

ОБРАЗАЦ ИЗЈАВЕ О УСКЛАЂЕНОСТИ ПРОПИСА СА ПРОПИСИМА ЕВРОПСКЕ УНИЈЕ

1. Орган државне управе, односно други овлашћени предлагач прописа:

Министарство информисања и телекомуникација

2. Назив прописа

Нацрт Закона о о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању

Draft Law on Electronic Documents, Electronic Identification and Trust Services for Electronic Transactions

3. Усклађеност прописа с одредбама Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране („Службени гласник РС“, број 83/08) (у даљем тексту: Споразум):

а) Одредба Споразума која се односе на нормативну садржину прописа

Члан 105. Информационо друштво - Споразум о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране.

б) Прелазни рок за усклађивање законодавства према одредбама Споразума

Три године.

в) Оцена испуњености обавезе које произлазе из наведене одредбе Споразума

Испуњава у потпуности.

г) Разлози за делимично испуњавање, односно неиспуњавање обавеза које произлазе из наведене одредбе Споразума

/

д) Веза са Националним програмом за усвајање правних тековина Европске уније

/

4. Усклађеност прописа са прописима Европске уније:

а) Навођење одредби примарних извора права Европске уније и оцене усклађености са њима

/

б) Навођење секундарних извора права Европске уније и оцене усклађености са њима

/

в) Навођење осталих извора права Европске уније и усклађеност са њима

/

г) Разлози за делимичну усклађеност, односно неусклађеност

/

д) Рок у којем је предвиђено постизање потпуне усклађености прописа са прописима Европске уније

/

5. Уколико не постоје одговарајуће надлежности Европске уније у материји коју регулише пропис, и/или не постоје одговарајући секундарни извори права Европске уније са којима је потребно обезбедити усклађеност, потребно је образложити ту чињеницу. У овом случају, није потребно попуњавати Табелу усклађености прописа. Табелу усклађености није потребно попуњавати и уколико се домаћим прописом не врши пренос одредби секундарног извора права Европске уније већ се искључиво врши примена или спровођење неког захтева који произилази из одредбе секундарног извора права (нпр. Предлогом одлуке о изради стратешке процене утицаја биће спроведена обавеза из члана 4. Директиве 2001/42/ЕЗ, али се не врши и пренос те одредбе директиве).

/

6. Да ли су претходно наведени извори права Европске уније преведени на српски језик?

/

7. Да ли је пропис преведен на неки службени језик Европске уније?

/

8. Сарадња са Европском унијом и учешће консултаната у изради прописа и њихово мишљење о усклађености

/

Београд, 22.12.2025. године



ИЗЈАВА
О ОСТВАРЕНОЈ САРАДЊИ, ОДНОСНО ПРИБАВЉАЊУ МИШЉЕЊА ОД
ОРГАНА, ОРГАНИЗАЦИЈА И ТЕЛА

Не постоје посебни прописи према којима би Министарство информисања и телекомуникација било обавезно да успостави сарадњу, односно прибави мишљења од органа, организација и тела у складу са чланом 39а став 4. Пословника Владе („Службени гласник РС”, бр. 61/06-пречишћен текст, 69/08, 88/09, 33/10, 69/10, 20/11, 37/11, 30/13, 76/14 и 8/2019 – др. уредба), приликом израде Предлог закључка о спровођењу јавне расправе о Нацрту Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању.

ИЗЈАВА
ДА ЛИ ЈЕ ПРЕДЛОГ ЗАКЉУЧКА ПЛАНИРАН
ГОДИШЊИМ ПЛАНОМ РАДА ВЛАДЕ

Предлог закључка о спровођењу јавне расправе о Нацрту Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању није предвиђен Годишњим планом Владе за 2025. годину.

Наведени акт се предлаже с обзиром да постојећи законски оквир више не обезбеђује довољно флексибилности и обухватности у домену електронске идентификације, електронског потписа и других услуга од поверења, посебно у контексту развоја дигиталног идентитета и увођења дигиталног идентификационог новчаника као кључног механизма за једноставно и сигурно електронско пословање.

Предлог закључка о спровођењу јавне расправе о Нацрту Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању усклађен је са Реформском агендом Републике Србије, као стратешким документом Владе, којим су дефинисани кључни правци и приоритети реформских процеса у оквиру приступања Европској унији.

ИЗЈАВА СА КОЈИМ ЈЕ СТРАТЕШКИМ ДОКУМЕНТОМ ВЛАДЕ
(СТРАТЕГИЈА, АКЦИОНИ ПЛАН И ДРУГО)
УСКЛАЂЕН АКТ КОЈИ СЕ ПРЕДЛАЖЕ

Предлог закључка о спровођењу јавне расправе о Нацрту Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању усклађен је са Реформском агендом Републике Србије, као стратешким документом Владе, којим су дефинисани кључни правци и приоритети реформских процеса у оквиру приступања Европској унији.

1. Назив прописа Европске уније :	2. „CELEX” ознака ЕУ прописа
REGULATION (EU) No 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework - Regulation on electronic identification and trust services for electronic transactions in the internal market 2.0 (EIDAS 2.0)	32024R1183
Уредба Европског парламента и Европског савета број 2024/1183 од 11. априла 2024. године којом се мења Уредба (ЕУ) бр. 910/2014 у погледу успостављања Европског оквира за дигитални идентитет - Уредба о електронској идентификацији и услугама поверења за електронске трансакције на унутрашњем тржишту 2.0 (EIDAS 2.0)	
3. Орган државне управе, односно други овлашћени предлагач прописа:	4. Датум израде табеле:
Министарство информисања и телекомуникација	29.10.2025. године
5. Назив (нацрта, предлога) прописа чије одредбе су предмет анализе усклађености са прописом Европске уније:	6. Бројане ознаке (шифре) планираних прописа из базе НПАА: 2024-436
Нацрт закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању	

7. Усклађеност одредби прописа са одредбама прописа ЕУ:

а)	а1)	б)	б1)	в)	г)	д)
Одредба прописа ЕУ	Садржина одредбе	Одредбе прописа Р. Србије	Садржина одредбе	Уск ¹	Разлози за делимичну усклађеност, неусклађеност или непреносивост	Напомена о усклађен.
1.1.1.a	This Regulation aims to ensure the proper functioning of the internal market and the provision of an adequate level of security of electronic identification means and trust services used across the Union, in order to enable and facilitate the exercise by natural and legal persons of the right to participate in digital society safely and to access online public and private services throughout the Union. For those purposes, this Regulation: (a) lays down the conditions under which Member States are to recognise natural and legal persons' electronic identification means falling under a notified electronic identification scheme of another Member State			НП	Одредбом је утврђено да ова уредба регулише услове на основу којих државе чланице признају средства електронске идентификације физичких и правних лица која се користе у оквиру шеме електронске идентификације друге државе чланице. Имајући у виду да Република Србија није чланица ЕУ, оваква одредба није преносива.	

¹ Потпуно усклађено - ПУ, делимично усклађено - ДУ, неусклађено - НУ, непреносиво – НП

a)	a1)	6)	61)	в)	г)	д)
1.1.1.b	(b) lays down rules for trust services, in particular for electronic transactions; and	1.	Овим законом уређује се електронски документ, електронска идентификација и услуге од поверења у електронском пословању.	ПУ		
1.1.1.c	(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving, electronic attestation of attributes, electronic signature creation devices, electronic seal creation devices, and electronic ledgers	1.	Овим законом уређују се електронски документ, електронска идентификација и услуге од поверења у електронском пословању.	ПУ		
2.1.	This Regulation applies to electronic identification schemes notified by a Member State, to European Digital Identity Wallets provided by a Member State and to trust service providers established in the Union.			НП	Одредба је непреносива у пропис Републике Србије, јер се њом одређује примена уредбе у државама чланицама Европске уније.	
2.2.	This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.	3.2.	Одредбе овог закона се не примењују на услуге од поверења које се пружају у оквиру ограниченог круга учесника и немају утицај на треће стране.	ПУ		
2.3.	This Regulation does not affect Union or national law related to the conclusion and validity of contracts, other legal or procedural obligations relating to form, or sector-specific requirements relating to form.			НП	Одредба је непреносива, јер се односи на домаћај примене ове уредбе када је правом ЕУ или националним правом предвиђена посебна форма за уговоре и друге акте.	
2.4.	This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council.			НП	Одредба је непреносива, јер се односи на домаћај примене ове уредбе када је правом ЕУ или националним правом предвиђена посебна форма за уговоре и друге акте.	
3.1.1.	For the purposes of this Regulation, the following definitions apply: 'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural	2.1.12.	електронска идентификација је поступак коришћења идентификационих података у електронском облику који недвосмислено одређују правно лице, физичко лице, или физичко лице у својству регистрованог субјекта, као и њиховог заступника	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	person representing another natural person or a legal person;					
3.1.2.	‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;	2.1.13.	средство електронске идентификације је материјално, односно нематеријално средство које садржи идентификационе податке и којим се врши аутентификација лица	ПУ		
3.1.3.	‘person identification data’ means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person;	2.1.11.	идентификациони подаци представљају скуп података на основу којих је могуће недвосмислено утврдити идентитет правног лица, физичког лица, или физичког лица у својству регистрованог субјекта, као и њиховог заступника	ПУ		
3.1.4.	‘electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons;	2.1.13.	шема електронске идентификације је систем издавања средства електронске идентификације правном лицу, физичком лицу или физичком лицу у својству регистрованог субјекта	ПУ		
3.1.5.	‘authentication’ means an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form;	2.1.10.	аутентификација је процес који обезбеђује потврду електронске идентификације правног лица, физичког лица, или физичког лица у својству регистрованог субјекта, или потврду интегритета и порекла података у електронској форми	ПУ		
3.1.5a	‘user’ means a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation;	2.1.9	корисник је правно или физичко лице, физичко лице у својству регистрованог субјекта, као и њихов заступник, који користи услуге од поверења или средства електронске идентификације у складу са овим законом	ПУ		
3.1.6.	‘relying party’ means a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service;	2.1.19.	поуздајућа страна је правно или физичко лице које, се поуздаје у услугу електронске идентификације, дигитални идентификациони новчаник или друго средство електронске идентификације, односно услугу од поверења	ПУ		
3.1.7.	‘public sector body’ means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or	2.1.7.	орган јавне власти је државни орган и организација, орган и организација аутономне покрајине, орган и организација јединице локалне самоуправе, јавно	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;		предузеће, установа, посебни орган преко кога се остварује регулаторна функција и правно и физичко лице коме је поверено јавно овлашћење			
3.1.8.	'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council;	2.1.7.	орган јавне власти је државни орган и организација, орган и организација аутономне покрајине, орган и организација јединице локалне самоуправе, јавно предузеће, установа, посебни орган преко кога се остварује регулаторна функција и правно и физичко лице коме је поверено јавно овлашћење	ПУ		
3.1.9.	'signatory' means a natural person who creates an electronic signature;	2.1.28.	потписник је физичко лице које је креирало електронски потпис и чији су идентификациони подаци садржани у сертификату на основу кога је креиран тај електронски потпис, то јест сертификату којим се потврђује веза између идентитета тог потписника и података за валидацију електронског потписа	ПУ		
3.1.10.	'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;	2.1.22.	електронски потпис је скуп података у електронском облику који су придружени или логички повезани са другим подацима у електронским облику, а које потписник користи за потписивање	ПУ		
3.1.11.	'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26	2.1.34.	напредни електронски потпис је електронски потпис који испуњава додатне услове за обезбеђивање вишег нивоа поузданости потврђивања интегритета података и идентитета потписника у складу са овим законом	ПУ		
3.1.12.	'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;	2.1.35.	квалификовани електронски потпис је напредни електронски потпис који је креиран квалификованим средством за креирање електронског потписа и који се заснива на квалификованом сертификату за електронски потпис и који је издат од стране пружаоца квалификоване услуге од поверења у складу са овим законом	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
3.1.13.	'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature	2.1.24.	подаци за креирање електронског потписа односно печата су јединствени подаци које користи потписник односно печатилац за креирање електронског потписа односно печата и који су логички повезани са одговарајућим подацима за валидацију електронског потписа односно печата	ПУ		
3.1.14.	'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person	2.1.26.	сертификат за електронски потпис је електронска потврда којом се потврђује веза између података за валидацију електронског потписа и идентитета потписника, потврђујући најмање лично име или псеудоним потписника	ПУ		
3.1.15.	'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;	2.1.37.	квалификовани сертификат за електронски потпис је сертификат за електронски потпис који издаје пружалац квалификоване услуге од поверења и који испуњава услове предвиђене овим законом	ПУ		
3.1.16.a-n.	'trust service' means an electronic service normally provided for remuneration which consists of any of the following: (a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; (c) the creation of electronic signatures or electronic seals; (d) the validation of electronic signatures or electronic seals; (e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;	2.1.17. 48.1-2.	услуга од поверења је електронска услуга која олакшава пословну активност између две или више страна којом пружалац услуге странама гарантује веродостојност података, а која је као таква одређена овим законом; Услуге од поверења се пружају у областима: 1) електронског потписа и електронског печата; 2) електронског временског жига; 3) електронске доставе; 4) аутентификације веб сајтова; 5) електронског архивирања; 6) електронске потврде атрибута; 7) вођења електронских евиденција. Квалификоване услуге од поверења су: 1) издавање квалификованих сертификата за електронски потпис;	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(f) the management of remote electronic signature creation devices or remote electronic seal creation devices; (g) the issuance of electronic attestations of attributes; (h) the validation of electronic attestations of attributes; (i) the creation of electronic timestamps; (j) the validation of electronic timestamps; (k) the provision of electronic registered delivery services; (l) the validation of data transmitted through electronic registered delivery services and related evidence; (m) the electronic archiving of electronic data and electronic documents; (n) the recording of electronic data in an electronic ledger;	6)	2) услуга управљања квалификованим средством за креирање електронског потписа на даљину; 3) услуга валидације квалификованог електронског потписа; 4) издавање квалификованих сертификата за електронски печат; 4б) услуга чувања квалификованог електронског потписа; 5) услуга управљања квалификованим средством за креирање електронског печата на даљину; 6) услуга валидације квалификованог електронског печата; 6а) услуга чувања квалификованог електронског печата; 7) издавање квалификованих електронских временских жигова; 8) услуга квалификоване електронске доставе; 9) услуга издавања квалификованих сертификата за аутентификацију веб сајтова; 9а) услуга издавања квалификованих електронских потврда атрибута; 10) услуга квалификованог електронског архивирања; 10а) услуга вођења електронске евиденције			
3.1.17.	'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;	2.1.20.	квалификована услуга од поверења је услуга од поверења која испуњава услове утврђене овим законом за квалификовану услугу од поверења	ПУ		
3.1.18.	'conformity assessment body' means a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or	2.1.53.	тело за оцењивање усаглашености је правно лице или део правног лица које је овлашћено да обавља послове оцењивања усаглашености пружаоца квалификоване услуге од поверења и квалификоване услуге од поверења коју он пружа са условима за пружање квалификованих услуга од	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	as competent to carry out certification of European Digital Identity Wallets or electronic identification means;		поверења, као и оцењивање усаглашености дигиталног идентификационог новчаника или другог средстава електронске идентификације, у складу са овим законом и законом којим се уређују технички захтеви за производе и оцењивање усаглашености, односно поступак акредитације и примену релевантних стандарда			
3.1.19.	'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider	2.1.18.	пужалац услуга од поверења је правно лице, или физичко лице у својству регистрованог субјекта које пружа једну или више услуга од поверења	ПУ		
3.1.20.	'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;	2.1.21.	пужалац квалификоване услуге од поверења је правно лице, или физичко лице у својству регистрованог субјекта које пружа једну или више квалификованих услуга од поверења, у складу са овим законом	ПУ		
3.1.21.	'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of electronic identification and trust services;	2.1.6.	производ је хардвер, софтвер односно хардвер са припадајућим софтвером, или њихове одговарајуће компоненте, намењен електронској обради, електронском преносу односно чувању података који омогућава пружање услуга електронске идентификације и услуга од поверења	ПУ		
3.1.22.	'electronic signature creation device' means configured software or hardware used to create an electronic signature;	2.1.30.	средство за креирање електронског потписа односно печата је техничко средство (софтвер односно хардвер) које се користи за креирање електронског потписа односно печата уз коришћење података за креирање електронског потписа односно печата	ПУ		
3.1.23.	qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;	2.1.32.	квалификовано средство за креирање електронског потписа је средство које испуњава услове прописане овим законом	ПУ		
3.1.23a.	'remote qualified electronic signature creation device' means a qualified electronic signature creation device that is managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory;	2.1.31.	квалификовано средство за креирање електронског потписа на даљину је квалификовано средство за креирање електронског потписа којим у име потписника управља пружалац квалификованих услуга од поверења у складу са овим законом	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
3.1.23b.	'remote qualified electronic seal creation device' means a qualified electronic seal creation device that is managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;	2.1.32.	квалификовано средство за креирање електронског печата на даљину је квалификовано средство за креирање електронског печата којим у име печатниоца управља пружалац квалификованих услуга од поверења у складу са овим законом	ПУ		
3.1.24.	'creator of a seal' means a legal person who creates an electronic seal	2.1.29.	печатилац је правно лице, физичко лице у својству регистраног субјекта, физичко лице коме је поверено вршење јавних овлашћења или физичко лице које у обављању делатности у складу са посебним прописима има право на коришћење печата (нпр. лица која имају лиценцу за вршење послова или обављање делатности), за чије потребе се креира електронски печат и чији су идентификациони подаци наведени у сертификату на основу кога је креиран тај електронски печат, односно у сертификату којим се потврђује веза између идентитета тог печатниоца и података за валидацију електронског печата	ПУ		
3.1.25.	'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity	2.1.23.	електронски печат је скуп података у електронском облику који су придружени или логички повезани са другим подацима у електронском облику, а које печатилац користи за печатање	ПУ		
3.1.26.	'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;	2.1.38.	напредни електронски печат је електронски печат који испуњава додатне услове за обезбеђивање вишег нивоа поузданости потврђивања интегритета података и идентитета печатниоца у складу са овим законом	ПУ		
3.1.27.	'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;	2.1.39.	квалификовани електронски печат је напредни електронски печат који је креиран квалификованим средством за креирање електронског печата и који је заснован на квалификованом сертификату за електронски печат	ПУ		
3.1.28.	'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;	2.1.24.	подаци за креирање електронског потписа односно печата су јединствени подаци које користи потписник односно печатилац за креирање електронског потписа односно печата и који су	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			логички повезани са одговарајућим подацима за валидацију електронског потписа односно печата			
3.1.29.	'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;	2.1.26.	сертификат за електронски потпис односно печат је електронска потврда којом се потврђује веза између података за валидацију електронског потписа и идентитета потписника, потврђујући најмање лично име или псеудоним потписника	ПУ		
3.1.30.	'qualified certificate for electronic seal' means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;	2.1.41.	квалификовани сертификат за електронски печат је сертификат за електронски печат који издаје пружалац квалификоване услуге од поверења и који испуњава услове предвиђене овим законом	ПУ		
3.1.31.	'electronic seal creation device' means configured software or hardware used to create an electronic seal;	2.1.30.	средство за креирање електронског потписа односно печата је техничко средство (софтвер, односно хардвер) које се користи за креирање електронског потписа, односно печата уз коришћење података за креирање електронског потписа односно печата	ПУ		
3.1.32.	'qualified electronic seal creation device' means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II	2.1.40.	квалификовано средство за креирање електронског печата је средство које испуњава услове прописане овим законом	ПУ		
3.1.33.	'electronic time stamp' means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time	2.1.46.	електронски временски жиг је време придружено подацима у електронском облику којим се потврђује да су ти подаци постојали у том временском тренутку	ПУ		
3.1.34.	'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42	2.1.47.	квалификовани електронски временски жиг је електронски временски жиг који испуњава услове утврђене овим законом	ПУ		
3.1.35.	'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording	2.1.4.	електронски документ је скуп података састављен од слова, бројева, симбола, графичких, звучних и видео материјала, у електронском облику	ПУ		
3.1.36.	'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence	2.1.48.	услуга електронске доставе је услуга преноса података електронским путем у оквиру које пружалац услуга обезбеђује доказе о поступању са	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;		пренесеним подацима, укључујући доказ слања и пријема података, којом се пренесени подаци штите од ризика губитка, крађе, оштећења односно било којих неовлашћених промена			
3.1.37.	'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44	2.1.49.	услуга квалификоване електронске доставе је услуга пружаоца квалификоване услуге од поверења која испуњава услове за квалификовану електронску доставу утврђене овим законом	ПУ		
3.1.38.	'certificate for website authentication' means an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;	2.1.44.	сертификат за аутентикацију веб сајта је потврда помоћу које је могуће извршити аутентификацију веб сајта и којом се веб сајт повезује са идентитетом физичког или правног лица коме је сертификат издат	ПУ		
3.1.39.	'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;	2.1.45.	квалификовани сертификат за аутентикацију веб сајта је сертификат за аутентификацију веб сајта коју издаје пружалац квалификоване услуге од поверења и испуњава услове предвиђене овим законом	ПУ		
3.1.40.	'validation data' means data that is used to validate an electronic signature or an electronic seal	2.1.25.	подаци за валидацију електронског потписа односно печата су подаци који се користе за валидацију, односно проверу и потврђивање исправности електронског потписа, односно печата	ПУ		
3.1.41.	'validation' means the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation;	2.1.33.	валидација је поступак провере и потврђивања исправности података у електронском облику у складу са овим законом	ПУ		
3.1.42.	'European Digital Identity Wallet' means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals;	2.1.54.	дигитални идентификациони новчаник је средство електронске идентификације које омогућава кориснику да на безбедан начин чува, управља и валидира личне идентификационе податке и електронске потврде атрибута, са циљем да их прикажује поузданим странама и другим корисницима дигиталног идентификационог новчаника, као и да омогући корисницима употребу квалификованог електронског потписа, односно печата	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
3.1.43.	'attribute' means a characteristic, quality, right or permission of a natural or legal person or of an object;	2.1.55.	атрибут је својство, карактеристика, квалитет, право или овлашћење физичког или правног лица, као и својство, односно карактеристика материјалног или нематеријалног објекта, односно ствари	ПУ		
3.1.44.	'electronic attestation of attributes' means an attestation in electronic form that allows attributes to be authenticated;	2.1.56.	електронска потврда атрибута је потврда у електронском облику којом се на поуздан начин омогућава аутентификација атрибута	ПУ		
3.1.45.	'qualified electronic attestation of attributes' means an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;	2.1.57.	квалификована електронска потврда атрибута је електронска потврда атрибута коју издаје пружалац квалификоване услуге од поверења, а која испуњава услове утврђене овим законом	ПУ		
3.1.46.	'electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source' means an electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII;	2.1.58.	електронска потврда атрибута органа јавне власти је електронска потврда издата од стране или у име органа јавне власти надлежног за вођење или управљање евиденцијом, односно регистром који је извор података о атрибутима, у складу са законом	ПУ		
3.1.47.	'authentic source' means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice;	2.1.59.	извор података о атрибутима је евиденција, односно регистар и други аутентичан извор који садржи податке о атрибутима физичког или правног лица, односно објекта и који је одређен као извор тих података	ПУ		
3.1.48.	'electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;	2.1.61.	услуга електронског архивирања је услуга која обезбеђује пријем, складиштење, претрагу и брисање електронских података и електронских докумената у циљу обезбеђења њихове трајности и употребљивости, као и очувања њиховог интегритета, поверљивости и доказа о пореклу током читавог периода чувања	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
3.1.49.	'qualified electronic archiving service' means an electronic archiving service which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45j;	2.1.62.	квалификовано електронско архивирање је услуга електронског архивирања коју врши пружалац квалификоване услуге од поверења и која испуњава услове утврђене овим законом	ПУ		
3.1.50.	'EU Digital Identity Wallet Trust Mark' means a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;			НП	Одредба је непреносива у пропис Републике Србије, јер се њом одређује примена уредбе у државама чланицама Европске уније.	
3.1.51.	'strong user authentication' means an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inheritance, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;	2.1.63.	аутентификација вишег нивоа поузданости корисника је аутентификација заснована на употреби најмање два фактора аутентификације из различитих категорија који означавају нешто што само корисник зна, поседује или што корисник јесте, а који су међусобно независни, тако да компромитовање једног фактора не угрожава поузданост осталих, и која је креирана тако да штити поверљивост података за аутентификацију	ПУ		
3.1.52.	'electronic ledger' means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records;	2.1.64.	услуга вођења електронске евиденције означава бележење низа електронских записа података, којима се обезбеђује интегритет тих записа и тачност хронолошког редоследа бележења тих записа	ПУ		
3.1.53.	'qualified electronic ledger' means an electronic ledger which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45l;	2.1.65.	квалификована услуга вођења електронске евиденције је услуга пружаоца квалификоване услуге од поверења која испуњава услове утврђене овим законом	ПУ		
3.1.54.	'personal data' means any information as defined in Article 4, point (1), of Regulation (EU) 2016/679;	2.1.66.	податак о личности је сваки податак у смислу закона којим се уређује заштита података о личности	ПУ		
3.1.55.	'identity matching' means a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person;	2.1.67.	упаривање идентитета је процес у којем се подаци за идентификацију лица или средства за електронску идентификацију упоређују или повезују са постојећим налогом који припада том лицу	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
3.1.56.	'data record' means electronic data recorded with related meta- data supporting the processing of the data;	2.1.68.	запис података су подаци у електронском облику који су забележени са повезаним метаподацима који подржавају обраду тих података, у смислу овог закона	ПУ		
3.1.57.	'offline mode' means, as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.	2.1.69.	режим „ван мреже” омогућава коришћење дигиталног идентификационог новчаника без потребе за повезивањем са удаљеним системима преко електронских комуникационих мрежа, при чему се интеракција између корисника и треће стране на физичкој локацији врши уз употребу технологија кратког домета	ПУ		
4.1.	There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.			НП	Одредба је непреносива, јер уређује питање пружања услуга од поверења на територији државе чланице ЕУ у случају када пружалац није основан у тој држави чланици.	
4.2.	Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.			НП	Одредба је непреносива, јер уређује промет услуга од поверења на унутрашњем тржишту Европске уније.	
5.1.	Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited.	4.6.	У оквиру електронске трансакције стране се могу представљати псеудонимом уколико прописом, уговором или на други обавезујући начин није другачије одређено.	ПУ		
5a.1-3.	For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6). European Digital Identity Wallets shall be provided in one or more of the following ways:			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније.	

