site internet**	**Articolul 33. Cerinţe pentru certificatele calificate pentru autentificarea unei pagini web**	**Compatibil**			**SIS al RM**

Articolul 45 Cerințe pentru certificatele calificate pentru autentificarea unui site internet(1) Certificatele calificate pentru autentificarea unui site internet îndeplinesc cerințele prevăzute în anexa IV.	Certificatele calificate pentru autentificarea unei pagini web trebuie să conțină: a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unei pagini web; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare şi alte date ale titularului certificatului cheii publice, precum şi informaţiile necesare pentru comunicarea cu acesta; d) data şi ora la care începe să curgă termenul de valabilitate a certificatului şi data şi ora la care acest termen încetează; e) numele domeniului (domeniilor) gestionate de titularul certificatului cheii publice căruia i s-a emis certificatul; f) numărul unic de înregistrare a certificatului; g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent sau semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru autentificarea unei pagini web recunoscute conform art. 3; h) date de verificare a certificatului calificat pentru autentificarea unei pagini web care corespund datelor de creare a acestuia.				
(2) Comisia poate, prin intermediul unor acte de punere în aplicare, să stabilească numere de referință ale standardelor pentru certificatele calificate pentru autentificarea unui site internet. În cazul în care un certificat calificat pentru autentificarea unui site internet îndeplineşte standardele respective, se presupune că respectă cerințele prevăzute în anexa IV. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
CAPITOLUL IV	**Articolul 39. Regimul juridic de utilizare a**	**Compatibil**			**SIS al RM**

DOCUMENTE ELECTRONICE **Articolul 46** **Efectele juridice ale documentelor electronice** Unui document electronic nu i se refuză efectul juridic şi posibilitatea de a fi acceptat ca dovadă în procedurile judiciare doar din motiv că este sub formă electronică.	**documentului electronic** (8) Documentul electronic asupra căruia a fost aplicată semnătura electronică sau sigiliul electronic este echivalat, după valoarea sa probantă, cu probele scrise sau mijloacele materiale de probă şi nu poate fi respins în calitate de probă doar pentru motivul că are o formă electronică.				
CAPITOLUL V **DELEGAREA DE COMPETENȚE ȘI MĂSURI DE PUNERE ÎN APLICARE** **Articolul 47** **Exercitarea delegării** (1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol. (2) Se conferă Comisiei, pentru o perioadă de timp nedeterminată de la 17 septembrie 2014, competența de a adopta actele delegate menționate la articolul 30 alineatul (4). (3) Delegarea competențelor menționată la articolul 30 alineatul (4) poate fi revocată în orice moment de către Parlamentul European sau de către Consiliu. Decizia de revocare pune capăt delegării competenței menționate în decizia respectivă. Aceasta produce efecte începând cu ziua următoare datei publicării în Jurnalul Oficial al Uniunii Europene sau la o dată ulterioară specificată în decizie. Aceasta nu aduce atingere valabilității actelor delegate aflate deja în vigoare. (4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European şi Consiliului. (5) Un act delegat adoptat în conformitate cu articolul 30 alineatul (4) intră în vigoare numai în cazul în care nici Parlamentul European şi nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea actului respectiv Parlamentului European şi Consiliului sau în cazul în care, înainte de expirarea termenului respectiv, Parlamentul European şi Consiliul au informat Comisia cu privire la faptul că nu vor formula obiecții. La inițiativa Parlamentului European sau a Consiliului, termenul respectiv se prelungește cu două luni.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