a)	a1)	б)	б1)	в)	г)	д)
	(a) directly by a Member State; (b) under a mandate from a Member State; (c) independently of a Member State but recognised by that Member State. The source code of the application software components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed.					
5a.4.	European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: (a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible; (b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet; (c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets; (d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to: (i) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged; (ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679;	15.1	Дигитални идентификациони новчаник омогућава кориснику да на једноставан и транспарентан начин: 1) под искључивом контролом корисника, на безбедан начин захтева, добија, бира, комбинује, чува, брише, дели и представља личне идентификационе податке, и када је то потребно, у комбинацији са електронском потврдом атрибута, да се аутентификује поуздајућим странама, у режиму рада на мрежи и када је то прикладно, у режиму рада ван мреже, ради приступања јавним и приватним услугама, уз могућност селективног откривања података; 2) креира псеудониме и чува их у криптованом облику, локално, на свом уређају, у оквиру дигиталног идентификационог новчаника; 3) безбедно изврши аутентификацију дигиталног идентификационог новчаника другог лица, прима и дели личне идентификационе податке и електронске потврде атрибута, на сигуран начин, између два дигитална идентификациона новчаника; 4) приступи евиденцији свих трансакција извршених употребом дигиталног идентификационог новчаника, коришћењем контролне табле дигиталног идентификационог новчаника, која кориснику омогућава да: 5) прегледа ажуран попис поуздајућих страна са којима је посредством дигиталног	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received; (e) sign by means of qualified electronic signatures or seal by means of qualified electronic seals; (f) download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations; (g) exercise the user's rights to data portability.		идентификационог новчаника остварио конекцију, а где је то могуће и све размењене податке; б) на једноставан начин захтева да поуздајућа страна обрише његове податке о личности у складу са законом којим се уређује заштита података о личности; 7) на једноставан начин пријави поуздајућу страну органу надлежном за заштиту података о личности, ако посумња да је примио незаконит или сумњив захтев за подацима; 8) врши потписивање коришћењем квалификованог електронског потписа, односно печатирање коришћењем квалификованог електронског печата; 9) преузме, у мери у којој је то технички изводљиво, податке корисника, електронске потврде атрибута и конфигурације; 10) остварује право корисника на преносивост података.			
5a.5.	European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: (i) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet; (ii) for relying parties to request and validate person identification data and electronic attestations of attributes; (iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode; (iv) for the user to allow interaction with the European Digital Identity Wallet and display an EU Digital Identity Wallet Trust Mark; (v) to securely onboard the user by using an electronic identification means in accordance with Article 5a(24);	15.2	Дигитални идентификациони новчаник посебно треба да: 1) подржава опште протоколе и интерфејсе: (1) за издавање личних идентификационих података, квалификованих и неквалификованих електронских потврда атрибута, или квалификованих и неквалификованих електронских сертификата дигиталном идентификационом новчанику; (2) како би се поуздајућој страни омогућило да захтева и потврђује валидност личних идентификационих података и електронских потврда атрибута; (3) за дељење и приказивање поуздајућој страни личних идентификационих података, електронских потврда атрибута, или селективно откривених података, у режиму рада на мрежи и када је то прикладно, у режиму рада ван мреже; (4) омогући безбедно укључивање корисника, употребом средстава електронске идентификације	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner; (vii) for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b; (viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets; (ix) for requesting a relying party the erasure of personal data pursuant to Article 17 of Regulation (EU) 2016/679; (x) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received; (xi) for the creation of qualified electronic signatures or electronic seals by means of qualified electronic signature or electronic seal creation devices; (b) not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations; (c) ensure that the relying parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article 5b; (d) meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication; (e) in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation; (f) ensure that the person identification data, which is available from the electronic identification scheme		високог нивоа поузданости, у складу са овим законом; (5) за комуникацију дигиталних идентификационих новчаника два корисника, у сврху безбедног преузимања, валидације и размене личних идентификационих података и електронских потврда атрибута; (6) за аутентификацију и идентификацију поуздајућих страна, кроз успостављање аутентификационих механизма утврђених овим законом; (7) како би се поуздајућим странама омогућила провера аутентичности и валидности дигиталних идентификационих новчаника; (8) како би се од поуздајуће стране могло захтевати брисање личних идентификационих података, у складу са законом којим се уређује заштита података о личности; (9) за пријаву поуздајуће стране органу надлежном за заштиту података о личности, у случају сумње да је примљен незаконит или сумњив захтев за подацима; (10) за креирање квалификованог електронског потписа, односно печата, употребом квалификованог средства за креирање електронског потписа, односно печата; 2) пружаоцима услуга од поверења који издају електронске потврде атрибута не пружа информације о употреби тих потврда коришћењем дигиталног идентификационог новчаника; 3) обезбеђује аутентификацију и идентификацију поуздајућих страна, кроз успостављање аутентификационих механизма утврђених овим законом; 4) испуњава услове прописане чланом 17. овог закона за шеме високог нивоа поузданости, нарочито када је реч о доказивању поузданости			

a)	a1)	б)	б1)	в)	г)	д)
	under which the European Digital Identity Wallet is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet; (g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge. Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.		идентитета и управљању средствима електронске идентификације и њихове аутентификације; 5) у случају електронске потврде атрибута са уграђеним политикама откривања, примењује одговарајући механизам обавештавања корисника да поуздајућа страна или корисник дигиталног идентификационог новчаника, који су поднели захтев за ту електронску потврду атрибута имају овлашћења за приступ тој потврди; 6) обезбеђује да лични идентификациони подаци који су садржани у средству електронске идентификације посредством које је дигитални идентификациони новчаник обезбеђен, јединствено представљају физичко или правно лице, односно физичко лице у својству регистрованог субјекта, као и њиховог заступника; 7) омогућава свим физичким лицима бесплатно коришћење квалификованог електронског потписа.			
5a.6.	Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its contents, in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.	16.9.	Канцеларија без одлагања обавештава све кориснике дигиталног идентификационог новчаника о сваком безбедносном инциденту који би могао компромитовати или утрозити дигитални идентификациони новчаник или податке садржане у њему, нарочито ако је дошло до опозива или суспензије дигиталног идентификационог новчаника у складу са одредбама овог закона.	ПУ		
5a.7.	Without prejudice to Article 5f, Member States may provide, in accordance with national law, for additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means. Those additional functionalities shall comply with this Article	16.2.	Канцеларија обезбеђује интероперабилност и коришћење дигиталног идентификационог новчаника у складу са условима за издавање средства електронске идентификације утврђеним овим законом.	ПУ		
5a.8.	Member States shall provide validation mechanisms free-of- charge, in order to: (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified;	16.4.	Издавање, коришћење и опозив дигиталног идентификационог новчаника, као и механизме за валидацију података садржаних у дигиталном идентификационом новчанику врши се без накнаде.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(b) allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b.					
5a.9.	Member States shall ensure that the validity of the European Digital Identity Wallet can be revoked in the following circumstances: (a) upon the explicit request of the user; (b) where the security of the European Digital Identity Wallet has been compromised; (c) upon the death of the user or cease of activity of the legal person	16.5.	Канцеларија може опозвати дигитални идентификациони новчаник: 1) на изричит захтев корисника; 2) ако је угрожена сигурност дигиталног идентификационог новчаника; 3) након смрти корисника или престанка обављања делатности правног лица, односно физичког лица у својству регистрованог субјекта.	ПУ		
5a.10.	Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of European Digital Identity Wallets	16.7.	Канцеларија омогућава корисници да на једноставан начин могу пријавити техничке проблеме или друге инциденте који негативно утичу на коришћење дигиталног идентификационог новчаника и пружа им техничку подршку у њиховом отклањању.	ПУ		
5a.11.	European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high	16.1.	Дигитални идентификациони новчаник издаје орган државне управе надлежан за пројектовање, усклађивање, развој и функционисање система електронске управе (у даљем тексту: канцеларија), као средство електронске идентификације, коришћењем шеме електронске идентификације високог нивоа поузданости.	ПУ		
5a.12.	European Digital Identity Wallets shall ensure security-by- design.	16.6.	Дигитални идентификациони новчаник израђује се у складу са домаћим и међународним стандардима информационе безбедности.	ПУ		
5a.13.	The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons.	16.4.	Издавање, коришћење и опозив дигиталног идентификационог новчаника, као и механизме за валидацију података садржаних у дигиталном идентификационом новчанику врши се без накнаде.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
5a.14.	Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply mutatis mutandis.	15.3. 16.3.	Корисник дигиталног идентификационог новчаника има потпуну контролу над његовим коришћењем и коришћењем података у оквиру њега. Подаци о личности на основу којих се користе дигитални идентификациони новчаник чувају се логички одвојено од свих других података које чува пружалац услуге од поверења.	ПУ		
5a.15.	The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.	16.10.	Физичким и правним лицима који не користе дигитални идентификациони новчаник не сме се ограничити нити отежати приступ услугама, тржишту рада и слобода предузетништва.	ПУ		
5a.16.	The technical framework of the European Digital Identity Wallet shall: (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;	16.6.	Канцеларија обезбеђује техничке мере које пружаоцима електронских потврда атрибута као и другој страни, након издавања електронске потврде атрибута, онемогућава праћење, повезивање или корелацију трансакција или понашања корисника.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(b) enable privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user.					
5a.17.	Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of European Digital Identity Wallets as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with Regulation (EU) 2016/679 shall be demonstrated. Member States may introduce national provisions to further specify the application of such measures.	4.1-3.	Пружалац услуга од поверења односно услуге електронске идентификације приликом обраде података о личности поступа у складу са законом којим се уређује заштита података о личности, нарочито поштујући начело минимизације. Сврха обраде података при пружању услуга из става 1. овог члана је идентификација лица коришћењем средстава електронске идентификације, као и пружање услуга од поверења физичким и правним лицима при електронском пословању. Подаци који се обрађују при електронској идентификацији, као и пружању услуга од поверења прописаних овим законом чувају се највише десет година од тренутка идентификације, односно пружања услуга од поверења, осим ако посебним законом није другачије уређено.	ПУ		
5a.18-24.	Member States shall, without undue delay, notify the Commission of information about: (a) the body responsible for establishing and maintaining the list of registered relying parties that rely on European Digital Identity Wallets in accordance with Article 5b(5) and the location of that list; (b) the bodies responsible for the provision of European Digital Identity Wallets in accordance with Article 5a(1); (c) the bodies responsible for ensuring that the person identification data is associated with the European Digital Identity Wallet in accordance with Article 5a(5), point (f); (d) the mechanism allowing for the validation of the person identification data referred to in Article 5a(5), point (f), and of the identity of the relying parties;			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније.	

a)	a1)	б)	б1)	в)	г)	д)
	(e) the mechanism by which to validate the authenticity and validity of European Digital Identity Wallets. The Commission shall make available the information notified pursuant to the first subparagraph to the public through a secure channel, in electronically signed or sealed form suitable for automated processing. Without prejudice to paragraph 22 of this Article, Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet. Article 24(2), points (b), and (d) to (h), shall apply mutatis mutandis to providers of European Digital Identity Wallets. European Digital Identity Wallets shall be made accessible for use, by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council (1). For the purposes of the provision of European Digital Identity Wallets, European Digital Identity Wallets and the electronic identification schemes under which they are provided shall not be subject to the requirements laid down in Articles 7, 9, 10, 12 and 12a. By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet either by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with					

a)	a1)	б)	б1)	в)	г)	д)
	additional remote onboarding procedures that together meet the requirements of assurance level high. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
5b.1.	Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.	17.1.	Поуздајућа страна која намерава да користи дигитални идентификациони новчаник за пружање услуга својим корисницима, дужна је да се за такву врсту услуге региструје у јавном регистру поуздајућих страна који успоставља и води Канцеларија.	ПУ		
5b.2.	The registration process shall be cost-effective and proportionate- to-risk. The relying party shall provide at least: (a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes: (i) the Member State in which the relying party is established; and (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record; (b) the contact details of the relying party; (c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.	17.2.	Приликом регистрације, поуздајућа страна дужна је да приложи: 1) податке неопходне за аутентификацију, и то: пословно име и седиште, матични број, порески идентификациони број; 2) идентификационе податке овлашћеног лица, и то: име и презиме, јединствен матични број и адресу електронске поште; 3) начин и сврху коришћења дигиталног идентификационог новчаника укључујући податке који ће се у пружању услуге захтевати од корисника.	ПУ		
5b.3.	Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).	17.4.	Поуздајућа страна приликом пружања услуга не сме тражити друге податке од корисника садржаних у дигиталном идентификационом новчанику осим оних које је приликом регистрације пријавила, у складу са ставом 2. тачка 3. овог члана.	ПУ		
5b.4.	Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније.	

а)	а1)	б)	б1)	в)	г)	д)
5b.5.	Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.	17.1.	Поуздајућа страна која намерава да користи дигитални идентификациони новчаник за пружање услуга својим корисницима, дужна је да се за такву врсту услуге региструје у јавном регистру поуздајућих страна који успоставља и води Канцеларија.	ПУ		
5b.6.	Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2.	17.3.	Поуздајућа страна без олагања пријављује Канцеларији сваку промену података из става 2. овог члана.	ПУ		
5b.7.	Member States shall provide a common mechanism for allowing the identification and authentication of relying parties, as referred to in Article 5a(5), point (c).	17.5.	Канцеларија у оквиру дигиталног идентификационог новчаника обезбеђује механизам за аутентификацију поуздајуће стране приликом коришћења личних идентификационих података и електронских потврда атрибута.	ПУ		
5b.8.	Where relying parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the user.	17.5.	Канцеларија у оквиру дигиталног идентификационог новчаника обезбеђује механизам за аутентификацију поуздајуће стране приликом коришћења личних идентификационих података и електронских потврда атрибута.	ПУ		
5b.9.	Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.	17.6-7.	Поуздајућа страна одговорна је за спровођење поступка аутентификације и валидације личних идентификационих података, као и електронске потврде атрибута које преузима из дигиталног идентификационог новчаника корисника. Поуздајућа страна прихвата коришћење псеудонима ако приликом пружања услуга није неопходна идентификација корисника.	ПУ		
5b.10.	Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.	17.8.	Посредник који реализује услугу у име поуздајуће стране има исте обавезе као и поуздајућа страна и не сме чувати податке о садржају трансакције.	ПУ		
5b.11.	By 21 November 2024, the Commission shall establish technical specifications and procedures for the requirements referred to in paragraphs 2, 5 and 6 to 9 of	17.9.	Министарство прописује садржај и начин вођења регистра из става 1 овог члана, начин подношења захтева за упис у регистар, садржину и форму	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).		захтева,потребну документацију и начин објављивања података из регистра.			
5c.1.	The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a (24), shall be certified by conformity assessment bodies designated by Member States.	18.1.	Оцену усаглашености дигиталног идентификационог новчаника и средстава електронске идентификације у оквиру којег се они стављају на располагање, са условима прописаних у чл. 14. и 15. Овог закона, врши тело за оцењивање усаглашености које је акредитовано у складу са законом којим се уређује поступак акредитације.	ПУ		
5c.2.	Certification of the conformity of European Digital Identity Wallets with requirements referred to in paragraph 1 of this Article, or parts thereof, that are relevant for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council (1) and referred to in the implementing acts referred to in paragraph 6 of this Article.	18.2.	При оцени усаглашености дигиталног идентификационог новчаника, проверава се усаглашеност са техничким и безбедносним стандардима.	ПУ		
5c.3.	For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e(1) (the 'Cooperation Group'). The Cooperation Group may issue opinions and recommendations.			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније.	

а)	а1)	б)	б1)	в)	г)	д)
5c.4.	Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied in a timely manner, certification shall be cancelled.	18.3-4.	Сертификација из става 1. овог члана важи пет година, уз спровођење процене рањивости на сваке две године. Ако се приликом процене утврди рањивост сертификација се поништава.	ПУ		
5c.5.	Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation(EU) 2016/679.	4.1.	Пружалац услуга од поверења односно услуге електронске идентификације приликом обраде података о личности поступа у складу са законом којим се уређује заштита података о личности, нарочито поштујући начело минимизације.	ПУ		
5c.6.	By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1. 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније. Указујемо да је одредбом 18. утврђено да Министарство прописује ближе услове за оцену усаглашености из ст. 1. и 2. овог члана.	
5c.7.	Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније. Указујемо да је одредбом 18. уређено да Листу акредитованих тела за оцену усаглашености из става 1. овог члана утврђује Министарство	
5c.8.	The Commission shall be empowered to adopt delegated acts in accordance with Article 47 establishing specific criteria to be met by the designated conformity assessment bodies referred to in paragraph 1 of this Article.			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније. Указујемо да је одредбом 18. утврђено да Министарство прописује ближе услове за оцену усаглашености из ст. 1. и 2. овог члана.	

a)	a1)	б)	б1)	в)	г)	д)
5d.	Member States shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay of European Digital Identity Wallets that have been provided pursuant to Article 5a and certified by the conformity assessment bodies referred to in Article 5c(1). They shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1), without undue delay if a certification is cancelled and shall state the reasons for the cancellation. Without prejudice to Article 5a(18), the information provided by Member States referred to in paragraph 1 of this Article shall include at least: (a) the certificate and certification assessment report of the certified European Digital Identity Wallet; (b) a description of the electronic identification scheme under which the European Digital Identity Wallet is provided; (c) the applicable supervisory regime and information on the liability regime with respect to the party providing the European Digital Identity Wallet; (d) the authority or authorities responsible for the electronic identification scheme; (e) arrangements for suspension or revocation of the electronic identification scheme or authentication or of the compromised parts concerned. On the basis of the information received pursuant to paragraph 1, the Commission shall establish, publish in the Official Journal of the European Union and maintain in a machine-readable form a list of certified European Digital Identity Wallets. A Member State may submit a request to the Commission to remove a European Digital Identity Wallet and the electronic identification scheme under which it is provided from the list referred to in paragraph 3.			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније.	

a)	a1)	б)	б1)	в)	г)	д)
	Where there are changes to the information provided pursuant to paragraph 1, the Member State shall provide the Commission with updated information. The Commission shall keep the list referred to in paragraph 3 updated by publishing in the Official Journal of the European Union the corresponding amendments to the list within one month of receipt of a request pursuant to paragraph 4 or of updated information pursuant to paragraph 5. By 21 November 2024, the Commission shall establish the formats and procedures applicable for the purposes of paragraphs 1, 4 and 5 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
5e.1.	Where European Digital Identity Wallets provided pursuant to Article 5a, the validation mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets. Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission accordingly.	19.1-2. 19.5.	Ако се утврди неправилност, рањивост односно безбедносни инцидент при коришћењу дигиталног идентификационог новчаника, механизма за валидацију или средства електронске идентификације у оквиру које се користи дигитални идентификациони новчаник, на начин који утиче на њихову поузданост или на поузданост других дигиталних идентификационих новчаника, Канцеларија без одлагања привремено обуставља коришћење дигиталног идентификационог новчаника. Ако је неправилност, рањивост односно безбедносни инцидент из става 1. изазвао или може да изазове озбиљне последице по безбедност дигиталног идентификационог новчаника, Канцеларија повлачи из употребе дигитални идентификациони новчаник. О инцидентима и предузетим мерама из ст. 1-3. овог члана Канцеларија обавештава кориснике, поуздајуће стране који их користе, као и Министарство.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
5e.2.	If the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is not remedied within three months of the suspension, the Member State that provided the European Digital Identity Wallets shall withdraw European Digital Identity Wallets and revoke their validity. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission of the withdrawal accordingly.	19.4.	Ако се неправилност, рањивост, односно безбедносни инцидент из става 1. овог члана не отклони у року од 90 дана од дана привремене обуставе, Канцеларија повлачи из употребе дигитални идентификациони новчаник и опозива његову ваљаност.	ПУ		
5e.3.	Where the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is remedied, the providing Member State shall re-establish the provision and the use of European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact designated pursuant to Article 46c(1) and the Commission without undue delay.	19.3.	Када се неправилност, рањивост, односно безбедносни инцидент при коришћењу дигиталног идентификационог новчаника из става 1. овог члана отклони и стекну услови за безбедно и поуздано коришћење дигиталног новчаника, Канцеларија га поново ставља на располагање.	ПУ		
5e.4.	The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 5d without undue delay.	19.6.		НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније. Указујемо да је одредбом 19. уређено да Министарство ближе прописује мере из ст. 1-4. овог члана.	
5e.5.	By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the measures referred to in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније. Указујемо да је одредбом 19. уређено да Министарство ближе прописује мере из ст. 1-4. овог члана.	
5f.	Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation.			НП	Одредба је непреносива, јер уређује европски дигитални новчаник на унутрашњем тржишту Европске уније.	

a)	a)	б)	в)	г)	д)
	Where private relying parties that provide services, with the exception of microenterprises and small enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC (1), are required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council (2) require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested. in cooperation with Member States, the Commission shall facilitate the development of codes of conduct in close collaboration with all relevant stakeholders, including civil society, in order to contribute to the wide availability and usability of European Digital Identity Wallets within the scope of this Regulation, and to encourage service providers to complete the development of codes of conduct. 5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall assess the demand for, and the availability and usability of, European Digital Identity Wallets, taking into account criteria such as user take-up, cross-border presence of				

a)	a1)	б)	б1)	в)	г)	д)
	service providers, technological developments, evolution in usage patterns and consumer demand.					
6.	When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met: (a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9; (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high; (c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online. Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to Article 9 and which corresponds to the assurance level low may be recognised by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.			НП	Одредба је непрениосива, јер се односи на признавање шема електронске идентификације између држава чланица ЕУ, и то шема које су пријављене Европској комисији. Напомињемо да је чланом 24. Нацрта закона предвиђено да Министарство Европској комисији пријављује регистроване шеме електронског идентитета које испуњавају услове из Уредбе ЕУ бр. 910/2014 Европског парламента и Савета, а та одредба ступа на снагу од дана приступања Републике Србије Европској унији.	

a)	a1)	б)	б1)	в)	г)	д)
7.	An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met: (a) the electronic identification means under the electronic identification scheme are issued: (i) by the notifying Member State; (ii) under a mandate from the notifying Member State; or (iii) independently of the notifying Member State and are recognised by that Member State; (b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State; (c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3); (d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued; (e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);			НП	Одредба је непреносива, јер се односи на услове за пријављивање шема електронске идентификације, које државе чланице ЕУ пријављују Европској комисији.	

a)	a1)	б)	б1)	в)	г)	д)
	(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form. For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body. Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes; (g) at least six months prior to notification pursuant to Article 9(1), the notifying Member State provides the other Member States, for the purposes of Article 12(5), with a description of that scheme in accordance with the procedural arrangements established by the implementing acts adopted pursuant to Article 12(6); (h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).					
8.1.	An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.	20.1.	Шема електронске идентификације мора: 1) да садржи податке за идентификацију лица на издатим средствима за електронску идентификацију, који јединствено одређују правно или физичко лице; 2) да обезбеди да пружалац услуге електронске идентификације обезбеди идентификационе податке у оквиру средства електронске идентификације који олговарају лицу коме је средство издато;	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			3) да јасно дефинише техничке и друге услове који омогућавају поуздајућој страни проверу идентитета; 4) да испуњава услове за ниво поузданости у који се разврстава, из члана 21. овог закона.			
8.2.a.	The assurance levels low, substantial and high shall meet respectively the following criteria: (a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity	21.1.1.	Шеме електронске идентификације се разврставају према нивоу поузданости на: 1) шеме ниског нивоа поузданости, које обезбеђују ограничено поверење у идентитет којим се лице представља и користе средства и процедуре чија је сврха да смање ризик злоупотребе односно неистинитог представљања	ПУ		
8.2.b.	(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity	21.1.2.	2) шеме средњег нивоа поузданости, које обезбеђују значајно поверење у идентитет којим се лице представља и користе средства и процедуре чија је сврха да значајно смање ризик злоупотребе односно неистинитог представљања	ПУ		
8.2.c.	(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity	21.1.3.	3) шеме високог нивоа поузданости, које обезбеђују високо поверење у идентитет којим се лице представља и користе средства и процедуре чија је сврха да онемогуће злоупотребу односно неистинитог представљања	ПУ		
8.3.	By 18 September 2015, taking into account relevant international standards and subject to paragraph 2. the Commission shall, by means of implementing acts, set			НП	Одредба је непреносива, јер се њом даје овлашћење Европској комисији да донесе	

a)	a1)	б)	б1)	в)	г)	д)
	out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means.				акте за имплементацију одређаба о шемама електронске идентификације. Напомињемо да је чланом 21. став 2. Закона предвиђено да Влада, на предлог министарства надлежног за послове информационог друштва, ближе уређује услове које морају да испуне шеме електронске идентификације за одређене нивое поузданости. Тај акт ће уредити материју која одговара актима за имплементацију које ће донети Европска комисија.	
8.4.	Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements: (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means; (b) the procedure for the issuance of the requested electronic identification means; (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party; (d) the entity issuing the electronic identification means; (e) any other body involved in the application for the issuance of the electronic identification means; (f) the technical and security specifications of the issued electronic identification means.	21.2.	Влада, на предлог Министарства ближе уређује услове које морају да испуне шеме електронске идентификације за одређене нивое поузданости, а посебно: 1) начин доказивања и провере идентитета физичког односно правног лица које захтева издавање средстава електронске идентификације; 2) начин издавања средстава електронске идентификације; 3) механизам аутентификације, путем кога физичко односно правно лице коришћењем средстава идентификације потврђује свој идентитет другој страни у електронској трансакцији; 4) услове које треба да испуни издавалац средстава електронске идентификације; 5) услове које треба да испуне други учесници који су укључени у поступак издавања средстава електронске идентификације; 6) технике и безбедносне карактеристике средстава електронске идентификације која се издају;	ПУ		
8.5.	Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се упућује на процедуру која спроводи Европска комисија у поступку усвајања аката за имплементацију.	

a)	a)	б)	б1)	в)	г)	д)
9.	1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto: (a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme; (b) the applicable supervisory regime and information on the liability regime with respect to the following: (i) the party issuing the electronic identification means; and (ii) the party operating the authentication procedure; (c) the authority or authorities responsible for the electronic identification scheme; (d) information on the entity or entities which manage the registration of the unique person identification data; (e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met; (f) a description of the authentication referred to in point (f) of Article 7; (g) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned. The Commission shall, without undue delay, publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 together with basic information about those schemes. The Commission shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within one month of the date of receipt of that notification.			НП	Одредбе су непреносиве, с обзиром да регулишу обавезу држава чланица ЕУ да пријаве шеме електронске идентификације Европској комисији. Напомињемо да је чланом 24. Нацрта закона предвиђено да Министарство Европској комисији пријављује регистроване шеме електронског идентитета које испуњавају услове из Уредбе ЕУ бр. 910/2014 Европског парламента и Савета, а та одредба ступа на снагу од дана приступања Републике Србије Европској унији.	

a)	a1)	б)	б1)	в)	г)	д)
	A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
10.	Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States and the Commission without undue delay. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.			НП	Одредба је непреносива, јер регулише обавезе држава чланица ЕУ када се деси нарушавање безбедности електронске идентификације, у ком случају то пријављују другим државама чланицама и Европској комисији.	
11.1.	The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its			НП	Одредба одређује одговорност државе чланице која не испуни обавезе које се односе на прекограничне трансакције у	

а)	а1)	6)	61)	в)	г)	д)
	obligations under points (d) and (f) of Article 7 in a cross-border transaction.				оковиру шема електронске идентификације.	
11.2.	The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.	25.1.	Издавалац средства електронске идентификације одговоран је за штету насталу услед тога што је издао средство електронске идентификације противно условима прописаним овим законом и шемом електронске идентификације.	ПУ		
11.3.	The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.	25.2.	Страна која спроводи поступак аутентификације одговара за штету насталу услед непрописно спроведеног поступка аутентификације.	ПУ		
11.4.	Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.	25.4.	Одредбе овог члана примењују се у складу са законом којим се уређују облигациони односи.	ДП	Одредба је делимично преносива, јер упућује да се одредбе чл.11. ст. 1-3. уређе врше у складу са националним прописима о одговорности за штету.	
11.5.	Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.	25.5.	У случају међународне сарадње у области електронске идентификације, примењују се одредбе утврђене међународним споразумима.	ДП	Одредба је делимично преносива, јер упућује да се одредбе чл.11. ст. 1-3. уређе врше у складу са националним прописима о одговорности за штету.	
11а.	1. When acting as relying parties for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets. 2. Member States shall provide for technical and organisational measures to ensure a high level of protection of personal data used for identity matching and to prevent the profiling of users. 3. By 21 November 2024, the Commission shall establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 1 of this Article by means of implementing acts. Those			НП	Одредба одређује одговорност државе чланице која не испуни обавезе које се односе на прекотграничне трансакције у оквиру шема електронске идентификације.	

a)	a1)	б)	б1)	в)	г)	д)
	implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
12.	The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable. For the purposes of paragraph 1, an interoperability framework shall be established. The interoperability framework shall meet the following criteria: (a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State; (b) it follows European and international standards, where possible; (c) it facilitates the implementation of the principle of privacy by design. The interoperability framework shall consist of: (a) a reference to minimum technical requirements related to the assurance levels under Article 8; (b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8; (c) a reference to minimum technical requirements for interoperability; (d) a reference to a minimum set of person identification data necessary to uniquely represent a natural or legal person, or a natural person representing another natural person or a legal person, which is available from electronic identification schemes; (e) rules of procedure; (f) arrangements for dispute resolution; and (g) common operational security standards.	27.	Министарство сарађује са надлежним међународним телима по питањима прекограничне интероперабилности шема електронске идентификације и предузима мере из своје надлежности како би се успоставила интероперабилност шема електронске идентификације на националном нивоу. Ради остваривања прекограничне интероперабилности успоставља се оквир интероперабилности који: 1) је технолошки неутралан; 2) примењује одговарајуће европске и међународне стандарде, нарочито у области информационе безбедности; 3) омогућава примену приватности по дизајну, укључујући минималну обраду података, селективно откривање идентитета, криптографску заштиту и спречавање профилисања, у складу са прописима о заштити података о личности. Канцеларија успоставља и управља чвором у оквиру интероперабилности који омогућава прекограничну аутентификацију лица, чиме се обезбеђује да се инфраструктура електронске идентификације Републике Србије повеже са инфраструктуром електронске идентификације друге државе. У процесу управљања чвором из става 3. овог члана Канцеларија: 1) обезбеђује повезивање са чворовима других држава кроз оквир интероперабилности чије су шеме електронске идентификације саставни део Регистра из члана 22. овог закона, односно које су признате на основу међународног споразума; 2) примењује техничке и организационе мере заштите ради спречавања неовлашћеног приступа подацима који се размењују и обезбеђује интегритет података, који се преносе између чворова употребом одговарајућих техничких решења и праксе; 3) обезбеђује да се подаци о личности не чувају или задржавају у чвору.	НП	Одредба регулише интероперабилност шема електронске идентификације које државе чланице ЕУ пријављују Европској комисији. Указујемо да је чланом 23. Напрта закона предвиђено да Министарство сарађује са надлежним телима Европске уније по питањима прекограничне интероперабилности шема електронске идентификације и предузима мере из своје надлежности како би се успоставио што виши ниво интероперабилности шема електронске идентификације на националном нивоу. Међутим, имајући у виду да су чланом 12. предметне уредбе предвиђене обавезе које искључиво предузимају државе чланице ЕУ, односно Европска комисија, те одредбе нису могле да се пренесу у домаћи пропис.	

a)	a1)	б)	б1)	в)	г)	д)
	Member States shall carry out peer reviews of the electronic identification schemes that fall within the scope of this Regulation and that are to be notified pursuant to Article 9(1), point (a). By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 of this Article with a view to fostering a high level of trust and security appropriate to the degree of risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). By 18 September 2025, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1 of this Article, the Commission shall, subject to the criteria set out in paragraph 3 of this Article and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). The implementing acts referred to in paragraphs 7 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).	6)	4) користи техничка решења која обезбеђују интегритет и аутентичност података, а која се користе приликом прекограничне размене података; 5) обезбеђује да чвор испуњава прописане услове који се односе на формат порука, структуру података и протоколе размене, у складу са важећим националним стандардима и регулативом, чиме се обезбеђује техничка интероперабилност и правна ваљаност прекограничне електронске идентификације; 6) обезбеђује достављање метаподатака о управљању чвором у стандардизованом, машински читљивом облику који је погодан за аутоматску обраду података, на безбедан и поуздан начин; 7) обезбеђује аутоматску обраду параметара који се односе на безбедност, уз примену техничких и организационих мера које омогућавају континуирано праћење, свједочивање, анализу и реаговање на безбедносне догађаје, у складу са важећим националним стандардима и регулативом, без угрожавања приватности или интегритета података; 8) чува податке који би у случају инцидента омогућавали утврђивање места и врсте инцидента у законском року. 9) омогућава пренос података који обезбеђују поуздано представљање физичког или правног лица, на основу употребе регистроване шеме електронске идентификације приликом прекограничне сарадње у складу са законом. У поступцима прекограничне електронске идентификације примењују се технолошка решења која омогућавају недвосмислено утврђивање и упаривање идентитета физичких и правних лица, на основу електронских идентификационих средстава издатих у складу са признатим и регистрованим шемама електронске идентификације, а у складу са важећим техничким стандардима и прописима. Канцеларија спроводи техничке и организационе мере у чвору на начин који спречава профилисање корисника и обезбеђује заштиту података о личности, у складу са прописима којима се уређује			

а)	а1)	б)	б1)	в)	г)	д)
			заштита података о личности и електронска идентификација у прекограничном контексту. Прописом Владе из члана 21. став 2. овог закона ближе се уређују услови из става 4. овог члана који се односе на чвор.			
12a.1.	The conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation, including conformity with the cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes, shall be certified by conformity assessment bodies designated by Member States.	23.1.	Тело за оцењивање усаглашености, које је акредитовано у складу са законом којим се уређује поступак акредитације издаје сертификат којим потврђује усклађеност шема електронске идентификације са безбедносним и техничким захтевима прописаним овим законом.			
12a.2.	Certification pursuant to paragraph 1 of this Article shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.	23.3.	Сертификација се врши у складу са: 1) захтевима из овог закона и прописа донетих на основу њега; 2) националним стандардима за безбедност и заштиту података; 3) међународним стандардима као што су ISO/IEC 27001 и ISO/IEC 29115, 4) препорукама надлежних међународних тела за информациону безбедност.			
12a.3.	Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied within three months of such identification, certification shall be cancelled.	23.5-9.	Сертификат о усаглашености важи највише пет година, уз обавезу спровођења редовне процене рањивости најмање сваке две године. Ако се утврди рањивост издате шеме електронске идентификације, тело које је издало шему без одлагања га суспендује. Када се рањивост из става 6. овог члана отклони шема електронске идентификације се поново ставља на располагање кориснику. Ако се рањивост из става 6. овог члана не отклони у року од 90 дана од суспензије сертификат се опозива и повлачи из употребе. Тело које је издало сертификат обавештава корисника, Канцеларију, као и Министарство о			

а)	а1)	б)	б1)	в)	г)	д)
			безбедносним инцидентима и предузетим мерама из ст. 6-8. овог члана.			
12a.4.	Notwithstanding paragraph 2, Member States may request, in accordance with that paragraph, additional information from a notifying Member State about electronic identification schemes or part thereof certified.	23.2.	Оцена усклађености, односно сертификација обухвата техничке, организационе и безбедносне аспекте шема електронске идентификације.			
12a.5.	The peer review of electronic identification schemes referred to in Article 12(5) shall not apply to electronic identification schemes or parts of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity-related requirements set out in Article 8(2) regarding the assurance level of electronic identification schemes.	26.	Пружалац услуга електронске идентификације предузима потребне техничке, физичке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга. Техничким и организационим мерама осигурава се да ниво безбедности одговара степену ризика и предвиђеном нивоу поузданости шеме електронске идентификације, узимајући у обзир најновија доступна технолошка решења, а посебно се предузимају мере за спречавање безбедносних инцидентата и ограничавање штетних последица евентуалних инцидентата, као и за обавештавање заинтересованих страна о нежељеним ефектима безбедносних инцидентата. Пружалац услуга електронске идентификације дужан је да најмање једном годишње спроводи процену ризика, идентификује претње и слабости, утврди и ревидира мере заштите које су примерене степену ризика и нивоу поузданости шеме. Резултати процене и мере из става 3. овог члана морају бити документовани и доступни Министарству, у складу са прописима, техничким стандардима, добром праксом и технолошким достигнућима.	ДУ	Прилагођено националном оквиру	
12a.6.	Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.	29.	Министарство може признати сертификате издате у иностранству, под условом да су усклађени са међународним стандардима и да су издати од стране тела која испуњавају захтеве прописане овим законом.	НП	Одредба одређује одговорност државе чланице која не испуни обавезе које се односе на сертификацију шема електронске идентификације.	

a)	a1)	б)	б1)	в)	г)	д)
			Министарство Европској комисији може пријављивати регистроване шеме електронског идентитета које испуњавају услове из Уредбе eIDAS.			
12b.	Where providers of European Digital Identity Wallets and issuers of notified electronic identification means that act in a commercial or professional capacity and use core platform services as defined in Article 2, point (2), of Regulation (EU) 2022/1925 of the European Parliament and of the Council (1) for the purpose or in the course of providing European Digital Identity Wallet services and electronic identification means to end-users are business users as defined in Article 2, point (21), of that Regulation, gatekeepers shall in particular allow them effective interoperability with, and, for the purposes of interoperability, access to, the same operating system, hardware or software features. Such effective interoperability and access shall be allowed free of charge and regardless of whether the hardware or software features are part of the operating system, are available to, or are used by, that gatekeeper when providing such services, within the meaning of Article 6(7) of Regulation (EU) 2022/1925. This Article is without prejudice to Article 5a(14) of this Regulation.	28.	Канцеларија је дужна да издаваоцима средстава за електронску идентификацију који та средства стављају у промет омогући: 1) интероперабилност, укључујући технике, организационе и правне мере неопходне за обезбеђивање приступа оперативним системима, хардверским и софтверским функцијама релевантним за пружање услуга електронске идентификације; 2) бесплатан приступ оперативним системима, хардверским и софтверским функцијама из тачке 1 овог става. Обавезе из овог члана тумаче се у складу са принципима равноправног приступа, транспарентности и недискриминације, узимајући у обзир прописе и одговарајуће међународне стандарде.	ПУ		
13.1.	Notwithstanding paragraph 2 of this Article and without prejudice to Regulation (EU) 2016/679, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. Any natural or legal person who has suffered material or non-material damage as a result of an infringement of this Regulation by a trust service provider shall have the right to seek compensation in accordance with Union and national law. The burden of proving the intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.	30.1-3.	Пружалац услуге од поверења одговоран је за штету насталу услед тога што није поступио у складу са овим законом уколико је штету проузроковао намерно или непажњом. Терет доказивања намере или непажње пружаоца услуга од поверења је на физичком или правном лицу које захтева накнаду штете из става 1. овог члана. Терет доказивања да штета није настала услед намере или непажње квалификованог пружаоца услуга од поверења из става 1. овог члана је на том пружаоцу услуга.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.					
13.2.	Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.	30.4.	Пружалац услуга од поверења није одговоран за штету насталу због коришћења услуге којом је препоручено назначено ограничење, ако је корисник услуге од поверења о таквом ограничењу унапред обавештен, и ако су та ограничења позната трећим лицима.	ПУ		
13.3.	Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.			НП	Одредба упућује да се чл.13. ст. 1. и 2. Уредбе примењује у складу са националним прописима држава чланица ЕУ о одговорности за штету, због чега није преносива.	
14.	Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU. The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2). The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in			НП	Одредба је непреносива, јер се њоме утврђују поступци и услови које Европска унија предвиђа ради признавања дејства услуга од поверења које врше пружаоци услуга из трећих земаља. Указујемо да је чланом 40. Напрта закона предвиђено да је квалификована услуга од поверења коју пружа страни пружалац услуге од поверења правноправна са домаћом услугом од поверења уколико је тако регулисано потврђеним међународним споразумом.	