Articolul 48 **Procedura comitetului** (1) Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011. (2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
CAPITOLUL VI **DISPOZIȚII FINALE** **Articolul 49** **Revizuire** Comisia evaluează modul de aplicare a prezentului regulament și prezintă un raport în acest sens Parlamentului European și Consiliului cel mai târziu la 1 iulie 2020. Comisia evaluează, în special, dacă este oportun să se modifice domeniul de aplicare al prezentului regulament sau dispozițiile sale specifice, inclusiv articolul 6, articolul 7 litera (f), articolele 34, 43, 44 și 45, ținând seama de experiența dobândită în aplicarea prezentului regulament, precum și de evoluțiile tehnologice, ale pieței și juridice. Raportul menționat la primul paragraf este însoțit, după caz, de propuneri legislative. În plus, Comisia prezintă un raport Parlamentului European și Consiliului, o dată la patru ani, ulterior raportului menționat la primul paragraf, cu privire la progresele realizate în vederea atingerii obiectivelor prezentului regulament.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 50 **Abrogare** (1) Directiva 1999/93/CE se abrogă cu efect de la 1 iulie 2016. (2) Trimiterile la directiva abrogată se interpretează ca trimiteri la prezentul regulament.		**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		
Articolul 51 **Măsuri tranzitorii** (1) Dispozitivele sigure de creare a semnăturilor a căror conformitate a fost determinată în conformitate cu articolul 3 alineatul (4) din Directiva 1999/93/CE sunt considerate dispozitive de creare a semnăturilor	**c) Articolul 56. Dispoziții tranzitorii(4)** (1) Certificatele cheilor publice eliberate în baza Legii nr. 91/2014 privind semnătura electronică și documentul electronic rămân valabile până la expirarea termenului de valabilitate a acestora. (2) În termen de 18 luni de la data publicării prezentei	**Parțial compatibil**	Transpunerea integrală este condiționată de aderarea RM la UE		**SIS al RM**

electronice calificate în temeiul prezentului regulament. (2) Certificatele calificate emise pentru persoane fizice în conformitate cu Directiva 1999/93/CE sunt considerate drept certificate calificate pentru semnături electronice în temeiul prezentului regulament, până la expirarea lor. (3) Un prestator de servicii de certificare care eliberează certificate calificate în temeiul Directivei 1999/93/CE prezintă un raport de evaluare a conformității către organismul de supraveghere cât mai curând posibil, dar nu mai târziu de 1 iulie 2017. Până la prezentarea unui astfel de raport de evaluare a conformității și până la finalizarea de către organismul de supraveghere a evaluării sale, prestatorul de servicii de certificare respectiv este considerat ca fiind prestator de servicii de încredere calificat în temeiul prezentului regulament. (4) În cazul în care un prestator de servicii de certificare care eliberează certificate calificate în temeiul Directivei 1999/93/CE nu prezintă un raport de evaluare a conformității către organismul de supraveghere în termenul prevăzut la alineatul (3), respectivul prestator de servicii de certificare nu este considerat ca fiind prestator de servicii de încredere calificat în temeiul prezentului regulament începând cu data de 2 iulie 2017.	legi în Monitorul Oficial al Republicii Moldova, prestatorii de servicii de certificare a cheilor publice acreditați în baza Legii nr. 91/2014 privind semnătura electronică și documentul electronic sunt obligați să treacă procedura de acreditare în conformitate cu prevederile prezentei legi. (3) În cazul în care prestatorii de servicii de certificare a cheilor publice acreditați în baza Legii nr. 91/2014 privind semnătura electronică și documentul electronic nu trec procedura de acreditare în conformitate cu prevederile prezentei legi în termenul stabilit la alin. (2), acestora li se retrage certificatul de acreditare.				
Articolul 52 **Intrarea în vigoare** (1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene. (2) Prezentul regulament se aplică de la 1 iulie 2016, cu excepția următoarelor dispoziții: (a) articolul 8 alineatul (3), articolul 9 alineatul (5), articolul 12 alineatele (2)-(9), articolul 17 alineatul (8), articolul 19 alineatul (4), articolul 20 alineatul (4), articolul 21 alineatul (4), articolul 22 alineatul (5), articolul 23 alineatul (3), articolul 24 alineatul (5), articolul 27 alineatele (4) și (5), articolul 28 alineatul (6), articolul 29 alineatul (2), articolul 30 alineatele (3) și (4), articolul 31 alineatul (3), articolul 32 alineatul (3), articolul 33 alineatul (2), articolul 34 alineatul (2),	**Articolul 55. Dispoziții finale** (1) Prezenta lege intră în vigoare la expirarea a 6 luni de la data publicării în Monitorul Oficial al Republicii Moldova. (2) La data intrării în vigoare a prezentei legi se abrogă Legea nr. 91/2014 privind semnătura electronică și documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr.174-177, art. 397), cu modificările ulterioare. (3) Guvernul, în termen de 12 luni de la data publicării prezentei legi: a) va prezenta propuneri Parlamentului privind aducerea legislației în vigoare în concordanță cu prezenta lege; b) va aduce actele sale normative în concordanță cu prezenta lege;	**Norme UE neaplicabile**	Transpunerea este condiționată de aderarea RM la UE		