a)	a1)	6)	61)	в)	г)	д)
	particular establish, maintain and publish a trusted list of recognised trust service providers. The agreement referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or by the international organisation with which the agreement is concluded.					
15.	The provision of electronic identification means, trust services and end- user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.	6.	Услуге од поверења, услуге електронске идентификације и производи који се користе за пружање тих услуга једнако су доступни и особама с инвалидитетом.	ПУ		
16.	Without prejudice to Article 31 of Directive (EU) 2022/2555 of the European Parliament and of the Council (1), Member States shall lay down the rules on penalties applicable to infringements of this Regulation. Those penalties shall be effective, proportionate and dissuasive. Member States shall ensure that infringements of this Regulation by qualified and non-qualified trust service providers be subject to administrative fines of a maximum of at least: (a) EUR 5 000 000 where the trust service provider is a natural person; or (b) where the trust service provider is a legal person, EUR 5 000 000 or 1 % of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher.	83-86.	Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај пружалац квалификоване услуге од поверења – правно лице ако: 1) не предузима потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга од поверења (члан 32. став 1); 2) без одлагања, а најкасније у року од 24 сата од сазнања, не обавести Министарство о сваком нарушавању безбедности или губитку интегритета услуге који имају значајан утицај на пружање услуга од поверења (члан 32. став 3); 3) о повреди безбедности или губитку интегритета услуге, без одлагања, не обавести корисника услуге од поверења, ако би угрожавање безбедности или губитак интегритета услуге од поверења могло неповољно утицати на кориснике услуга од поверења (члан 32. став 4); 4) пре закључења уговора из члана 35. став 1. овог закона не обавести лице које је поднело захтев за	ПУ		

a)	a1)	6)	61)	в)	г)	д)
	Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fine is initiated by the competent supervisory body and imposed by competent national courts. The application of such rules in those Member States shall ensure that those legal remedies are effective and have an equivalent effect to administrative fines imposed directly by supervisory authorities.	6)	пужање квалификоване услуге од поверења о свим важним околностима коришћења услуге из члана 35. став 2. тач. 1)–3) овог закона (члан 35. став 2); 5) не испуњава услове из члана 36. овог закона; 6) при издавању квалификованог сертификата за услуге од поверења не провери податке о идентитету физичког односно правног лица који су садржани у квалификованом сертификату, у складу са чланом 38. став 1. овог закона (члан 38. ст. 1. и 2); 7) не изврши проверу испуњености услова пре почетка пужања квалификованих услуга од поверења, односно најмање једном у 24 месеца (члан 40. став 3); 8) не изврши налог за ванредно оцењивање испуњености услова (члан 40. став 5); 9) пре отпочињања пужања квалификованих услуга од поверења не буде уписан у Регистар пужаоца квалификованих услуга од поверења (члан 41. став 3); 10) издавалац квалификованих електронских сертификата, који намерава да престане са обављањем делатности, о намери раскида уговора не обавести сваког корисника квалификоване услуге од поверења и Министарство најмање три месеца пре настанка о намераваном престанку обављања делатности (члан 42. став 1); 11) у случају престанка са обављањем послова не обезбеди код другог пужаоца услуга од поверења наставак обављања услуга за кориснике којима је издао сертификат, или не опозове све издате сертификате и о предузетим мерама одмах не обавести Министарство (члан 42. став 2); 12) не достави сву документацију у вези са обављањем услуга од поверења другом издаваоцу на кога преноси обавезе обављања једне или више услуга од поверења, односно Министарству (члан 42. ст. 3. и 4); 13) квалификовани електронски сертификат не садржи све податке из члана 50. став 1. овог закона (члан 50. став 1); 14) издавалац квалификованих сертификата не изврши опозив издатих сертификата, у случајевима из члана 51. став 1. (члан 51. став 1) овог закона;	в)	г)	д)

a)	a1)	6)	61)	в)	г)	д)
			15) издавалац квалификованих сертификата не обавести корисника квалификоване услуге од поверења о опозиву сертификата у року од 24 часа од примљеног обавештења, односно настанка околности због којих се сертификат опозива (члан 51. став 2); 16) издавалац квалификованих сертификата не чува комплетну документацију о издатим и опозваним квалификованим сертификатима као средство за доказивање и верификацију у управним, судским и другим поступцима најмање десет година по престанку важења сертификата (члан 52.); 17) не обезбеди пријем и слање порука и кала је пошљалац или прималац поруке корисник другог пружаоца услуге квалификоване електронске доставе (члан 66. став 1); 18) пружалац услуга који омогућава претрагу веб сајтова путем интернет претраживача не обезбеди подршку, односно интероперабилност квалификованих сертификата за аутентификацију веб сајтова, као и да се подаци о идентитету и додатни атрибути потврђени у сертификату приказују на начин прилагођен корисницима у складу са чланом 70. овог закона; 19) не издаје квалификовану електронску потврду атрибута са садржајем из члана 71. став 2. овог закона; 20) не пружа квалификовану услугу електронског архивирања у складу са чланом 77. овог закона; 21) не пружа квалификовану услугу од поверења вођења електронске евиденције у складу са чланом 79. овог закона. За прекршај из става 1. овог члана казниће се и одговорно лице пружаоца услуге од поверења новчаном казном од 5.000 до 100.000 динара. За прекршај из става 1. овог члана казниће се пружалац услуге од поверења – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 500.000 динара. Новчаном казном од 50.000 до 200.000 динара казниће се за прекршај корисник квалификоване			

а)	а1)	б)	б1)	в)	г)	д)
			услуге од поверења – правно лице ако, у случају промене података из става 1. члана 38. овог закона не обавести без одлагања пружаоца квалификоване услуге од поверења. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу новчаном казном од 5.000 до 50.000 динара. За прекршај из става 1. овог члана казниће се корисник услуге од поверења – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 100.000 динара. За прекршај из става 1. овог члана казниће се корисник услуге од поверења – физичко лице новчаном казном од 5.000 до 50.000 динара. Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај регистрован пружалац услуге електронске идентификације – правно лице ако: 1) дигитални идентификациони новчаник не испуњава услове из члана 15. и 16. овог закона; 2) не предузима потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно коришћење дигиталног идентификационог новчаника из члана 15. ст. 1. и 2., члана 16. став 7. и члана 19. овог закона; 3) пре отпочивања коришћења дигиталног идентификационог новчаника не буде уписан у регистар поуздајуће стране за коришћење дигиталног идентификационог новчаника у складу са чланом 17. овог закона; 4) шема електронске идентификације не испуњава услове из члана 21. овог закона; 5) не предузима потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга из члана 26. став 2. овог закона. За прекршај из става 1. овог члана казниће се и одговорно лице пружаоца услуге електронске			

а)	а1)	б)	б1)	в)	г)	д)
			идентификације новчаном казном од 5.000 до 100.000 динара. За прекршај из става 1. овог члана казниће се пружалац услуге електронске идентификације – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 500.000 динара. Новчаном казном од 50.000 до 2.000.000 динара казниће се за прекршај пружалац услуге из члана 64. овог закона ако не поступи по налогу инспектора у остављеном року из члана 82. став 1. овог закона. За прекршај из става 1. овог члана казниће се и одговорно лице пружаоца услуге новчаном казном од 5.000 до 100.000 динара. За прекршај из става 1. овог члана казниће се пружалац услуге – физичко лице у својству регистрованог субјекта новчаном казном од 10.000 до 500.000 динара.			
18.	Supervisory bodies shall cooperate with a view to exchanging good practice. A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds: (a) the supervisory body is not competent to provide the requested assistance; (b) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;			НП	Одредбе се односе на поступање држава чланица ЕУ у погледу узајамне помоћи у овој области, одређује њихово поступање и примењивање се у Републици Србији од дана приступања Европској унији.	

a)	a1)	б)	б1)	в)	г)	д)
	(c) providing the requested assistance would be incompatible with this Regulation. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law					
19.1.	Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.	27.1-2.	Пружаоци услуга од поверења, укључујући квалификоване услуге од поверења, предузимају потребне техничке и организационе мере за управљање ризицима који угрожавају поуздано и безбедно пружање тих услуга од поверења. Техничким и организационим мерама осигурава се да ниво безбедности одговара степену ризика, узимајући у обзир најновија доступна технолошка решења, а посебно се предузимају мере за спречавање безбедносних инцидената и ограничавање штетних последица евентуалних инцидената, као и за обавештавање заинтересованих страна о нежељеним ефектима безбедносних инцидената.	ПУ		
19.2.1.	Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.	27.3.	Пружаоци услуга од поверења, укључујући пружаоце квалификованих услуга од поверења, без одлагања, а најкасније у року од 24 сата од сазнања, обавештавају Министарство о сваком нарушавању безбедности или губитку интегритета услуге који имају значајан утицај на пружање услуга од поверења или на заштити података о личности који се обрађују у оквиру пружања услуга.	ПУ		
19.2.2.	Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of	27.4.	Уколико би угрожавање безбедности или губитак интегритета услуге од поверења могло неповољно утицати на кориснике услуга од поверења, пружалац услуга од поверења о повреди безбедности или губитку интегритета услуге без	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	the breach of security or loss of integrity without undue delay.		одлагања обавештава корисника услуга од поверења.			
19.2.3.	Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.	27.6.	Министарство ће остварити сарадњу са одговарајућим институцијама других држава по питању размене података о нарушавању безбедности и интегритета, у складу са одговарајућим потврђеним међународним споразумима.	ПУ		
19.2.4.	The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.	27.5.	Министарство обавештава јавност или захтева од пружаоца услуга од поверења да то учини ако утврди да је објављивање података о повреди безбедности или губитка интегритета услуге у јавном интересу.	ПУ		
19.3.	The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.			НП	Одредба се односи на извештавање Европске агенције за мрежну и информациону безбедност од стране надлежних тела држава чланица. Напомињемо да Министарство остварује сарадњу са Међународном унијом за телекомуникације у погледу изrade Глобалног индекса сајбер безбедности, као и са Агенцијом Европске Уније за сајбер безбедност ЕНИСА учешћем у радној групи за електронску идентификацију и квалификоване услуге од поверења. ЦЕРТ-ови из Републике из Србије налазе се на Trusted Introducer листи, а Национални ЦЕРТ и ЦЕРТ МУП чланови су Forum of Incident Response and Security Teams организације.	
19a.1.	A non-qualified trust service provider providing non-qualified trust services shall:	37.1-5.	Пружаоци услуга од поверења треба да усвоје одговарајуће политике и процедуре и предузму друге релевантне мере у циљу управљања правним,			

a)	a1)	6)	61)	в)	г)	д)
	(a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service, which shall, notwithstanding Article 21 of Directive (EU) 2022/2555, include at least measures relating to: (i) registration and onboarding procedures for a trust service; (ii) procedural or administrative checks needed to provide trust services; (iii) the management and implementation of trust services; (b) notifying the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (a) (i), (ii) or (iii), that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.	6)	пословним, оперативним и другим директним или индиректним ризицима по пружање услуге од поверења и да поред предузимања мера из закона који уређује информациону безбедност обухвата мере управљања ризиком приликом: 1) регистрације и приступа корисника услугама од поверења; 2) спровођења административних провера неопходних за пружање услуга од поверења; 3) управљања и спровођења услуга од поверења. Пружаоци услуга од поверења без одлагања, а најкасније 24 сата од сазнања, обавештавају Министарство и друге надлежне органе, уgroжене кориснике, као и јавност уколико је то у јавном интересу, о свакој безбедносној компромитацији или сметњама у пружању услуга или примени мера из става 2. овог члана које имају значајан утицај на пружање услуге од поверења или на заштиту података о личности који се обрађују у оквиру пружања услуга. Ако би угрожавање безбедности или губитак интегритета услуге од поверења могли неповољно утицати на кориснике услуга од поверења, пружалац услуга од поверења о повреди безбедности или губитку интегритета услуге, без одлагања, обавештава корисника услуга од поверења, а ако би појединачно обавештавање представљало неразуман утронак времена и средстава, путем средстава јавног информисања, веб презентације министарства и на други погодан начин. Министарство обавештава јавност или захтева од пружаоца услуга од поверења да то учини, ако утврди да је објављивање података о повреди безбедности или губитка интегритета услуге у јавном интересу. Министарство сарађује са надлежним органима других држава у вези са разменом података о			

a)	a1)	б)	б1)	в)	г)	д)
19a.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for paragraph 1, point (a), of this Article. Compliance with the requirements laid down in this Article shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	37.6.	Министарство прописује стандарде, техничке спецификације и процедуре за испуњење услова из става 1. овог члана.			
20.1.1a.1b	Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt. Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request. Member States shall, without undue delay, notify to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States.	34.1-4. 34.7.	Оцењивање испуњености услова за пружање квалификованих услуга од поверења (у даљем тексту: оцењивање испуњености услова) обавља тело за оцењивање усаглашености које је, у складу са законом којим се уређује акредитација, акредитовано за оцењивање усаглашености пружаоца квалификованих услуга од поверења и квалификованих услуга од поверења које они пружају. Након спроведеног оцењивања испуњености услова тело за оцењивање усаглашености сачињава извештај о оцењивању усаглашености. Оцењивање испуњености услова врши се пре почетка пружања квалификованих услуга од поверења и најмање једном у 24 месеца. Након завршеног оцењивања испуњености услова пружалац услуге од поверења доставља Министарству извештај о оцењивању усаглашености, у року од три радна дана од дана када га је примио. Трошкове оцењивања испуњености услова, укључујући ванредна оцењивања, сноси пружалац квалификоване услуге од поверења.	ПУ		
20.2.	Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of	34.5-6.	Министарство може захтевати ванредно оцењивање испуњености услова како би потврдило да пружалац квалификованих услуга од поверења и	ПУ		

a)	a1)	6)	61)	в)	г)	д)
	the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.		квалификоване услуге од поверења које он пружа испуњавају услове прописане овим законом, а посебно ако се утврде неправилности у пружању квалификованих услуга од поверења, односно ако наступи инцидент који је у значајној мери угрозио или нарушио информациону безбедност. Ванредно оцењивање испуњености услова врши тело за оцењивање усаглашености које није повезано са вршењем претходног оцењивања.			
20.3.3a.3b.3c	Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable. Where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides. 3a. Where the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in Article 21 of that Directive, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service that it provides. 3b. Where the supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in that Regulation, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides. 3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status	35.8-11 45.1.	Ако пружалац квалификоване услуге од поверења не испуњава неки од услова прописаних овим законом, Министарство му налаже отклањање утврђених недостатака у року не дужем од 90 дана. Ако пружалац квалификоване услуге од поверења у задатом року не отклони утврђене неправилности и не испуни прописане услове, Министарство доноси решење о укидању статуса квалификованог пружаоца услуга од поверења и обустављању пружања одговарајуће услуге од поверења коју пружа и доставља га, у складу са законом. Ако орган надлежан за заштиту података о личности приликом вршења надзора утврди да је пружалац квалификоване услуге од поверења вршио обраду података о личности супротно закону и донесе решење којим се захтева престанак обраде, министарство привремено предузима одговарајуће мере у складу са овим законом и законом којим се уређује инспекцијски надзор. Сваку измену квалификованог статуса из ст. 9-10. овог члана Министарство ажурира у регистру пружалаца квалификованих услуга од поверења. Јавна листа квалификованих услуга од поверења на аутоматизован начин поуздајућој страни обезбеђује поуздану информацију о статусу пружаоца квалификованих услуга од поверења и њихових квалификованих услуга у складу са подацима уписаним у регистар из члана 41. овог закона.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	or of the qualified status of the service concerned. The supervisory body shall inform the body notified pursuant to Article 22(3) of this Regulation for the purposes of updating the trusted lists referred to in paragraph 1 of that Article and the competent authority designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555.					
20.4.	The Commission may, by means of implementing acts, establish reference number of the following standards: (a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1; (b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	40.12.	Министарство утврђује листу стандарда које мора да испуни тело за оцењивање усаглашености, обавезну садржину извештаја о оцењивању усаглашености и поступак оцењивања испуњености услова односно оцењивања усаглашености квалификованих услуга од поверења.	НП	Одредба се односе на овлашћење Европске комисије да доноси акта за примену наведених одредаби.	
21.1.	Where trust service providers intend to start providing a qualified trust service, they shall notify the supervisory body of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555.	41.2-3.	Пружалац квалификованих услуга од поверења подноси Министарству захтев за упис у Регистар пружалаца квалификованих услуга од поверења. Уз захтев из става 1. овог члана прилажу се докази о чињеницама исказаним у захтеву укључујући извештај о оцењивању усаглашености из члана 40. став 4. овог закона којим је оцењено да подносилац захтева и квалификоване услуге од поверења које он намерава да пружа испуњавају услове из овог закона.	ПУ		
21.2.	The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation and, in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.	35.4-7. 45.1.	Министарство решава о упису пружаоца квалификованих услуга од поверења у регистар из става 1. овог члана у року од 60 дана од дана доношења уредног захтева. У поступку решавања из става 4. овог члана Министарство може захтевати прилагање додатних	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	In order to verify the compliance of the trust service provider with the requirements laid down in Article 21 of Directive (EU) 2022/2555, the supervisory body shall request the competent authorities designated or established pursuant to Article 8(1) of that Directive to carry out supervisory actions in that regard and to provide information about the outcome without undue delay and in any event within two months of receipt of that request. If the verification is not concluded within two months of the notification, those competent authorities shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded. Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article. Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.		доказа, као и додатну проверу техничких и безбедносних компоненти и оперативног рада. Ако пружалац квалификованих услуга од поверења испуњава услове утврђене овим законом, Министарство решењем утврђује врсту услуге коју пружа, и врши упис у регистар из става 1. овог члана. Пружалац квалификованих услуга од поверења може почети да пружа квалификовану услугу од поверења након уписа у регистар из става 5. овог члана. Јавна листа квалификованих услуга од поверења на аутоматизован начин поузлађујућој страни обезбеђује поуздану информацију о статусу пружаоца квалификованих услуга од поверења и њихових квалификованих услуга у складу са подацима уписаним у регистар из члана 41. овог закона.			
21.3.	Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).	42.7-8. 45.1.	Пружалац квалификованих услуга од поверења може почети да пружа квалификовану услугу од поверења након уписа у регистар из става 5. овог члана. Ако пружалац услуга престане да испуњава услове прописане овим законом Министарство доноси решење о његовом брисању из регистра из става 1. овог члана. Јавна листа квалификованих услуга од поверења на аутоматизован начин поузлађујућој страни обезбеђује поуздану информацију о статусу пружаоца	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			квалификованих услуга од поверења и њихових квалификованих услуга у складу са подацима уписаним у регистар из члана 41. овог закона.			
21.4.	By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба се односе на овлашћење Европске комисије да доноси акта за примену наведених одредаби.	
22.1-2.	Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.	45.1-4.	Јавна листа квалификованих услуга од поверења на аутоматизован начин поуздајућој страни обезбеђује поуздану информацију о статусу пружаоца квалификованих услуга од поверења и њихових квалификованих услуга у складу са подацима уписаним у регистар из члана 41. овог закона. Јавна листа квалификованих услуга од поверења садржи информацију о релевантним протеклим догађајима у вези са статусом садашњих и бивших пружалаца и њихових услуга током времена, укључујући информацију о почетку пружања, губитку целovitости услуге од поверења, привременој забрани, престанку пружања услуге, брисању из регистра и другим догађајима забележеним у оквиру послова вођења регистра, инспекцијског надзора или догађајима пријављеним од стране пружаоца, а који утичу на прихватљивост квалификоване услуге од поверења и поступак утврђивања њеног статуса у одређеном временском тренутку. У Јавну листу квалификованих услуга од поверења уписују се подаци из ст. 1. и 2. овог члана као и други подаци утврђени прописом Министарства из става 6. овог члана и одговарајућим стандардима. Пружаоци квалификованих услуга од поверења дужни су да, на захтев Министарства, у року од седам дана, доставе податке из става 3. овог члана, као и да о свакој промени података из става 3. овог члана обавесте Министарство без одлагања.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
22.3-5.	Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба се односи на обавезу државна чланица Европске уније да обавесте Европску комисију о телу које је надлежно за јавне листе квалификованих услуга од поверења. Поред тога, одредбом се предвиђа овлашћење Европске комисије да донесе акте за примену предметних одредаби на нивоу Европске уније.	
23.1-3.	After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, с обзиром да се њом предвиђа издавање ЕУ знака поузданости за пружаоце услуга од поверења из ЕУ.	
24.1.1.	When issuing a qualified certificate or a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if	38.1.	Пружалац квалификованих услуга од поверења приликом пружања услуга дужан је да приликом издавања квалификованог сертификата или	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued. 1a. The verification of the identity referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, when needed, on a combination thereof in accordance with the implementing acts referred to in paragraph 1c: (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high; (b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in compliance with point (a), (c) or (d); (c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body; (d) through the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.		квалификоване електронске потврде атрибута провери идентитет физичког или правног лица којем се сертификат, односно потврда атрибута издаје, уз примену једне или више метода, и то: 1) коришћењем дигиталног идентификационог новчаника или другог средства електронске идентификације у оквиру шеме електронске идентификације високог нивоа поузданости; 2) коришћењем квалификованог електронског потписа, односно печата; 3) коришћењем других метода идентификације којима се обезбеђује висок ниво поузданости; 4) уз присуство физичког лица, односно овлашћеног представника правног лица уз подношење одговарајућих доказа као што је лична карта или путна исправа, односно други идентификациони документ са фотографијом.			
24.1b.	1b. The verification of the attributes referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, where necessary, on a combination thereof, in accordance with the implementing acts referred to in paragraph 1c: (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;	39.1.	Пружалац квалификованих услуга од поверења приликом издавања квалификоване електронске потврде атрибута, поред провере идентитета на начин из члана 38. овог закона, за проверу атрибута: 1) користи дигитални идентификациони новчаник или друга средства електронске идентификације у оквиру шеме електронске идентификације високог нивоа поузданости; 2) користи квалификован електронски потпис, односно печат; 3) користи квалификовану електронску потврду атрибута која садржи информацију о атрибуту; 4) проверава атрибуте присутног физичког лица која захтева услугу у своје име, односно у име			