articolul 37 alineatele (4) şi (5), articolul 38 alineatul (6), articolul 42 alineatul (2), articolul 44 alineatul (2), articolul 45 alineatul (2) şi articolele 47 şi 48 se aplică de la 17 septembrie 2014; (b) articolul 7, articolul 8 alineatele (1) şi (2), articolele 9, 10, 11 şi articolul 12 alineatul (1) se aplică de la data aplicării actelor de punere în aplicare menţionate la articolul 8 alineatul (3) şi la articolul 12 alineatul (8); (c) articolul 6 se aplică după trei ani de la data aplicării actelor de punere în aplicare menţionate la articolul 8 alineatul (3) şi la articolul 12 alineatul (8). (3) În cazul în care sistemul de identificare electronică notificat este inclus în lista publicată de Comisie în conformitate cu articolul 9 înainte de data menţionată la alineatul (2) litera (c) de la prezentul articol, recunoaşterea mijloacelor de identificare electronică din cadrul sistemului respectiv în temeiul articolului 6 are loc cel târziu în termen de 12 luni de la publicarea respectivului sistem, dar nu înainte de data menţionată la alineatul (2) litera (c) de la prezentul articol. (4) Fără a aduce atingere alineatului (2) litera (c) de la prezentul articol, un stat membru poate decide ca mijloacele de identificare electronică din cadrul unui sistem de identificare electronică notificat în temeiul articolului 9 alineatul (1) de către un alt stat membru să fie recunoscute de primul stat membru de la data aplicării actelor de punere în aplicare menţionate la articolul 8 alineatul (3) şi la articolul 12 alineatul (8). Statele membre vizate informează Comisia. Comisia publică aceste informaţii. Prezentul regulament este obligatoriu în toate elementele sale şi se aplică direct în toate statele membre.	c) va elabora şi va adopta actele normative necesare pentru implementarea prezentei legi.				
ANEXA I **CERINŢE PENTRU CERTIFICATELE CALIFICATE PENTRU SEMNĂTURI ELECTRONICE** Certificatele calificate pentru semnături electronice conţin: (a) o indicaţie, cel puţin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice; (b) un set	**Articolul 24. Cerinţe pentru certificatele calificate pentru semnături electronice sau pentru sigilii electronice** Certificatele calificate pentru semnături electronice sau pentru sigilii electronice conţin: a) o indicaţie, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii	**Compatibil**			**SIS al RM**

de date care reprezintă fără ambiguitate prestatorul de servicii de încredere calificat care emite certificatele calificate, care includ cel puțin statul membru în care este stabilit prestatorul respectiv; și— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;— în cazul unei persoane fizice: numele persoanei; (c) cel puțin numele semnatarului sau un pseudonim; în cazul în care se utilizează un pseudonim, acesta este indicat în mod clar; (d) datele de validare a semnăturilor electronice care corespund datelor de creare a semnăturilor electronice; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; (f) codul de identitate al certificatului care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; (g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; (h) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (g) este disponibil gratuit; (i) localizarea serviciilor care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat; (j) în cazul în care datele de creare a semnăturilor electronice legate de datele de validare a semnăturilor electronice sunt situate într-un dispozitiv de creare a semnăturilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.	electronice; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale semnatarului sau creatorului sigiliului electronic; d) datele de validare a semnăturilor electronice sau sigiliilor electronice care corespund datelor de creare a acestora; e) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează; f) numărul unic de înregistrare a certificatului; g) date de verificare a certificatului calificat pentru semnătura electronică sau sigiliul electronic care corespund datelor de creare a acestora; h) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent, sau; i) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice recunoscute conform art. 3, sau; j) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere de nivel superior, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice ale prestatorilor de servicii de întredere acreditați.				
ANEXA II **CERINȚE PENTRU DISPOZITIVELE DE CREARE A SEMNĂTURILOR ELECTRONICE CALIFICATE** 1. Dispozitivele de creare a semnăturilor electronice calificate garantează, prin mijloace tehnice și procedurale adecvate, cel puțin că: (a) caracterul confidențial al datelor de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice este asigurat în mod rezonabil;	**Articolul 26. Cerințe pentru dispozitivele de creare a semnăturilor sau sigiliilor electronice** (1) Dispozitivele de creare a semnăturilor electronice sau sigiilor electronice avansate sau calificate trebuie să asigure, prin mijloace tehnice și proceduri corespunzătoare, cel puțin că: a) datele de creare a semnăturii sau a sigiliului electronic nu pot apărea decât o singură dată, iar confidențialitatea acestora este asigurată în	**Parțial compatibil**	Prevederile pct.3 și pct.4 nu sunt fundamentale, respectiv vor fi expuse în actele normative subordonate legii.		**SIS al RM**