a)	a1)	б)	б1)	в)	г)	д)
	(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in accordance with paragraph 1a. point (a), (c) or (d); (c) by means of a qualified electronic attestation of attributes; (d) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body; (e) by means of the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.		правног лица на основу поднетих одговарајућих доказа.			
24.1c.	1c. By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes in accordance with paragraphs 1, 1a and 1b of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се предвиђа овлашћење Европске комисије да донесе акте за примену предметних одредаби на нивоу Европске уније.	
24.2.1a	A qualified trust service provider providing qualified trust services shall: (a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities;	36.3.	Пружалац квалификованих услуга од поверења дужан је да писаним путем обавести Министарство о свакој планираној измени у пружању квалификованих услуга од поверења најкасније 30 дана пре увођења те измене, односно о намери престанка обављања делатности најкасније 90 дана пре престанка.	ПУ		
24.2.1b	(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;	36.1.1.	Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 1) има запослене који поседују неопходну стручност, искуство и квалификације за примену административних и управљачких процедура које одговарају домаћим и међународним стандардима и који су прошли одговарајућу обуку у области	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			информационе безбедности и заштите података о личности, у односу на услугу коју пружа;			
24.2.1e.	(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;	31.1.2.	Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 2) се осигура од одговорности за штету насталу пружањем квалификоване услуге од поверења.;	ПУ		
24.2.1d	(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;	35.2.	Пружалац квалификоване услуге од поверења дужан је да, пре закључивања уговора из става 1. овог члана, на свеобухватан и лако доступан начин, у разумљивом облику, обавести лице које је поднело захтев за пружање квалификоване услуге од поверења о свим важним околностима коришћења услуге, а нарочито о: 1) прописима и правилима који се односе на коришћење квалификоване услуге од поверења; 2) евентуалним ограничењима у коришћењу квалификоване услуге од поверења; 3) мерама које треба да реализују корисници квалификоване услуге од поверења и о потребној технологији за безбедно коришћење квалификоване услуге од поверења.	ПУ		
24.2.1e	(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques;	36.1.3.	Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 3) користи поуздане уређаје и производе који су заштићени од неовлашћене промене и гарантују техничку безбедност и поузданост процеса које подржавају, укључујући коришћење одговарајућих криптографских техника;	ПУ		
24.2.1f	(f) use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data,	36.1.4.	Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 4) користи поуздане системе за чување података који су му поверени тако: (1) да су подаци доступни само уз сагласност лица чији су то подаци. (2) да само овлашћена лица могу уносити податке и вршити измене,	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(iii) the data can be checked for authenticity;		(3) да се може проверавати аутентичност података;			
24.2.1fa	(fa) notwithstanding Article 21 of Directive (EU) 2022/2555, have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service, including at least measures related to the following: (i) registration and onboarding procedures for a service; (ii) procedural or administrative checks; (iii) the management and implementation of services;	32.1.	Пружаоци услуга од поверења треба да усвоје одговарајуће политике и процедуре и предузму друге релевантне мере у циљу управљања правним, пословним, оперативним и другим директним или индиректним ризицима по пружање услуге од поверења и да поред предузимања мера из закона који уређује информациону безбедност обухвата мере управљања ризиком приликом: 1) регистрације и приступа корисника услугама од поверења; 2) спровођења административних провера неопходних за пружање услуга од поверења; 3) управљања и спровођења услуга од поверења.			
24.2.1fb	(fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (fa)(i), (ii) or (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident;	32.2.	Пружаоци услуга од поверења без одлагања, а најкасније 24 сата од сазнања, обавештавају Министарство и друге надлежне органе, угрожене кориснике, као и јавност уколико је то у јавном интересу, о свакој безбедносној компромитацији или сметњама у пружању услуге или примени мера из става 2. овог члана које имају значајан утицај на пружање услуге од поверења или на заштити података о личности који се обрађују у оквиру пружања услуге.			
24.2.1g	(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;	36.1.5.	Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 5) спроводити мере против злоупотребе и крађе података;	ПУ		
24.2.1h	(h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;	36.1.6.	Пружалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: б) чува у одговарајућем временском периоду, не дужем од десет година, све релевантне информације које се односе на податке који су креирани или примљени од стране пружаоца квалификованих услуга од поверења, а посебно за сврху пружања	ПУ		

a)	a1)	6)	61)	в)	г)	д)
			доказа у правним поступцима, осим ако посебним законом није предвиђен другачији период чувања;			
24.2.1i	(i) have an up-to-date termination plan to ensure the continuity of service in accordance with provisions that are verified by the supervisory body pursuant to Article 46b(4), point (i);	36.1.8.	Пужалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 8) има ажуран план завршетка рада који осигурава континуитет квалификованих услуга од поверења;	ПУ		
24.2.1k	(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.	36.1.7.	Пужалац квалификованих услуга од поверења дужан је да, поред услова из члана 32. овог закона: 7) води ажуру, тачну и безбедним мерама заштићену базу података издатих електронских сертификата у случају када пружа услугу издавања квалификованих електронских сертификата, као и базу података који су креирани или примљени од стране пружаоца квалификованих услуга од поверења у оквиру пружања квалификованих услуга од поверења;	ПУ		
24.2.2.	The supervisory body may request information in addition to the information notified pursuant to point (a) of the first subparagraph or the result of a conformity assessment and may condition the granting of the permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.	41.4-5.	Министарство решава о упису пружаоца квалификованих услуга од поверења у регистар из става 1. овог члана у року од 60 дана од дана подношења уредног захтева. У поступку решавања из става 4. овог члана Министарство може захтевати прилагање додатних доказа, као и додатну проверу техничких и безбедносних компоненти и оперативног рада.			
24.3.	If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.	51.2. 51.4. 52.1-2.	Издавалац квалификованих сертификата дужан је да обавести корисника квалификоване услуге од поверења о опозиву сертификата у року од 24 часа од примљеног обавештења, односно настанка околности због којих се сертификат опозива. У случају опозива квалификовани електронски сертификат трајно престаје да важи од тренутка опозива. Издавалац квалификованих електронских сертификата дужан је да чува комплетну	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			документацију о издатим и опозваним квалификованим електронским сертификатима, као средство за доказивање и верификацију у управним, судским и другим поступцима, најмање десет година по престанку важења сертификата. Подаци из става 1. овог члана могу се чувати у електронској форми.			
24.4.	With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.	50.1.10. 52.1-2.	Квалификовани електронски сертификат мора да садржи: 10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата; Издавалац квалификованих електронских сертификата дужан је да чува комплетну документацију о издатим и опозваним квалификованим електронским сертификатима, као средство за доказивање и верификацију у управним, судским и другим поступцима, најмање десет година по престанку важења сертификата. Подаци из става 1. овог члана могу се чувати у електронској форми.	ПУ		
24.4a.	Paragraphs 3 and 4 shall apply accordingly to the revocation of qualified electronic attestations of attributes.	71.2.9.	Квалификована електронска потврда атрибута садржи: 9) информације или локација услуге где се проверава валидност квалификоване електронске потврде.	ПУ		
24.4b.	The Commission shall be empowered to adopt delegated acts in accordance with Article 47, establishing additional measures referred to in paragraph 2, point (fa), of this Article.			НП	Одредба се односи на овлашћење Европске комисије да донесе акте за примену ових одредаба на нивоу ЕУ.	
24.5.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 2 of this Article. Compliance with the requirements laid			НП	Одредба се односи на овлашћење Европске комисије да донесе акте за примену ових одредаба на нивоу ЕУ.	

a)	a1)	б)	б1)	в)	г)	д)
	down in this paragraph shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
24a.	Qualified electronic signatures based on a qualified certificate issued in one Member State and qualified electronic seals based on a qualified certificate issued in one Member State shall be recognised, respectively, as qualified electronic signatures and qualified electronic seals in all other Member States. Qualified electronic signature creation devices and qualified electronic seal creation devices certified in one Member State shall be recognised, respectively, as qualified electronic signature creation devices and qualified electronic seal creation devices in all other Member States. A qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices provided in one Member State shall be recognised, respectively, as a qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices in all other Member States. A qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals in all other Member States. A qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals provided in one Member State			НП	Одредба се односи на признавање квалификованих услуга од поверења на нивоу ЕУ.	

a)	a1)	б)	б1)	в)	г)	д)
	shall be recognised, respectively, as a qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals in all other Member States. A qualified electronic time stamp provided in one Member State shall be recognised as a qualified electronic time stamp in all other Member States. A qualified certificate for website authentication issued in one Member State shall be recognised as a qualified certificate for website authentication in all other Member States. A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in all other Member States. A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States. A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States.					
25.1.	An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.	60.1.	Електронском потпису не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику или што не испуњава услове за квалификовани електронски потпис.	ПУ		
25.2.	A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.	60.2.	Квалификовани електронски потпис има исто правно дејство као и својеручни потпис.	ПУ		
26.1.a	An advanced electronic signature shall meet the following requirements: (a) it is uniquely linked to the signatory;	49.1.1.	Напредни електронски потпис односно напредни електронски печат мора:	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			1) на недвосмислен начин да буде повезан са потписником, односно печатом;			
26.1.b	(b) it is capable of identifying the signatory;	49.1.2.	2) да омогућава утврђивање идентитета потписника односно печатноца;	ПУ		
26.1.c	(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and	49.1.3.	3) да буде израђен коришћењем података за израду електронског потписа односно електронског печата које потписник односно печатилац може, уз висок ниво поузданости, користи под својом искључивом контролом;	ПУ		
26.1.d	(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.	49.1.4.	4) да буде повезан са електронски потписаним односно електронски печатираним подацима на начин да се може утврдити било која накнадна измена тих података.	ПУ		
26.2.	By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic signatures. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic signatures shall be presumed where an advanced electronic signature complies with the standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба се односи на овлашћење Европске комисије да донесе акте за примену ових одредаба на нивоу ЕУ.	
27.1-5.	If a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5. If a Member State requires an advanced electronic signature based on a qualified certificate to use an online service offered by, or on behalf of, a public sector body,			НП	Одредбе се односе на поступање држава чланица ЕУ у погледу међусобног признавања напредних електронских потписа и квалификованих електронских потписа приликом коришћења услуга органа јавне власти. Такође, одредбе се односе и на овлашћење Европске комисије да донесе акта за примену одредаба на нивоу ЕУ.	

a)	a1)	6)	61)	в)	г)	д)
	that Member State shall recognise advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
28.1-2.	Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.	50.1.	Квалификовани електронски сертификат мора да садржи: 1) ознаку, у форми погодној за аутоматску обраду, да се електронски сертификат користи као квалификовани сертификат за електронски потпис, односно печат; 2) скуп података који јединствено идентификују квалификованог пружаоца услуге од поверења за издавање квалификованог електронског сертификата укључујући, најмање, земљу порекла пружаоца и назив пружаоца; 3) скуп података који јединствено идентификују потписника односно печатиоца укључујући најмање: (1) за потписника: - име и презиме или псеудоним, а уколико је употребљен псеудоним то мора бити јасно обележено у оквиру квалификованог електронског сертификата; - ЈМБГ, уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи ЈМБГ;	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			- свиденички број странца уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи евиденцијски број странца; - број стране путне исправе из машински чилеве зоне путне исправе, односно број стране личне карте и ознаку земље издаваоца путне исправе, односно стране личне карте, као идентификациону ознаку странца коју додељује Република Србија; (2) за печатиоца: назив, држава и матични број односно јединствена идентификациона ознака у складу са правном регулативом те државе, уколико постоји; 4) податке за проверу електронског потписа односно електронског печата, који одговарају подацима за креирање тог електронског потписа односно електронског печата; 5) податке о почетку и крају важења квалификованог електронског сертификата; 6) серијски број квалификованог електронског сертификата, који мора бити јединствен у оквиру издаваоца квалификованог електронског сертификата; 7) напредни електронски потпис или напредни електронски печат издаваоца квалификованог електронског сертификата; 8) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа односно напредног електронског печата из тачке 7) овог става; 9) информацију о сервисима који врше проверу валидности сертификата; 10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата; 11) ознаку да су подаци за креирање електронског потписа односно печата, који одговарају подацима за проверу електронског потписа односно печата из квалификованог електронског сертификата, садржани у квалификованом средству за креирање електронског потписа односно печата, уколико је тај услов испуњен.			

a)	a1)	б)	б1)	в)	г)	д)
28.3.	Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.	50.2.	Квалификовани електронски сертификати, поред обележја из става 1. овог члана, могу укључивати додатна обележја.	ПУ		
28.4.	If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	51.4.	У случају опозива квалификовани електронски сертификат трајно престаје да важи од тренутка опозива.	ПУ		
28.5.a	Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature: (a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;	51.5.	У случају суспензије квалификовани електронски сертификат губи важност током периода трајања суспензије.	ПУ		
28.5.b.	(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate	51.6.	Подаци о суспензији и периоду трајања суспензије квалификованог електронског сертификата уписују се у базу података издатих сертификата коју води издавалац квалификованих електронских сертификата и морају бити видљиви током трајања суспензије у оквиру услуга којима се пружају информације о статусу сертификата.	ПУ		
28.6.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се даје овлашћење Европској комисији да донесе акте за примену на нивоу ЕУ. Указујемо да је чланом 43. став 3. Нацрта закона предвиђено да Министарство ближе прописује услове које мора да испуњавају квалификовани електронски сертификати.	
29.1.	Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.	53.1-4.	Квалификовано средство за креирање електронског потписа односно печата мора да, помоћу одговарајућих техничких решења и поступака, обезбеди:	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			1) поверљивост података за креирање електронског потписа односно печата; 2) да се подаци за креирање електронског потписа, односно печата појављују само једном; 3) да се подаци за креирање електронског потписа, односно печата не могу добити изван средства за креирање електронског потписа, односно печата употребом доступне технологије у разумном времену; 4) да је електронски потпис, односно печат поуздано заштићен од фалсификовања употребом доступне технологије; 5) могућност поуздане заштите података за креирање електронског потписа, односно печата од неовлашћеног коришћења. Средства за креирање квалификованог електронског потписа, односно печата, приликом креирања електронског потписа односно печата, не смеју променити податке који се потписују односно печетирају или онемогућити потписнику, односно печатиоцу увид у те податке пре процеса креирања квалификованог електронског потписа односно печата. Квалификовано средство за креирање електронског потписа, односно печата на даљину (у даљем тексту: услуга управљања квалификованим средством на даљину) корисник квалификоване услуге од поверења може користити путем услуге управљања квалификованим средством за креирање електронског потписа, односно печата, што такође представља квалификовану услугу од поверења. Изузетно од става 1. овог члана, квалификовани пружалац услуга од поверења из става 3. овог члана може израдити копију података за израду електронског потписа, односно печата у сврху заштите од губитка података ако: 1) израда и чување копија података за креирање квалификованог електронског потписа односно печата не умањују прописани ниво заштите тих података; 2) број израђених копија података за креирање електронског потписа односно печата			

a)	a1)	б)	б1)	в)	г)	д)
			није већи него што је то неопходно за обезбеђивање континуитета пружања услуге.			
29.1a.	Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.	53.5.	Пружалац квалификоване услуге од поверења који пружа услугу управљања квалификованим средствима за креирање електронског потписа на даљину креира, односно управља подацима за креирање квалификованог електронског потписа и, на захтев корисника, израђује резервне копије тих података у сврху заштите од губитка података.			
29.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, јер се њом даје овлашћење Европској комисији да донесе акта за примену на нивоу ЕУ.	
29a.1.	The management of remote qualified electronic signature creation devices as a qualified service shall be carried out only by a qualified trust service provider that: (a) generates or manages electronic signature creation data on behalf of the signatory; (b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data for back-up purposes only, provided that the following requirements are met: (i) the security of the duplicated datasets must be at the same level as for the original datasets; (ii) the number of duplicated datasets must not exceed the minimum needed to ensure continuity of the service; (c) complies with any requirements identified in the certification report of the specific remote qualified electronic signature creation device issued pursuant to Article 30.	54.1.	Пружалац услуга од поверења који управља квалификованим средствима за креирање електронског потписа на даљину је дужан да: 1) креира или управља подацима за креирање електронског потписа на захтев потписника и искључиво у његово име; 2) прави резервне копије података за креирање електронског потписа само у сврху заштите од губитка података, под следећим условима: (1) да се безбедност резервних копија података одржава на истом нивоу као и безбедност изворних података; (2) да је број резервних копија података ограничен на минимум неопходан за осигурање континуитета услуге; 3) испуњава све захтеве утврђене за сертификат за квалификовано средство на даљину за креирање електронског потписа, у складу са прописима.			

a)	a1)	б)	б1)	в)	г)	д)
29a.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, specifications and procedures for the purposes of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, јер се њом даје овлашћење Европској комисији да донесе акта за примену на нивоу ЕУ.	
30.1.	Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.	55.1.	У складу са законом којим се уређују технички захтеви за производе и оцењивање усаглашености, Министарство именује тело за оцењивање усаглашености средстава за креирање квалификованог електронског потписа односно печата (у даљем тексту: именовано тело) које врши оцену усаглашености у складу са прописом из члана 53. овог закона.	ПУ		
30.2.	Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.			НП	Одредба је непреносива, с обзиром да се њом задужују државе чланице ЕУ да пријављују Европској комисији тела за оцењивање усаглашености која су именовали.	
30.3.1.a	The certification referred to in paragraph 1 shall be based on one of the following: (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or	55.1-2. 54.2.	У складу са законом којим се уређују технички захтеви за производе и оцењивање усаглашености Министарство именује тело за оцену усаглашености средстава за креирање квалификованог електронског потписа односно печата са техничким прописом из члана 46. (у даљем тексту: именовано тело). Прописом из члана 53. овог закона ближе се уређују и услови које мора да испуњава именовано тело. Министарство ближе прописује услове које мора да испуњава средство за креирање квалификованог електронског потписа односно печата техничким прописом.	ПУ		
30.3.1.b	(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission.			НП	Одредба је у вези са пријављивањем процеса сертификације Европској комисији.	

a)	a1)	б)	б1)	в)	г)	д)
	That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.					
30.3.2. 30.3a. 30.4.	The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). 3a The validity of a certification referred to in paragraph 1 shall not exceed five years, provided that vulnerabilities assessments are carried out every two years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.			НП	Одредбе су непрениосиве, јер се чланом 30. став. 3. подстав 2. даје овлашћење Европској комисији за доношење акта за примену на нивоу ЕУ, а чланом 30. став 4. врши се пренос надлежности Европској комисији за доношење акта.	
31.1-3.	Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures applicable for the purpose of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance			НП	Одредба је непрениосива, јер се односи на пријављивање информација о сертификованим средствима за издавање квалификованог електронског потписа Европској комисији, као и на овлашћење Европске комисије да доноси акте за примену на нивоу ЕУ. Указујемо да је чланом 55. Нацрта закона предвиђено да Министарство води Регистар квалификованих средстава за креирање електронских потписа и електронских печата на основу извештаја које добија од именованих тела, као и да се у тај регистар уписују и квалификована средства за креирање електронског потписа и електронског печата са списка који према члану 31. Регулative који објављује Европска комисија.	