(b) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturii electronice pot, practic, să apară numai o dată; (c) există suficiente asigurări că datele de creare a semnăturilor electronice utilizate pentru crearea semnăturilor electronice nu pot să fie descoperite prin deducție și că semnătura electronică este protejată în mod fiabil împotriva falsificării utilizând tehnologia disponibilă în prezent; (d) datele de creare a semnăturilor electronice utilizate pentru crearea semnăturilor electronice pot să fie protejate în mod fiabil de către semnatarul legitim împotriva utilizării de către alte persoane. 2. Dispozitivele de creare a semnăturilor electronice calificate nu modifică datele care urmează să fie semnate sau nu împiedică prezentarea lor semnatarului înainte de a semna. 3. Generarea sau gestionarea datelor de creare a semnăturilor electronice în numele semnatarului se pot realiza numai de către un prestator de servicii de încredere calificat. 4. Fără a aduce atingere punctului 1 litera (d), prestatorii de servicii de încredere calificați care gestionează datele de creare a semnăturilor electronice în numele semnatarului pot duplica datele de creare a semnăturilor electronice numai în scopul de a le avea de rezervă, cu condiția ca următoarele cerințe să fie îndeplinite: (a) securitatea seturilor de date duplicate trebuie să fie la același nivel ca pentru seturile de date originale; (b) numărul seturilor de date duplicate nu depășește minimul necesar pentru a asigura continuitatea serviciului.	conformitate cu prezenta lege; b) datele de creare a semnăturii electronice sau a sigiliului electronic nu pot fi deduse prin calcul și semnătura electronică sau sigiliul electronic sunt protejate împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată; c) datele de creare a semnăturii electronice sau a sigiliului electronic sunt protejate în mod fiabil de semnatarul sau creatorul legitim împotriva utilizării de către alte persoane; d) oferă posibilitatea afișării conținutului documentului electronic pe care se aplică semnătura electronică sau sigiliul electronic sau face referința irevocabilă la documentul dat; e) semnătura electronică sau sigiliul electronic este creat numai după confirmarea de către semnatar sau creatorul unui sigiliu a operațiunii de creare a semnăturii electronice sau a sigiliului electronic; f) confirmă în mod univoc crearea semnăturii sau a sigiliului electronic. (2) Dispozitivele de creare a semnăturii electronice sau a sigiliului electronic avansate sau calificate nu trebuie să modifice datele asupra cărora se aplică semnătura electronică sau sigiliul electronic avansat sau calificat, sau să împiedice prezentarea lor semnatarului sau creatorului înainte de semnare sau aplicare a sigiliului.				
ANEXA III **CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU SIGILIILE ELECTRONICE** Certificatele calificate pentru sigiliile electronice conțin: (a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru sigilii electronice; (b) un set de date care reprezintă fără ambiguitate prestatorul de servicii	**Articolul 24. Cerințe pentru certificatele calificate pentru semnături electronice sau pentru sigilii electronice** Certificatele calificate pentru semnături electronice sau pentru sigilii electronice conțin: a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru semnături electronice sau sigilii	**Compatibil**			**SIS al RM**

de încredere calificat care emite certificatele calificate, care include cel puțin statul membru în care este stabilit prestatorul respectiv; și— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale;— în cazul unei persoane fizice: numele persoanei; (c) cel puțin numele creatorului sigiliului și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale; (d) datele de validare a sigiliilor electronice, care corespund datelor de creare a sigiliilor electronice; (e) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; (f) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; (g) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; (h) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (g) este disponibil gratuit; (i) localizarea serviciilor care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat; (j) în cazul în care datele de creare a sigiliilor electronice legate de datele de validare a sigiliilor electronice sunt situate într-un dispozitiv de creare a sigiliilor electronice calificat, o indicație corespunzătoare referitoare la aceasta, cel puțin într-o formă adecvată pentru prelucrarea automată.	electronice; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate; c) datele de identificare și alte date ale semnatarului sau creatorului sigiliului electronic; d) datele de validare a semnăturilor electronice sau sigiliilor electronice care corespund datelor de creare a acestora; e) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează; f) numărul unic de înregistrare a certificatului; g) date de verificare a certificatului calificat pentru semnătura electronică sau sigiliul electronic care corespund datelor de creare a acestora; h) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent, sau; i) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice recunoscute conform art. 3, sau; j) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere de nivel superior, în cazul certificatelor calificate pentru semnături electronice sau pentru sigilii electronice ale prestatorilor de servicii de întredere acreditați.				
ANEXA IV **CERINȚE PENTRU CERTIFICATELE CALIFICATE PENTRU AUTENTIFICAREA UNUI SITE INTERNET** Certificatele calificate pentru autentificarea unui site internet conțin: (a) o indicație, cel puțin într-o formă adecvată pentru prelucrarea automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unui site internet; (b) un set de date care reprezintă fără ambiguitate	**Articolul 33. Cerințe pentru certificatele calificate pentru autentificarea unei pagini web** Certificatele calificate pentru autentificarea unei pagini web trebuie să conțină: a) o indicație, într-o formă pasibilă de prelucrare automată, că certificatul a fost emis ca certificat calificat pentru autentificarea unei pagini web; b) datele de identificare ale prestatorului de servicii de încredere calificat care emite certificatele calificate;	**Compatibil**			**SIS al RM**

prestatorul de servicii de încredere calificat care emite certificatele calificate, care include cel puțin statul membru în care este stabilit prestatorul respectiv; și— în cazul unei persoane juridice: denumirea și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale,— în cazul unei persoane fizice: numele persoanei; (c) în cazul persoanelor fizice: cel puțin numele persoanei căreia i s-a eliberat certificatul sau un pseudonim. În cazul în care se utilizează un pseudonim, acesta este indicat în mod clar;în cazul persoanelor juridice: cel puțin denumirea persoanei juridice căreia i se eliberează certificatul și, după caz, numărul de înregistrare astfel cum se menționează în registrele oficiale; (d) elemente ale adresei persoanei fizice sau juridice căreia i s-a eliberat certificatul, incluzând cel puțin orașul și statul, și, dacă este cazul, în forma în care sunt înscrise în registrele oficiale; (e) numele domeniului (domeniilor) gestionat(e) de persoana fizică sau juridică căreia i s-a emis certificatul; (f) detalii privind începutul și sfârșitul perioadei de valabilitate a certificatului; (g) codul de identitate al certificatului, care trebuie să fie unic pentru prestatorul de servicii de încredere calificat; (h) semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent; (i) locul în care certificatul care stă la baza semnăturii electronice avansate sau a sigiliului electronic avansat menționate la litera (h) este disponibil gratuit; (j) localizarea serviciilor privind statutul valabilității certificatului care pot fi utilizate pentru a cunoaște statutul valabilității certificatului calificat.	c) datele de identificare și alte date ale titularului certificatului cheii publice, precum și informațiile necesare pentru comunicarea cu acesta; d) data și ora la care începe să curgă termenul de valabilitate a certificatului și data și ora la care acest termen încetează; e) numele domeniului (domeniilor) gestionate de titularul certificatului cheii publice căruia i s-a emis certificatul; f) numărul unic de înregistrare a certificatului; g) semnătura electronică calificată sau sigiliul electronic calificat al prestatorului de servicii de încredere calificat emitent sau semnătura electronică avansată sau sigiliul electronic avansat al prestatorului de servicii de încredere calificat emitent cu domiciliul sau cu sediul într-un alt stat, în cazul certificatelor calificate pentru autentificarea unei pagini web recunoscute conform art. 3; h) date de verificare a certificatului calificat pentru autentificarea unei pagini web care corespund datelor de creare a acestuia.				