a)	a1)	6)	61)	в)	г)	д)
	with the examination procedure referred to in Article 48(2).					
32.1.a	The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that: (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I; (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing; (c) the signature validation data corresponds to the data provided to the relying party; (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party; (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing; (f) the electronic signature was created by a qualified electronic signature creation device; (g) the integrity of the signed data has not been compromised; (h) the requirements provided for in Article 26 were met at the time of signing. Compliance with the requirements laid down in the first subparagraph of this paragraph shall be presumed where the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 3.	56.1. 58.1.	Поступком валидације утврђује се да електронски потпис представља исправан квалификовани електронски потпис када: 1) је утврђено да је сертификат који прати електронски потпис у тренутку потписивања представљао квалификовани електронски сертификат; 2) је утврђено да је квалификовани електронски сертификат издат од стране пружаоца услуге издавања квалификованих сертификата за електронски потпис и да је важно у тренутку потписивања; 3) је утврђено да подаци за валидацију електронског потписа из квалификованог електронског сертификата одговарају комбинацији електронског потписа и података који су потписани електронским потписом; 4) је поуздајућој страни тачно приказан скуп података из квалификованог електронског сертификата који јединствено идентификују потписника; 5) су поуздајућој страни тачно приказани подаци који су потписани електронским потписом; 6) је коришћење псеудонима јасно назначено поуздајућој страни, у случају да је приликом електронског потписивања коришћен псеудоним; 7) је утврђено да је електронски потпис креиран коришћењем квалификованог средства за креирање електронског потписа; 8) је утврђено да није нарушен интегритет података који су потписани електронским потписом; 9) је утврђено да електронски потпис испуњава услове за напредни електронски потпис из овог закона. Пружалац квалификоване услуге валидације квалификованих електронских потписа односно печата обезбеђује:	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			1) валидацију квалификованог електронског потписа односно печата у складу са чланом 56. овог закона; 2) да поуздајућа страна која користи услугу добије резултат поступка валидације електронским путем на аутоматизован начин, који је поуздан и ефикасан; 3) да је резултат поступка валидације из тачке 2) овог става печатан напредним електронским печатом или потписан напредним електронским потписом пружаоца услуге.			
32.2.	The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	56.2.	Систем који се користи за валидацију квалификованог електронског потписа обезбеђује тачан резултат поступка валидације поуздајућој страни и омогућава јој идентификовање било ког проблема од значаја за поузданост.	ПУ		
32.3.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непрениосива, јер се њоме даје овлашћење Европској комисији да доноси акте за примену предметног члана. Напомињемо да је чланом 56. Нацрта закона предвиђено да ће Министарство ближе прописује услове за поступак валидације квалификованог електронског потписа и квалификованог електронског печата.	
33.1.a	A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who: (a) provides validation in compliance with Article 32(1); and (b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	58.1.	Пружалац квалификоване услуге валидације квалификованих електронских потписа односно печата обезбеђује: 1) валидацију квалификованог електронског потписа односно печата у складу са чланом 56. овог закона; 2) да поуздајућа страна која користи услугу добије резултат поступка валидације електронским путем на аутоматизован начин, који је поуздан и ефикасан; 3) да је резултат поступка валидације из тачке 2) овог става печатан напредним електронским	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			печатом или потписан напредним електронским потписом пружаоца услуге.			
33.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified validation service referred to in paragraph 1 of this Article. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the qualified validation service for qualified electronic signatures complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, јер се односи на овлашћење Европске комисије да донесе акт за примену наведеног члана. Указујемо да је чланом 49. Нацрта закона предвиђено да Министарство ближе прописује услове за пружање услуге квалификоване валидације квалификованих електронских потписа и квалификованих електронских печата.	
34.1-1a.	A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period. 1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 2.	59.1-2.	Пружалац квалификоване услуге чувања електронских потписа, односно печата обезбеђује поузданост квалификованог електронског потписа, односно печата и након његовог престанка важења. Министарство ближе прописује стандарде, спецификације и процедуре за пружање квалификоване услуге чувања електронских потписа, односно печата.	ПУ		
34.2.	The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непреносива, јер се односи на овлашћење Европске комисије да донесе акт за примену наведеног члана. Указујемо да је чланом 59. став 2. Нацрта закона предвиђено ближе уређење ове материје од стране Министарства.	
35.1.	An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on	61.1.	Електронском печату не може се оспорити пуноважност или доказна снага само због тога што	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.		је у електронском облику или што не испуњава услове за квалификован електронски печат.			
35.2.	A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.	61.2.	За квалификовани електронски печат важи правна претпоставка да обезбеђује порекло и интегритет података за које је везан.	ПУ		
36.1.	An advanced electronic seal shall meet the following requirements: (a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.	49.1.	Напредни електронски потпис односно напредни електронски печат мора: 1) на недвосмислен начин да буде повезан са потписником, односно печатником; 2) да омогућава утврђивање идентитета потписника, односно печатника; 3) да буде израђен коришћењем података за израду електронског потписа односно електронског печата које потписник односно печатилац може, уз висок ниво поузданости, користити под својом искључивом контролом; 4) да буде повезан са електронски потписаним односно електронски печатаним подацима, на начин да се може утврдити било која накнадна измена тих података.	ПУ		
36.2.	By 21 May 2026, the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic seals. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic seals shall be presumed where an advanced electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредба је непрениосива, јер се односи на овлашћење Европске комисије да донесе акт за примену наведеног члана	
37.1-5.	If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for			НП	Одредбе се односе на поступање држава чланица ЕУ у погледу међусобног признавања напредних електронских потписа и квалификованих електронских потписа приликом	

a)	a1)	б)	б1)	в)	г)	д)
	electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5. If a Member State requires an advanced electronic seal based on a qualified certificate in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals based on a qualified certificate and qualified electronic seal at least in the formats or using methods defined in the implementing acts referred to in paragraph 5. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).				коришћења услуга органа јавне власти. Такође, одредбе се односе и на овлашћење Европске комисије да донесе акта за примену одредаба на нивоу ЕУ.	
38.1-2.	Qualified certificates for electronic seals shall meet the requirements laid down in Annex III. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.	50.1.	Квалификовани електронски сертификат мора да садржи: 1) ознаку, у форми погодној за аутоматску обраду, да се електронски сертификат користи као квалификовани сертификат за електронски потпис, односно печат; 2) скуп података који јединствено идентификују квалификованог пружаоца услуга од поверења за издавање квалификованог електронског сертификата укључујући, најмање, земљу порекла пружаоца и назив пружаоца; 3) скуп података који јединствено идентификују потписника односно печатиоца укључујући најмање: (1) за потписника: – име и презиме или псеудоним, а уколико је употребљен псеудоним то мора бити	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			јасно обележено у оквиру квалификованог електронског сертификата; - ЈМБГ, уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи ЈМБГ; - евиденцијски број странца уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи евиденцијски број странца; - број стране путне исправе из машински читљиве зоне путне исправе, односно број стране личне карте и ознаку земље издаваоца путне исправе, односно стране личне карте, као идентификациону ознаку странца коју додељује Република Србија; (2) за печатноца: назив, држава и матични број односно јединствена идентификациона ознака у складу са правном регулативом те државе, уколико постоји; 4) податке за проверу електронског потписа односно електронског печата, који одговарају подацима за креирање тог електронског потписа односно електронског печата; 5) податке о почетку и крају важења квалификованог електронског сертификата; 6) серијски број квалификованог електронског сертификата, који мора бити јединствен у оквиру издаваоца квалификованог електронског сертификата; 7) напредни електронски потпис или напредни електронски печат издаваоца квалификованог електронског сертификата; 8) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа односно напредног електронског печата из тачке 7) овог става; 9) информацију о сервисима који врше проверу валидности сертификата; 10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата;			

а)	а1)	б)	б1)	в)	г)	д)
			11) ознаку да су подаци за креирање електронског потписа односно печата, који одговарају подацима за проверу електронског потписа односно печата из квалификованог електронског сертификата, садржани у квалификованом средству за креирање електронског потписа односно печата, уколико је тај услов испуњен.			
38.3.	Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.	50.2.	Квалификовани електронски сертификати, поред обележја из става 1. овог члана, могу укључивати додатна обележја.	ПУ		
38.4.	If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.	51.4.	У случају опозива квалификовани електронски сертификат трајно престаје да важи од тренутка опозива.	ПУ		
38.5.	Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals: (a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension; (b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate	51.5-6.	У случају суспензије квалификовани електронски сертификат губи важност током периода трајања суспензије. Подаци о суспензији и периоду трајања суспензије квалификованог електронског сертификата уписују се у базу података издатих сертификата коју води издавалац квалификованих електронских сертификата и морају бити видљиви током трајања суспензије у оквиру услуга којима се пружају информације о статусу сертификата.	ПУ		
38.6.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal complies with those standards, specifications and procedures. Those implementing acts			НП	Одредбом се даје овлашћење Европској комисији да донесе акте за примену на нивоу ЕУ. Указујемо да је чланом 43. став 3. Нацрта закона предвиђено да Министарство ближе прописује услове које мора да испуњавају квалификовани електронски сертификати.	

a)	a1)	6)	61)	в)	г)	д)
	shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
39.1.	Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.	53.1-4.	Квалификовано средство за креирање електронског потписа односно печата мора да, помоћу одговарајућих техничких решења и поступака, обезбеди: 1) поверљивост података за креирање електронског потписа односно печата; 2) да се подаци за креирање електронског потписа, односно печата појављују само једном; 3) да се подаци за креирање електронског потписа, односно печата не могу добити изван средства за креирање електронског потписа, односно печата употребом доступне технологије у разумном времену; 4) да је електронски потпис, односно печат поуздано заштићен од фалсификовања употребом доступне технологије; 5) могућност поуздане заштите података за креирање електронског потписа, односно печата од неовлашћеног коришћења. Средства за креирање квалификованог електронског потписа, односно печата, приликом креирања електронског потписа односно печата, не смеју променити податке који се потписују односно печетирају или онемогућити потписнику, односно печатиоцу увид у те податке пре процеса креирања квалификованог електронског потписа односно печата. Квалификовано средство за креирање електронског потписа, односно печата на даљину (у даљем тексту: услуга управљања квалификованим средством на даљину) корисник квалификоване услуге од поверења може користити путем услуге управљања квалификованим средством за креирање електронског потписа, односно печата, што такође представља квалификовану услугу од поверења. Изузетно од става 1. овог члана, квалификовани пружалац услуга од поверења из става 3. овог члана може израдити копију података за израду	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			електронског потписа, односно печата у сврху заштите од губитка података ако: 1) израда и чување копија података за креирање квалификованог електронског потписа односно печата не умањују прописани ниво заштите тих података; 2) број израђених копија података за креирање електронског потписа односно печата није већи него што је то неопходно за обезбеђивање континуитета пружања услуге. Пружалац квалификоване услуге од поверења који пружа услугу управљања квалификованим средствима за креирање електронског потписа на даљину креира, односно управља подацима за креирање квалификованог електронског потписа и, на захтев корисника, израђује резервне копије тих података у сврху заштите од губитка података.			
39.2.	Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.	55.1-2. 53.5.	У складу са законом којим се уређују технички захтеви за производе и оцењивање усаглашености, Министарство именује тело за оцењивање усаглашености средстава за креирање квалификованог електронског потписа односно печата (у даљем тексту: именовано тело) које врши оцену усаглашености у складу са прописом из члана 53. овог закона. Прописом из члана 53. овог закона ближе се уређују и услови које мора да испуњава именовано тело. Министарство ближе прописује услове које мора да испуњава средство за креирање квалификованог електронског потписа односно печата техничким прописом.	ПУ		
39.3.	Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.			НП	Одредба је непрениосива, јер се односи на пријављивање информација о сертификованим средствима за издавање квалификованог електронског потписа Европској комисији, као и на овлашћење Европске комисије да доноси акте за примену на нивоу ЕУ.	

a)	a1)	б)	б1)	в)	г)	д)
					Указујемо да је чланом 47. Напрта закона предвиђено да Министарство води Регистар квалификованих средстава за креирање електронских потписа и електронских печата на основу извештаја које добија од именованих тела, као и да се у тај регистар уписују и квалификована средства за креирање електронског потписа и електронског печата са списка који према члану 31. Регулative који објављује Европска комисија.	
39a.	Article 29a shall apply mutatis mutandis to a qualified service for the management of remote qualified electronic seal creation devices.	54.2.	Пружалац услуге од поверења који управља квалификованим средствима за креирање електронског потписа на даљину је дужан да: 1) креира или управља подацима за креирање електронског потписа на захтев потписника и искључиво у његово име; 2) прави резервне копије података за креирање електронског потписа само у сврху заштите од губитка података, под следећим условима: (1) да се безбедност резервних копија података одржава на истом нивоу као и безбедност изворних података; (2) да је број резервних копија података ограничен на минимум неопходан за осигурање континуитета услуге; 3) испуњава све захтеве утврђене за сертификат за квалификовано средство на даљину за креирање електронског потписа, у складу са прописима. На пружаоца услуге од поверења који управља квалификованим средствима за креирање електронског печата на даљину сходно се примењује став 1. овог члана.	ПУ		
40.	Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.	56.1-3. 58.1.	Поступком валидације утврђује се да електронски потпис представља исправан квалификовани електронски потпис када:	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
			1) је утврђено да је сертификат који прати електронски потпис у тренутку потписивања представљао квалификовани електронски сертификат; 2) је утврђено да је квалификовани електронски сертификат издат од стране пружаоца услуге издавања квалификованих сертификата за електронски потпис и да је важио у тренутку потписивања; 3) је утврђено да подаци за валидацију електронског потписа из квалификованог електронског сертификата одговарају комбинацији електронског потписа и података који су потписани електронским потписом; 4) је поуздајућој страни тачно приказан скуп података из квалификованог електронског сертификата који јединствено идентификују потписника; 5) су поуздајућој страни тачно приказани подаци који су потписани електронским потписом; 6) је коришћење псеудонима јасно назначено поуздајућој страни, у случају да је приликом електронског потписивања коришћен псеудоним; 7) је утврђено да је електронски потпис креиран коришћењем квалификованог средства за креирање електронског потписа; 8) је утврђено да није нарушен интегритет података који су потписани електронским потписом; 9) је утврђено да електронски потпис испуњава услове за наредни електронски потпис из овог закона. Систем који се користи за валидацију квалификованог електронског потписа обезбеђује тачан резултат поступка валидације поуздајућој страни и омогућава јој идентификовање било ког проблема од значаја за поузданост. Одредбе ст. 1. и 2. овог члана сходно се примењују на електронски печат.			

a)	a1)	б)	б1)	в)	г)	д)
			Пружалац квалификоване услуге валидације квалификованих електронских потписа односно печата обезбеђује: 1) валидацију квалификованог електронског потписа односно печата у складу са чланом 56. овог закона; 2) да поуздајућа страна која користи услугу добије резултат поступка валидације електронским путем на аутоматизован начин, који је поуздан и ефикасан; 3) да је резултат поступка валидације из тачке 2) овог става печатан напредним електронским печатом или потписан напредним електронским потписом пружаоца услуге.			
40a.	Article 32a shall apply mutatis mutandis to the validation of advanced electronic seals based on qualified certificates.	57.1-3.	Валидација напредног електронског потписа заснованог на квалификованом сертификату потврђује исправност потписа, ако су испуњени следећи услови: 1) сертификат који прати електронски потпис је у време потписивања представљао квалификовани сертификат за електронски потпис; 2) квалификовани сертификат је издат од стране пружаоца квалификоване услуге од поверења и био је важећи у време потписивања; 3) подаци за валидацију потписа одговарају подацима достављеним поуздајућој страни; 4) јединствени сет података који идентификује потписника је исправно достављен поуздајућој страни; 5) коришћење псеудонима је јасно назначено поуздајућој страни, у случају да је приликом електронског потписивања коришћен псеудоним; 6) обезбеђен је интегритет потписаних података; 7) захтеви за напредне електронске потписе су били испуњени у време потписивања. Систем који се користи за валидацију напредног електронског потписа мора да омогући кориснику да сазна тачан резултат процеса валидације и открије све безбедносне неправилности.			

а)	а1)	б)	б1)	в)	г)	д)
			Одредбе ст. 1. и 2. овог члана сходно се примењују на електронски печат.			
41.1.	An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.	63.1.	Електронском временском жигу не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику или што не испуњава услове за квалификован временски жиг.	ПУ		
41.2.	A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.	63.2.	За квалификовани електронски временски жиг и податке којима је тај временски жиг придружен важи правна претпоставка тачности датума и времена исказаног у временском жигу и очуваности интегритета тих података у односу на тај временски тренутак.	ПУ		
42.1.	A qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; (b) it is based on an accurate time source linked to Coordinated Universal Time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.	62.1.	Квалификовани електронски временски жиг мора: 1) да је повезан са координисаним универзалним временом (UTC) тако да се спречава свака могућност промене података која се не може открити; 2) да је заснован на прецизном временском извору; 3) да је издат од стране пружаоца услуге издавања квалификованог временског жига; 4) да је потписан, односно печатиран од стране пружаоца услуге издавања квалификованог временског жига помоћу напредног електронског потписа или напредног електронског печата	ПУ		
42.1a.	Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accuracy of the time source comply with the standards, specifications and procedures referred to in paragraph 2.	62.2.	Министарство прописује ближе услове за квалификоване електронске временске жигове.	ПУ		
42.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the binding of date and time to data and for establishing the accuracy of time sources. Those			НП	Одредбом је дато овлашћење Европској комисији да својим актом ближе уреди стандарде за временски жиг. Указујемо да је чланом 62. став 2. Нацрта закона предвиђено да Министарство	

a)	a1)	6)	61)	в)	г)	д)
	implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).				ближе прописује услове за квалификоване електронске временске жигове.	
43.1.	Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.	67.1.	Пошлицама послатим или примљеним путем услуге електронске доставе не може се оспорити правна снага и допуштеност као доказ у правном промету само из разлога што су у електронској форми или из разлога што не испуњавају све услове услуге квалификоване електронске доставе.	ПУ		
43.2.	Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.	67.2.	За податке из електронске поруке послате или примљене путем услуге квалификоване електронске доставе важи правна претпоставка интегритета података, слања података од назначеног пошиљаоца, пријем од стране назначеног примаоца, поузданости датума и времена слања или примања.	ПУ		
44.1.1.a	Qualified electronic registered delivery services shall meet the following requirements: (a) they ensure with a high level of confidence the identification of the sender; (b) they are provided by one or more qualified trust service provider(s); (c) they ensure the identification of the addressee before the delivery of the data; (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.	64.1.	Услуга квалификоване електронске доставе мора: 1) да је пружана од стране једног или више пружаоца квалификованих услуга од поверења; 2) да, уз висок ниво поузданости, обезбеђује идентификацију пошиљаоца; 3) да обезбеђује идентификацију примаоца приликом доставе података; 4) у процесу слања и пријема електронске поруке, да користи напредни електронски потпис или напредни електронски печат пружаоца услуге квалификоване електронске доставе у сврху спречавања непримећене промене података; 5) да обезбеди да измена података извршена у сврху слања или пријема података мора бити јасно назначена пошиљаоцу и примаоцу; 6) да обезбеди да време и датум слања, пријема и евентуалне измене података морају бити назначени квалификованим електронским временским жигом.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.		7) да, у случају да се подаци преносе између два или више пружалаца услуге квалификоване електронске доставе, обезбеди да се услови из овог става примењују на сваког од њих.			
44.1 а.	Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data complies with the standards, specifications and procedures referred to in paragraph 2.	64.2.	Ако поступак слања и пријема података испуњава норме и стандарде прописане у члану 65. став 7. овог члана сматра се да су испуњени услови из става 1. овог члана.			
44.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2). 2a. Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 and such compliance shall be confirmed by a conformity assessment body. 2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a of this Article. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непреносива. Указујемо да је чланом 65. став 7. предвиђено да Министарство ближе прописује услове за услуге квалификоване електронске доставе.	
45.1-1b.	1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.	69.1-2. 70.1.	Квалификовани сертификати за аутентификацију веб сајтова садрже: 1) ознаку, која се може препознати при аутоматској обради, да је сертификат издат као квалификовани сертификат за аутентификацију веб сајтова:	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	1a. Qualified certificates for website authentication issued in accordance with paragraph 1 of this Article shall be recognised by providers of web-browsers. Providers of web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner. Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 of this Article, with the exception of microenterprises or small enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC during the first five years of operating as providers of web-browsing services. 1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.		2) скуп података који недвосмислено представљају пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова, што обавезно укључује државу седишта, пословно име и матични број тог пружаоца услуге; 3) име и презиме или псеудоним физичког лица коме је издат сертификат, односно пословно име и матични број правног лица коме је издат сертификат; 4) адресу, односно седиште физичког или правног лица коме је издат сертификат; 5) назив интернет домена физичког или правног лица коме је издат сертификат; 6) податке о почетку и крају рока важења сертификата; 7) идентификациону ознаку сертификата која мора да буде јединствена за пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова; 8) напредан електронски потпис, или напредан електронски печат пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова; 9) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа, односно напредног електронског печата из тачке 8) овог става; 10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата. Квалификовани сертификати за аутентификацију веб сајтова потребно је да испуњавају искључиво захтеве утврђене ставом 1. овог члана. Пружалац услуга претраге веб сајтова путем интернет претраживача дужан је да обезбеди подршку, односно интероперабилност квалификованих сертификата за аутентификацију веб сајтова, као и да се атрибути потврђени у сертификату приказују на начин прилагођен корисницима.			

a)	a1)	б)	б1)	в)	г)	д)
45.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непреносива. Указујемо да је чланом 69. став 5. предвиђено да Министарство ближе прописује услове за пружање услуге издавања квалификованог сертификата за аутентификацију веб сајтова.	
45a.	1. Providers of web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise qualified certificates for website authentication and to display the identity data provided in a user-friendly manner. 2. By way of derogation from paragraph 1 and only in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates. 3. Where a provider of a web-browser takes precautionary measures pursuant to paragraph 2, the provider of the web-browser shall notify its concerns in writing, without undue delay, together with a description of the measures taken to mitigate those concerns, to the Commission, the competent supervisory body, the entity to whom the certificate was issued and to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory body shall issue an acknowledgement of receipt to the provider of the web-browser in question. 4. The competent supervisory body shall investigate the issues raised in the notification in accordance with Article 46b(4), point (k). Where the outcome of that investigation does not result in the withdrawal of the qualified status of the certificate, the supervisory body shall inform the provider of the web-browser accordingly and shall request that provider to put an end	70.	Пружалац услуга претраге веб сајтова путем интернет претраживача дужан је да обезбеди подршку, односно интероперабилност квалификованих сертификата за аутентификацију веб сајтова, као и да се атрибути потврђени у сертификату приказују на начин прилагођен корисницима. Пружалац услуга из става 1. овог члана може предузети додатне мере предострожности ако посумња у рањивост једног или више квалификованих сертификата за аутентификацију веб сајтова, о чему, без одлагања, обавештава Министарство, Регистар националног интернет домена Србије и пружаоца квалификоване услуге од поверења који је издао сертификат. По пријему обавештења из става 2. овог члана Министарство спроводи инспекцијски надзор и одлучује да ли је потребно опозвати сертификат који је предмет надзора.			

a)	a1)	б)	б1)	в)	г)	д)
	to the precautionary measures referred to in paragraph 2 of this Article.					
45b.	An electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes. A qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form. An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in one Member State shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.	75.	Електронској потврди атрибута не може се оспорити пуноважност или доказна снага само због тога што је у електронском облику, односно због тога што не испуњава услове за квалификовану електронску потврду атрибута. Квалификована електронска потврда атрибута и потврда атрибута коју издаје орган јавне власти имају пуноважност и доказну снагу као и издате потврде, односно исправе у папирном облику. Потврда атрибута коју издаје орган јавне власти може бити призната у другој држави или међународној организацији ако је то предвиђено међународним споразумом који закључи република србија са другом државом или међународном организацијом.	ПУ		
45c.	Where an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.	39.1.	Пружалац квалификованих услуга од поверења приликом издавања квалификоване електронске потврде атрибута, поред провере идентитета на начин из члана 38. овог закона, за проверу атрибута: 1) користи дигитални идентификациони новчаник или друга средства електронске идентификације у оквиру шеме електронске идентификације високог нивоа поузданости; 2) користи квалификован електронски потпис, односно печат; 3) користи квалификовану електронску потврду атрибута која садржи информацију о атрибуту; 4) проверава атрибуте присутног физичког лица која захтева услугу у своје име, односно у име правног лица на основу поднетих одговарајућих доказа.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
45d.1-4.	Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V. The evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 5 of this Article. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not in any circumstances be reverted.	71.1-3.	Квалификовану електронску потврду атрибута издаје пружалац квалификоване услуге од поверења регистрован за пружање те услуге. Квалификована електронска потврда атрибута садржи: 1) ознаку, која се може препознати при аутоматској обради, да је потврда издата као квалификована електронска потврда атрибута; 2) скуп података који недвосмислено идентификују пружаоца услуге од поверења који издаје квалификовану електронску потврду атрибута, укључујући податке о држави седишта, пословном имену и матичном броју; 3) скуп података који недвосмислено идентификују лице на које се односе потврђени атрибут, односно његов псеудоним ако га користи; 4) потврђен атрибут, односно атрибуте, и по потреби додатне информације о атрибуту; 5) податке о почетку и крају рока важења потврде; 6) идентификациону ознаку потврде јединствену за пружаоца квалификоване услуге од поверења и, по потреби, идентификациону ознаку, односно назнаку шеме аутентичног извора атрибута као и назив тог извора, односно назив евиденције, односно регистра у коме се води атрибут; 7) квалификован електронски потпис, односно квалификован електронски печат пружаоца квалификоване услуге од поверења који издаје потврду; 8) локацију на којој је, без накнаде, доступан сертификат квалификованог електронског потписа, односно печата из тачке 7) овог става; 9) информације или локација услуге где се проверава валидност квалификоване електронске потврде. Квалификована електронска потврда атрибута која је опозвана након почетног издавања трајно губи валидност од тренутка опозива.	ПУ		

a)	a1)	6)	61)	в)	г)	д)
45d.5.	By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic attestations of attributes. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непреносива. Указујемо да је чланом 71. став 4. предвиђено да Министарство ближе прописује стандарде, спецификације и процедуре за пружање услуге издавања квалификоване електронске потврде атрибута	
45e.1.	Member States shall ensure, within 24 months of the date of entry into force of the implementing acts referred to in Articles 5a(23) and 5c (6), that, at least for the attributes listed in Annex VI, wherever those attributes rely on authentic sources within the public sector, measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify those attributes by electronic means at the request of the user, in accordance with Union or national law.	72.1.	Пружалац квалификоване услуге од поверења који издаје електронске потврде атрибута, на захтев корисника, може вршити проверу аутентичности атрибута из изворних евиденција за следеће атрибуте о кориснику: 1) адресу пребивалишта, односно боравишта; 2) године; 3) пол; 4) брачно стање; 5) сродство; 6) чланове домаћинства; 7) држављанство; 8) ниво образовања и титуле; 9) занимање; 10) стручне лиценце; 11) овлашћења за заступање физичких и правних лица; 12) податке о адвокатима, јавним извршитељима, односно бележницима; 13) пословно име, адресу седишта као и финансијске податке правног лица, односно физичког лица у својству регистрованог субјекта.	ПУ		
45e.2.	By 21 November 2024, the Commission shall, taking into account relevant international standards, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the catalogue of attributes, as well as schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes for the purposes of paragraph 1 of this Article.			НП	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непреносива. Указујемо да је чланом 72. став 2. предвиђено да Министарство ближе прописује стандарде, спецификације и	

a)	a1)	б)	б1)	в)	г)	д)
	Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).				процедуре за оцену усаглашености пружаоца услуге издавања електронске потврде атрибута.	
45f.1-5.	An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements: (a) those set out in Annex VII; (b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46), identified as the issuer referred to in point (b), of Annex VII, containing a specific set of certified attributes in a form suitable for automated processing and: (i) indicating that the issuing body is established in accordance with Union or national law as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf; (ii) providing a set of data unambiguously representing the authentic source referred to in point (i); and (iii) identifying the Union or national law referred to in point (i). The Member State where public sector bodies referred to in Article 3, point (46), are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet a level of reliability and trustworthiness equivalent to qualified trust service providers in accordance with Article 24. Member States shall notify public sector bodies referred to in Article 3, point (46), to the Commission. That notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure	73.1-3.	Орган јавне власти који води изворну евиденцију одређеног атрибута издаје, сам или преко овлашћеног лица, електронску потврду атрибута која садржи: 1) ознаку, која се може препознати при аутоматској обради, да је потврда издата као електронска потврда атрибута коју издаје орган јавне власти; 2) скуп података који недвосмислено идентификују орган јавне власти који издаје електронску потврду атрибута, пословно име и матични број; 3) скуп података који недвосмислено идентификују лице на које се односи потврђени атрибут а ако се користи псеудоним, то мора бити јасно назначено; 4) потврђен атрибут, односно атрибуте, и по потреби додатне информације о атрибуту; 5) податке о почетку и крају рока важења потврде; 6) јединствена идентификациона ознака и назив евиденције, односно регистра у којем се атрибут води; 7) квалификован електронски потпис овлашћеног лица, односно квалификован електронски печат органа који издаје потврду; 8) локацију на којој је, без накнаде, доступан сертификат квалификованог електронског потписа, односно печата из тачке 7) овог става; 9) локацију на којој се може проверити валидност квалификоване електронске потврде.	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	channel, the list of public sector bodies referred to in Article 3, point (46), in electronically signed or sealed form suitable for automated processing. Where an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not be reverted. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be deemed to be compliant with the requirements laid down in paragraph 1, where it complies with the standards, specifications and procedures referred to in paragraph 6.		Електронска потврда атрибута која је опозвана након издавања трајно губи валидност од тренутка опозива. Орган јавне власти који издаје електронску потврду атрибута из става 1. овог члана дужан је да испуни услове из члана 36. овог закона који се односе на пружаоца квалификоване услуге од поверења			
45f.6-8.	By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2). By 21 November 2024, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the purposes of paragraph 3 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2). Public sector bodies referred to in Article 3, point (46), issuing electronic attestation of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance with Article 5a.			НП	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непрениосива. Указујемо да је чланом 73. став 4. предвиђено да Министарство ближе прописује стандарде, спецификације и процедуре за оцену усаглашености пружаоца услуге издавања електронске потврде атрибута коју издаје орган јавне власти.	

a)	a1)	б)	б1)	в)	г)	д)
45g.	Providers of electronic attestations of attributes shall provide European Digital Identity Wallet users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member State where the European Digital Identity Wallet is provided. Providers of qualified electronic attestations of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance in Article 5a.	74.	Пружалац услуге од поверења који издаје електронске потврде атрибута дужан је да на захтев корисника дигиталног идентификационог новчаника изда електронску потврду атрибута коју корисник може сачувати и користити у свом дигиталном идентификационом новчанику. Пружалац услуге од поверења издавања квалификоване електронске потврде атрибута мора испуњавати услове за дигитални идентификациони новчаник из чл. 15. и 16. овог закона.	ПУ		
45h.	Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them or their commercial partners. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the provider of electronic attestation of attributes. Providers of qualified electronic attestation of attributes' services shall implement the provision of such qualified trust services in a manner that is functionally separate from other services provided by them.	76.	Подаци о личности који се обрађују приликом издавања електронске потврде атрибута као и квалификоване електронске потврде атрибута не смеју се комбиновати са другим подацима о личности који се обрађују приликом пружања других услуга од поверења. Подаци о личности који се обрађују приликом издавања електронске потврде атрибута чувају се логички одвојено од других података које чува пружалац услуге од поверења. Пружалац квалификоване услуге од поверења дужан је да функционално раздвоји услугу издавања квалификоване електронске потврде атрибута од других услуга које пружа.	ПУ		
45i.	Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in electronic form or that they are not preserved using a qualified electronic archiving service. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider.	78.	Подацима и електронским документима који су електронски архивирани не може се оспорити пуноважност или доказна снага само због тога што су у електронском облику, односно због тога што нису чувани коришћењем квалификоване услуге електронског архивирања. Пружалац квалификоване услуге од поверења електронског архивирања гарантује интегритет и порекло података и електронских докумената који су чувани у електронском архиву за период чувања.	ПУ		

a)	a1)	6)	61)	в)	г)	д)
45j.1.	Qualified electronic archive services shall meet the following requirements: (a) they are provided by qualified trust service providers; (b) they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin; (c) they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format; (d) they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval. The report referred to in point (d) of the first subparagraph shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.	77.1.	Пужалап квалификоване услуге од поверења електронског архивирања дужан је да: 1) се региструје као пужалап квалификоване услуге од поверења у складу са законом; 2) примењује поступке и користи технологије којима се обезбеђује трајност и читљивост података и електронских докумената најмање током законом прописаног рока, односно рока утврђеног листом категорија архивске грађе и документарног материјала са роковима чувања, уз очување интегритета података; 3) обезбеди да се подаци и електронска документа заштите од губитка и промена, осим података које се односе на медиј или електронски облик; 4) поуздајућој страни омогући аутоматско преузимање потврде потписане, односно печатане квалификованим електронским потписом, односно печатом, којом се гарантује интегритет података и електронских докумената преузетих из електронског архива у периоду чувања.	ПУ		
45j.2.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НП	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непреносива. Указујемо да је чланом 77. став 2. предвиђено да Министарство ближе прописује услове, стандарде, спецификације и процедуре које је потребно да испуни пужалап квалификоване услуге од поверења електронског архивирања	

a)	a1)	6)	61)	в)	г)	д)
45k.	An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.	80.1-2.	Подацима из електронских евиденција не може се оспорити пуноважност или доказна снага само због тога што су у електронском облику. односно због тога што не испуњавају захтеве квалификоване услуге вођења електронске евиденције. Пружалац квалификоване услуге од поверења вођења електронске евиденције гарантује јединствен и тачан хронолошки редослед, као и целовитост, односно интегритет података које евидентира.	ПУ		
45l.1-2.	Qualified electronic ledgers shall meet the following requirements: (a) they are created and managed by one or more qualified trust service providers; (b) they establish the origin of data records in the ledger; (c) they ensure the unique sequential chronological ordering of data records in the ledger; (d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger complies with the standards, specifications and procedures referred to in paragraph 3.		Пружалац квалификоване услуге од поверења вођења електронске евиденције дужан је да: 1) успоставља и води самостално, односно са другим пружаоцима услуге, електронску евиденцију; 2) утврђује порекло записа података у евиденцији; 3) обезбеди јединствен секвенцијални хронолошки редослед уписа података у евиденцију; 4) бележи податке тако да је свака накнадна промена података одмах уочљива, чиме се обезбеђује њихова целовитост, односно интегритет током времена. Евиденција коју води орган јавне власти сматра се квалификованом услугом вођења електронске евиденције ако испуњава услове из става 1. овог члана и ако се води у складу са законом којим се уређује електронска управа.	ПУ		
45l.3.	By 21 May 2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).			НИИ	Одредбом се даје овлашћење Европској комисији да доноси акте којим се ближе уређује наведено питање, због чега је одредба непреносива. Указујемо да је чланом 79. став 3. предвиђено да Министарство ближе прописује услове, стандарде, спецификације и процедуре које је потребно да испуни пружалац	

a)	a1)	б)	б1)	в)	г)	д)
					квалификоване услуге од поверења електронског архивирања	
46.	An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.	7.	Електронском документу не може се оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику.	ПУ		
46a.	Member States shall designate one or more supervisory bodies established in their territory. The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner. Member States shall notify to the Commission the names and the addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies. The role of the supervisory bodies designated pursuant to paragraph 1 shall be: (a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, by means of ex ante and ex post supervisory activities, that those providers and European Digital Identity Wallets they provide meet the requirements laid down in this Regulation; (b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, by means of ex post supervisory activities, when informed that providers or European Digital Identity Wallets that they provide infringe this Regulation. The tasks of the supervisory bodies designated pursuant to paragraph 1 shall include, in particular, the following: (a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;			НП	Одредбом се уређује вршење надзора над пружаоцима услуге издавања европског дигиталног идентитета, због чега је одредба непреносива. Указујемо да су члановима 81. и 82. уређени послови инспекције за електронску идентификацију и услуге од поверења у електронском пословању и њихова овлашћења. Такође, прекогранична сарадња у области електронске идентификације уређена је члановима 27-29. у којима је прописано да Министарство сарађује са надлежним међународним телима по питањима прекограничне интероперабилности шема електронске идентификације и предузима мере из своје надлежности како би се успоставила интероперабилност шема електронске идентификације на националном нивоу. као и да Министарство може признати сертификате издате у иностранству, под условом да су усклађени са међународним стандардима и да су издати од стране тела која испуњавају захтене прописане овим законом. Осим тога, Министарство Европској комисији може пријављивати регистроване шеме електронског идентитета које испуњавају услове из Уредбе eIDAS.	

a)	a1)	6)	61)	Б)	Г)	П)
	(b) to request information necessary to monitor compliance with this Regulation; (c) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breaches or loss of integrity of which they become aware in the performance of their tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require providers of European Digital Identity Wallet to do so where the supervisory body determines that disclosure of the security breach or of the loss of integrity would be in the public interest; (d) to carry out on-site inspections and off-site supervision; (e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation; (f) to suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 5b(7) in the case of illegal or fraudulent use of the European Digital Identity Wallet; (g) to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them without undue delay, where personal data protection rules appear to have been infringed and about security breaches which appear to constitute personal data breaches. Where the supervisory body designated pursuant to paragraph 1 requires the provider of a European Digital Identity Wallet to remedy any failure to fulfil requirements under this Regulation pursuant to					

a)	a1)	б)	б1)	в)	г)	д)
	paragraph 4, point (e), and that provider does not act accordingly and, if applicable, within a time limit set by that supervisory body, the supervisory body designated pursuant to paragraph 1 may, taking into account, in particular, the extent, duration and consequences of that failure, order the provider to suspend or to cease the provision of the European Digital Identity Wallet. The supervisory body shall inform the supervisory bodies of other Member States, the Commission, relying parties and users of the European Digital Identity Wallet without undue delay of the decision to require the suspension or cessation of the provision of the European Digital Identity Wallet. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council. By 21 May 2025, the Commission shall, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
46b.	Member States shall designate a supervisory body established in their territory or designate, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That supervisory body shall be responsible for supervisory tasks in the designating Member State as regards trust services. The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks. Member States shall notify to the Commission the names and addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent			НП	Одредбом се уређује вршење надзора над пружаоцима услуга од поверења, због чега је одредба непереносива. Указујемо да су члановима 81. и 82. уређени послови инспекције за електронску идентификацију и услуге од поверења у електронском пословању и њихова овлашћења. Такође, члановима 32-34. у којима је прописано да Министарство Министарство сарађује са надлежним органима других држава у вези са разменом података о нарушавању безбедности и интегритета услуга од	

a)	a1)	б)	б1)	в)	г)	д)
	changes thereto. The Commission shall publish a list of the notified supervisory bodies. The role of the supervisory bodies designated pursuant to paragraph 1 shall be: (a) to supervise qualified trust service providers established in the territory of the designating Member State and to ensure, by means of ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation; (b) to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, by means of ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation. The tasks of the supervisory body designated pursuant to paragraph 1 shall include in particular the following: (a) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breach or loss of integrity of which it becomes aware in the performance of its tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require the trust service provider to do so where the supervisory body determines that disclosure of the breach of security or loss of integrity would be in the public interest;				поверења, у складу са међународним споразумима, као и да Министарство: 1) обавештава надлежна тела страних држава о угрожавању безбедности или губитку целовитости који имају значајан утицај на пружену услугу од поверења или у њој садржане личне податке; 2) извештава Европску комисију о својим активностима у складу са Уредбом eIDAS, почев од дана ступања Републике Србије у чланство у Европској унији.	

a)	a1)	6)	61)	B)	Г)	Д)
	(b) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e; (c) to analyse the conformity assessment reports referred to in Article 20(1) and Article 21(1); (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article; (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2); (f) to cooperate with competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them, without undue delay, where personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches; (g) to grant qualified status to trust service providers and to the services they provide, and to withdraw that status in accordance with Articles 20 and 21; (h) to inform the body responsible for the national trusted list referred to in Article 22(3) of its decisions to grant or withdraw qualified status, unless that body is also the supervisory body designated pursuant to paragraph 1 of this Article; (i) to verify the existence and correct application of provisions on termination plans where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h); (j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation; (k) to investigate claims made by providers of web-browsers pursuant to Article 45a and to take action if necessary.					

a)	a1)	б)	б1)	в)	г)	д)
	Member States may require the supervisory body designated pursuant to paragraph 1 to establish, maintain and update a trust infrastructure in accordance with national law. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council. By 21 May 2025, the Commission shall adopt guidelines on the exercise by the supervisory bodies designated pursuant to paragraph 1 of this Article of the tasks referred to in paragraph 4 of this Article, and, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
46c.	Each Member State shall designate a single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes. Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member State. Each Member State shall make public and, without undue delay, notify to the Commission the names and the addresses of the single point of contact designated pursuant to paragraph 1 and any subsequent change thereto. The Commission shall publish a list of the single points of contact notified pursuant to paragraph 3.	27.	Министарство сарађује са надлежним међународним телима по питањима прекограничне интероперабилности шема електронске идентификације и предузима мере из своје надлежности како би се успоставила интероперабилност шема електронске идентификације на националном нивоу. Ради остваривања прекограничне интероперабилности успоставља се оквир интероперабилности који: 1) је технолошки неутралан; 2) примењује одговарајуће европске и међународне стандарде, нарочито у области информационе безбедности; 3) омогућава примену приватности по дизајну, укључујући минималну обраду података, селективно откривање идентитета, криптографску заштиту и спречавање профилисања, у складу са прописима о заштити података о личности.	ДП	Одредбом се уређује јединствену контакт тачку у оквиру ЕУ, због чега је одредба непреносива.	

а)	а1)	б)	б1)	в)	г)	д)
			Канцеларија успоставља и управља чвором у оквиру интероперабилности који омогућава прекограничну аутентификацију лица, чиме се обезбеђује да се инфраструктура електронске идентификације Републике Србије повеже са инфраструктуром електронске идентификације друге државе. У процесу управљања чвором из става 3. овог члана Канцеларија: 1) обезбеђује повезивање са чворовима других држава кроз оквир интероперабилности чије су шеме електронске идентификације саставни део Регистра из члана 22. овог закона, односно које су признате на основу међународног споразума; 2) примењује техничке и организационе мере заштите ради спречавања неовлашћеног приступа подацима који се размењују и обезбеђује интегритет податка, који се преносе између чворова употребом одговарајућих техничких решења и праксе; 3) обезбеђује да се подаци о личности не чувају или задржавају у чвору; 4) користи техничка решења која обезбеђују интегритет и аутентичност података, а која се користе приликом прекограничне размене података; 5) обезбеђује да чвор испуњава прописане услове који се односе на формат порука, структуру података и протоколе размене, у складу са важећим националним стандардима и регулативом, чиме се обезбеђује техничка интероперабилност и правна ваљаност прекограничне електронске идентификације; 6) обезбеђује достављање метаподатака о управљању чвором у стандардизованом, машински читљивом облику који је погодан за аутоматску обраду података на безбедан и поуздан начин; 7) обезбеђује аутоматску обраду параметара који се односе на безбедност, уз примену техничких и организационих мера које омогућавају континуирано праћење, евидентирање, анализу и реаговање на безбедносне догађаје, у складу са важећим националним стандардима и регулативом, без угрожавања приватности или интегритета података;			

a)	a1)	6)	61)	в)	г)	д)
			8) чува податке који би у случају инцидента омогућавали утврђивање места и врсте инцидента у законском року. 9) омогућава пренос података који обезбеђују поуздано представљање физичког или правног лица, на основу употребе регистроване шеме електронске идентификације приликом прекограничне сарадње у складу са законом. У поступцима прекограничне електронске идентификације примењују се технолошка решења која омогућавају недвосмислено утврђивање и упаривање идентитета физичких и правних лица, на основу електронских идентификационих средстава издатих у складу са признатим и регистрованим шемама електронске идентификације, а у складу са важећим техничким стандардима и прописима.			
46d.	In order to facilitate the supervision and enforcement of obligations under this Regulation, the supervisory bodies designated pursuant to Article 46a(1) and Article 46b(1) may seek, including through the Cooperation Group established pursuant to Article 46c (1), mutual assistance from the supervisory bodies of another Member State where the provider of the European Digital Identity Wallet or the trust service provider is established, or where its network and information systems are located or its services are provided. The mutual assistance shall at least entail that: (a) the supervisory body applying supervisory and enforcement measures in one Member State shall inform and consult the supervisory body from the other Member State concerned; (b) a supervisory body may request the supervisory body of another Member State concerned to take supervisory or enforcement measures, including, for instance, requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services;			НП	Одредбом се уређује вршење надзора над пружаоцима услуга од поверења, због чега је одредба непреносива. Указујемо да је одредбама 32-34. прописано да Министарство Министарство сарађује са надлежним органима других држава у вези са разном података о нарушавању безбедности и интегритета услуга од поверења, у складу са међународним споразумима, као и да Министарство: 1) обавештава надлежна тела страних држава о угрожавању безбедности или губитку целовитости који имају значајан утицај на пружену услугу од поверења или у њој садржане личне податке; 2) извештава Европску комисију о својим активностима у складу са Уредбом eIDAS, почев од дана ступања Републике Србије у чланство у Европској унији.	

a)	a1)	б)	б1)	в)	г)	д)
	(c) where appropriate, supervisory bodies may carry out joint investigations with the supervisory bodies of other Member States. The arrangements and procedures for joint actions under the first subparagraph shall be agreed upon and established by the Member States concerned in accordance with their national law. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds: (a) the assistance requested is not proportionate to the supervisory activities of the supervisory body carried out in accordance with Articles 46a and 46b; (b) the supervisory body is not competent to provide the requested assistance; (c) providing the requested assistance would be incompatible with this Regulation. By 21 May 2025 and every two years thereafter, the Cooperation Group established pursuant to Article 46e(1) shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2 of this Article.					
46e.	In order to support and facilitate Member States' cross-border cooperation and exchange of information on trust services, European Digital Identity Wallets and notified electronic identification schemes, the Commission shall establish a European Digital Identity Cooperation Group (the 'Cooperation Group'). The Cooperation Group shall be composed of representatives appointed by the Member States and of the Commission. The Cooperation Group shall be chaired by the Commission. The Commission shall provide the Cooperation Group's Secretariat. Representatives of relevant stakeholders may, on an ad hoc basis, be invited to attend meetings of the			НП	Одредбом се уређује вршење надзора над пружаоцима услуге издавања европског дигиталног идентитета, због чега је одредба непреносива. Указујемо да је члановима 27-29. уређена прекогранична сарадња у области електронске идентификације, у којима је прописано да Министарство сарађује са надлежним међународним телима по питањима прекограничне интероперабилности шема електронске идентификације и предузима мере из своје надлежности како би се успоставила интероперабилност шема електронске идентификације на националном нивоу, као и да	

a)	a1)	б)	б1)	в)	г)	д)
	Cooperation Group and to participate in its work as observers. ENISA shall be invited to participate as observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed. The Cooperation Group shall have the following tasks: (a) exchange advice and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services; (b) advise the Commission, as appropriate, in the early preparation of draft implementing and delegated acts to be adopted pursuant to this Regulation; (c) in order to support the supervisory bodies in the implementation of the provisions of this Regulation: (i) exchange best practices and information regarding the implementation of the provisions of this Regulation; (ii) assess the relevant developments in the digital identity wallet, electronic identification and trust services sectors; (iii) organise joint meetings with relevant interested parties from across the Union to discuss activities carried out by the cooperation group and gather input on emerging policy challenges; (iv) with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services; (v) exchange best practices in relation to the development and implementation of policies on the notification of security breaches, and common measures as referred to in Articles 5e and 10;				Министарство може признати сертификате издате у иностранству, под условом да су усклађени са међународним стандардима и да су издати од стране тела која испуњавају захтеве прописане овим законом. Осим тога, Министарство Европској комисији може пријављивати регистроване шеме електронског идентитета које испуњавају услове из Уредбе eIDAS. Министарство остварује сарадњу са Међународном унијом за телекомуникације у погледу израде Глобалног индекса сајбер безбедности, као и са Агенцијом Европске Уније за сајбер безбедност ЕНИСА учешћем у радној групи за електронску идентификацију и квалификоване услуге од поверења. ЦЕРТ-ови из Републике из Србије налазе се на Trusted Introducer листи, а Национални ЦЕРТ и ЦЕРТ МУП чланови су Forum of Incident Response and Security Teams организације.	

a)	a1)	б)	б1)	в)	г)	д)
	(vi) organise joint meetings with the NIS Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 to exchange relevant information in relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications; (vii) discuss, upon a request of a supervisory body, specific requests for mutual assistance as referred to in Article 46d; (viii) facilitate the exchange of information between the supervisory bodies by providing guidance on the organisational aspects and procedures for the mutual assistance referred to in Article 46d; (d) organise peer reviews of electronic identification schemes to be notified under this Regulation. Member States shall ensure effective and efficient cooperation of their designated representatives in the Cooperation Group. By 21 May 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraph 5, point (d), of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).					
47.	The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. The power to adopt delegated acts referred to in Article 5c(7), Article 24(4b) and Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014. The delegation of power referred to in Article 5c(7), Article 24 (4b) and Article 30(4) may be revoked at any time by the European Parliament or by the Council. A			НП	Одредба уређује питање поверавања надлежности Европској комисији за доношење аката на основу предметне уредбе.	

a)	a1)	б)	б1)	в)	г)	д)
	decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. A delegated act adopted pursuant to Article 5c(7), Article 24(4b) or Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.					
48.	The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.			НП	Одредбом се уређује образовање комитета који обавља послове заједно са Европском комисијом у вези са спровођењем ове уредбе.	
48a.	Member States shall ensure the collection of statistics in relation to the functioning of European Digital Identity Wallets and the qualified trust services provided on their territory. The statistics collected in accordance with paragraph 1 shall include the following: (a) the number of natural and legal persons having a valid European Digital Identity Wallet; (b) the type and number of services accepting the use of the European Digital Identity Wallet;			НП	Одредбом се уређује да Европска комисија испитује примену ове уредбе при коришћењу европских дигиталних новчаника и извештава Европски парламент и Савет о томе, због чега је ова одредаба непрениосива у пропис Републике Србије. Напомињемо да је одредбом 34. уређено да Министарство извештава Европску комисију о својим активностима у складу са Уредбом eIDAS, почев од дана	

a)	a1)	б)	б1)	в)	г)	д)
	(c) the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services; (d) a summary report including data on incidents preventing the use of the European Digital Identity Wallet; (e) a summary of significant security incidents, data breaches and affected users of European Digital Identity Wallets or of qualified trust services. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format. By 31 March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.				ступања Републике Србије у чланство у Европској унији.	
49.	The Commission shall review the application of this Regulation and shall, by 21 May 2026, submit a report to the European Parliament and to the Council. In that report, the Commission shall, in particular, evaluate whether it is appropriate to modify the scope of this Regulation or its specific provisions including, in particular, the provisions included in Article 5c(5), taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal to amend this Regulation. The report referred to in paragraph 1 shall include an assessment of the availability, security and usability of the notified electronic identification means and European Digital Identity Wallets that fall within the scope of this Regulation and assess whether all online private service providers relying on third-party electronic identification services for users authentication, shall be required to accept the use of notified electronic identification means and European Digital Identity Wallet.			НП	Одредбом се уређује да Европска комисија испитује примену ове уредбе и извештава Европски парламент и Савет о томе, због чега је ова одредба непрениосива у пропис Републике Србије. Напомињемо да је одредбом 34. уређено да Министарство извештава Европску комисију о својим активностима у складу са Уредбом eIDAS, почев од дана ступања Републике Србије у чланство у Европској унији.	

а)	а1)	б)	б1)	в)	г)	д)
	By 21 May 2030 and every four years thereafter, the Commission shall submit a report to the European Parliament and the Council on progress made towards achieving the objectives of this Regulation.					
50.	Directive 1999/93/EC is repealed with effect from 1 July 2016. References to the repealed Directive shall be construed as references to this Regulation.			НП	Одредбом се предвиђа престанак важења директиве ЕУ, због чега је одредба непреносива.	
51.1.	Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered to be qualified electronic signature creation devices under this Regulation until 21 May 2027.			НУ	Досадашњи прописи у овој области нису предвиђали оцену усаглашености средстава за креирање електронског потписа, услед чега се ова одредба није могла пренети.	
51.2.	Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until 21 May 2026.	91.3-6.	Даном ступања на снагу овог закона пружаоци квалификованих услуга од поверења који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге за коју су били регистровани. Даном ступања на снагу овог закона пружаоци услуга од поверења дуготрајног чувања који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге електронског архивирања и квалификовани пружаоци услуге чувања квалификованог електронског потписа, односно печата. Пужаоци услуга од поверења из ст. 3. и 4. овог члана дужни су да у року од 18 месеци од дана ступања на снагу овог закона ускладе своје пословање са одредбама овог закона и доставе	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			Министарству извештај о оцењивању усаглашености из члана 40. овог закона. Министарство врши оцењивање усаглашености из члана 40. овог закона до акредитације првог тела за оцењивање усаглашености, у складу са прописима.			
51.3.	The management of remote qualified electronic signature and seal creation devices by qualified trust service providers other than qualified trust service providers providing qualified trust services for the management of remote qualified electronic signature and seal creation devices in accordance with Articles 29a and 39a may be carried out without the need to obtain the qualified status for the provision of these management services until 21 May 2026.	91.3-6.	Даном ступања на снагу овог закона пружаоци квалификованих услуга од поверења који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге за коју су били регистровани. Даном ступања на снагу овог закона пружаоци услуга од поверења дуготрајног чувања који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге електронског архивирања и квалификовани пружаоци услуге чувања квалификованог електронског потписа, односно печата. Пружаоци услуга од поверења из ст. 3. и 4. овог члана дужни су да у року од 18 месеци од дана ступања на снагу овог закона ускладе своје пословање са одредбама овог закона и доставе Министарству извештај о оцењивању усаглашености из члана 40. овог закона. Министарство врши оцењивање усаглашености из члана 40. овог закона до акредитације првог тела за оцењивање усаглашености, у складу са прописима.	ПУ		
51.4.	Qualified trust service providers that have been granted their qualified status under this Regulation before 20 May 2024 shall submit a conformity assessment report to the supervisory body proving compliance with	91.3-6.	Даном ступања на снагу овог закона пружаоци квалификованих услуга од поверења који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021)	ДУ	Одредба само није усклађена у погледу рока за доставу извештаја о оцени усаглашености. Пружаоци квалификованих услуга од поверења бити дужни да доставе предметни	

a)	a1)	б)	б1)	в)	г)	д)
	Article 24(1), (1a) and (1b) as soon as possible and in any event by 21 May 2026.		настављају са радом као квалификовани пружаоци услуге за коју су били регистровани. Даном ступања на снагу овог закона пружаоци услуга од поверења дуготрајног чувања који су регистровани на основу закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/2017, 52/2021) настављају са радом као квалификовани пружаоци услуге електронског архивирања и квалификовани пружаоци услуге чувања квалификованог електронског потписа, односно печата. Пружаоци услуга од поверења из ст. 3. и 4. овог члана дужни су да у року од 18 месеци од дана ступања на снагу овог закона ускладе своје пословање са одредбама овог закона и доставе Министарству извештај о оцењивању усаглашености из члана 40. овог закона. Министарство врши оцењивање усаглашености из члана 40. овог закона до акредитације првог тела за оцењивање усаглашености, у складу са прописима.		извештај када се донесу подзаконска акта за примену овог закона.	
52.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. This Regulation shall apply from 1 July 2016, except for the following: (a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32 (3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014; (b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);			НП	Одредба предвиђа ступање на снагу ове уредбе, због чега је непреносива у домаћи пропис.	

a)	a1)	б)	б1)	в)	г)	д)
	(c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12 (8). 3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article. 4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public. This Regulation shall be binding in its entirety and directly applicable in all Member States.					
AI	Qualified certificates for electronic signatures shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name; (c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated; (d) electronic signature validation data that corresponds to the electronic signature creation data;	50.1.	Квалификовани електронски сертификат мора да садржи: 1) ознаку, у форми погодној за аутоматску обраду, да се електронски сертификат користи као квалификовани сертификат за електронски потпис, односно печат; 2) скуп података који јединствено идентификују квалификованог пружаоца услуге од поверења за издавање квалификованог електронског сертификата укључујући, најмање, земљу порекла пружаоца и назив пружаоца; 3) скуп података који јединствено идентификују потписника односно печатноца укључујући најмање: (1) за потписника: - име и презиме или псеудоним, а уколико је употребљен псеудоним то мора бити јасно	ПУ		

a)	a1)	6)	61)	в)	г)	д)
	(e) details of the beginning and end of the certificate's period of validity; (f) the certificate identity code, which must be unique for the qualified trust service provider; (g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge; (i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate; (i) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.		обележено у оквиру квалификованог електронског сертификата; - ЈМБГ, уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи ЈМБГ; - евиденцијски број странаца уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи евиденцијски број странаца; - број стране путне исправе из машински читљиве зоне путне исправе, односно број стране личне карте и ознаку земље издаваоца путне исправе, односно стране личне карте, као идентификациону ознаку странаца коју додељује Република Србија; (2) за печатноца: назив, држава и матични број односно јединствена идентификациона ознака у складу са правном регулативом те државе, уколико постоји; 4) податке за проверу електронског потписа односно електронског печата, који одговарају подацима за креирање тог електронског потписа односно електронског печата; 5) податке о почетку и крају важења квалификованог електронског сертификата; 6) серијски број квалификованог електронског сертификата, који мора бити јединствен у оквиру издаваоца квалификованог електронског сертификата; 7) напредни електронски потпис или напредни електронски печат издаваоца квалификованог електронског сертификата; 8) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа односно напредног електронског печата из тачке 7) овог става; 9) информацију о сервисима који врше проверу валидности сертификата; 10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата; 11) ознаку да су подаци за креирање електронског потписа односно печата, који одговарају подацима за Проверу електронског			

a)	a1)	б)	б1)	в)	г)	д)
			потписа односно печата из квалификованог електронског сертификата, садржани у квалификованом средству за креирање електронског потписа односно печата, уколико је тај услов испуњен.			
АШ	Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured; (b) the electronic signature creation data used for electronic signature creation can practically occur only once; (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology; (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.	53.1.4.	Квалификовано средство за креирање електронског потписа односно печата мора да, помоћу одговарајућих техничких решења и поступака, обезбеди: 1) поверљивост података за креирање електронског потписа односно печата; 2) да се подаци за креирање електронског потписа, односно печата појављују само једном; 3) да се подаци за креирање електронског потписа, односно печата не могу добити изван средства за креирање електронског потписа, односно печата употребом доступне технологије у разумном времену; 4) да је електронски потпис, односно печат поуздано заштићен од фалсификовања употребом доступне технологије; 5) могућност поуздане заштите података за креирање електронског потписа, односно печата од неовлашћеног коришћења. Средства за креирање квалификованог електронског потписа, односно печата, приликом креирања електронског потписа односно печата, не смеју променити податке који се потписују односно печатају или онемогућити потписнику, односно печатаоцу увид у те податке пре процеса креирања квалификованог електронског потписа односно печата. Квалификовано средство за креирање електронског потписа, односно печата на даљину (у даљем тексту: услуга управљања квалификованим средством на даљину) корисник квалификоване услуге од поверења може користити путем услуге управљања квалификованим средством за креирање електронског потписа, односно печата, што такође представља квалификовану услугу од поверења.	ПУ		

a)	a1)	6)	б1)	в)	г)	д)
			Изузетно од става 1. овог члана, квалификовани пружалац услуга од поверења из става 3. овог члана може израдити копију података за израду електронског потписа, односно печата у сврху заштите од губитка података ако: 1) израда и чување копија података за креирање квалификованог електронског потписа односно печата не умањују прописани ниво заштите тих података; 2) број израђених копија података за креирање електронског потписа односно печата није већи него што је то неопходно за обезбеђивање континуитета пружања услуге.			
AIII	Qualified certificates for electronic seals shall contain: (a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name; (c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records; (d) electronic seal validation data, which corresponds to the electronic seal creation data; (e) details of the beginning and end of the certificate's period of validity; (f) the certificate identity code, which must be unique for the qualified trust service provider;	50.1.	Квалификовани електронски сертификат мора да садржи: 12) ознаку, у форми погодној за аутоматску обраду, да се електронски сертификат користи као квалификовани сертификат за електронски потпис, односно печат; 13) скуп података који јединствено идентификују квалификованог пружаоца услуге од поверења за издавање квалификованог електронског сертификата укључујући, најмање, земљу порекла пружаоца и назив пружаоца; 14) скуп података који јединствено идентификују потписника односно печатиоца укључујући најмање: (3) за потписника: — име и презиме или псеудоним, а уколико је употребљен псеудоним то мора бити јасно обележено у оквиру квалификованог електронског сертификата; — ЈМБГ, уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи ЈМБГ; — евиденцијски број странца уколико је у захтеву за издавање сертификата потписник захтевао да сертификат садржи евиденцијски број странца;	ПУ		

a)	a1)	6)	б1)	в)	г)	д)
	(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge; (i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate; (j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate		– број стране путне исправе из машински чиљиве зоне путне исправе, односно број стране личне карте и ознаку земље издаваоца путне исправе, односно стране личне карте, као идентификациону ознаку странца коју додељује Република Србија; (4) за печатиоца: назив, држава и матични број односно јединствена идентификациона ознака у складу са правном регулативом те државе, уколико постоји; 15) податке за проверу електронског потписа односно електронског печата, који одговарају подацима за креирање тог електронског потписа односно електронског печата; 16) податке о почетку и крају важења квалификованог електронског сертификата; 17) серијски број квалификованог електронског сертификата, који мора бити јединствен у оквиру издаваоца квалификованог електронског сертификата; 18) напредни електронски потпис или напредни електронски печат издаваоца квалификованог електронског сертификата; 19) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа односно напредног електронског печата из тачке 7) овог става; 20) информацију о сервисима који врше проверу валидности сертификата; 21) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата; ознаку да су подаци за креирање електронског потписа односно печата, који одговарају подацима за проверу електронског потписа односно печата из квалификованог електронског сертификата, садржани у квалификованом средству за креирање електронског потписа односно печата, уколико је тај услов испуњен.			
ATV	Qualified certificates for website authentication shall contain:	69.1-2.	Квалификовани сертификати за аутентификацију веб сајтова садрже:	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name; (c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym; if a pseudonym is used, it shall be clearly indicated; (ca) for legal persons: a unique set of data unambiguously representing the legal person to whom the certificate is issued, with at least the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records; (d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records; (e) the domain name(s) operated by the natural or legal person to whom the certificate is issued; (f) details of the beginning and end of the certificate's period of validity; (g) the certificate identity code, which must be unique for the qualified trust service provider; (h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider; (i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;	1) ознаку, која се може препознати при аутоматској обради, да је сертификат издат као квалификовани сертификат за аутентификацију веб сајтова; 2) скуп података који недвосмислено представљају пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова, што обавезно укључује државу седишта, пословно име и матични број тог пружаоца услуге; 3) име и презиме или псеудоним физичког лица коме је издат сертификат, односно пословно име и матични број правног лица коме је издат сертификат; 4) адресу, односно седиште физичког или правног лица коме је издат сертификат; 5) назив интернет домена физичког или правног лица коме је издат сертификат; 6) податке о почетку и крају рока важења сертификата; 7) идентификациону ознаку сертификата која мора да буде јединствена за пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова; 8) напредан електронски потпис, или напредан електронски печат пружаоца услуге издавања квалификованих сертификата за аутентификацију веб сајтова; 9) локацију на којој је, без накнаде, доступан сертификат напредног електронског потписа, односно напредног електронског печата из тачке 8) овог става; 10) локацију услуге путем које се проверава статус валидности квалификованог електронског сертификата.					

a)	a1)	б)	б1)	в)	г)	д)
	(i) the information or the location of the certificate validity status services that can be used to enquire about the validity status of the qualified certificate.					
AV	Qualified electronic attestation of attributes shall contain: (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and: (i) for a legal person: the name and, where applicable, registration number as stated in the official records; (ii) for a natural person: the person's name; (c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated; (d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes; (e) details of the beginning and end of the attestation's period of validity; (f) the attestation identity code, which must be unique for the qualified trust service provider and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of; (g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;	71.2.	Квалификована електронска потврда атрибута садржи: 1) ознаку, која се може препознати при аутоматској обради, да је потврда издата као квалификована електронска потврда атрибута; 2) скуп података који недвосмислено идентификују пружаоца услуге од поверења који издаје квалификовану електронску потврду атрибута, укључујући податке о држави седишта, пословном имену и матичном броју; 3) скуп података који недвосмислено идентификују лице на које се односе потврђени атрибут, односно његов псеудоним ако га користи; 4) потврђен атрибут, односно атрибутс, и по потреби додатне информације о атрибуту; 5) податке о почетку и крају рока важења потврде; 6) идентификациону ознаку потврде јединствену за пружаоца квалификоване услуге од поверења и, по потреби, идентификациону ознаку, односно назнаку шеме аутентичног извора атрибута као и назив тог извора, односно назив евиденције, односно регистра у коме се води атрибут; 7) квалификован електронски потпис, односно квалификован електронски печат пружаоца квалификоване услуге од поверења који издаје потврду; 8) локацију на којој је, без накнаде, доступан сертификат квалификованог електронског потписа, односно печата из тачке 7) овог става;	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	(i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.		9) информације или локација услуге где се проверава валидност квалификоване електронске потврде.			
AVI	Pursuant to Article 45e, Member States shall ensure that measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with Union or national law and where these attributes rely on authentic sources within the public sector: 1. Address; 2. Age; 3. Gender; 4. Civil status; 5. Family composition; 6. Nationality or citizenship; 7. Educational qualifications, titles and licences; 8. Professional qualifications, titles and licences; 9. Powers and mandates to represent natural or legal persons; 10. Public permits and licences; 11. For legal persons, financial and company data.	72.1.	Пружалац квалификоване услуге од поверења који издаје електронске потврде атрибута, на захтев корисника, може вршити проверу аутентичности атрибута из изворних евиденција за следеће атрибуте о кориснику: 1) адресу пребивалишта, односно боравишта; 2) године; 3) пол; 4) брачно стање; 5) сродство; 6) чланове домаћинства; 7) држављанство; 8) ниво образовања и титуле; 9) занимање; 10) стручне лиценце; 11) овлашћења за заступање физичких и правних лица; 12) податке о адвокатима, јавним извршитељима, односно бележницима; 13) пословно име, адресу седишта као и финансијске податке правног лица, односно физичког лица у својству регистрованог субјекта.	ПУ		
AVII	An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source shall contain: (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by	73.1.	Орган јавне власти који води изворну евиденцију одређеног атрибута издаје, сам или преко овлашћеног лица, електронску потврду атрибута која садржи: 1) ознаку, која се може препознати при аутоматској обради, да је потврда издага као	ПУ		

a)	a1)	б)	б1)	в)	г)	д)
	or on behalf of a public body responsible for an authentic source; (b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official records; (c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated; (d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes; (e) details of the beginning and end of the attestation's period of validity; (f) the attestation identity code, which must be unique for the issuing public body and, if applicable, an indication of the scheme of attestations that the attestation of attributes is part of; (g) the qualified electronic signature or qualified electronic seal of the issuing body; (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge; (i) the information or location of the services that can be used to enquire about the validity status of the attestation.		електронска потврда атрибута коју издаје орган јавне власти; 2) скуп података који недвосмислено идентификују орган јавне власти који издаје електронску потврду атрибута, пословно име и матични број; 3) скуп података који недвосмислено идентификују лице на које се односи потврђени атрибут а ако се користи псеудоним, то мора бити јасно назначено; 4) потврђен атрибут, односно атрибуте, и по потреби додатне информације о атрибуту; 5) податке о почетку и крају рока важења потврде; 6) јединствена идентификациона ознака и назив евидениције, односно регистра у којем се атрибут води; 7) квалификован електронски потпис овлашћеног лица, односно квалификован електронски печат органа који издаје потврду; 8) локацију на којој је, без накнаде, доступан сертификат квалификованог електронског потписа, односно печата из тачке 7) овог става; 9) локацију на којој се може проверити валидност квалификоване електронске потврде.			