►B

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2015/1502

(2015. gada 8. septembris),

kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras

(Dokuments attiecas uz EEZ)

(OV L 235, 9.9.2015., 7. lpp.)

Grozīta ar:

		Oficiālais Vēstnesis		
		Nr.	Lappuse	Datums
►M1	Komisijas Īstenošanas regula (ES) 2022/960 (2022. gada 20. jūnijs)	L 165	40	21.6.2022.

▼B

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2015/1502

(2015. gada 8. septembris),

kas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū 8. panta 3. punktu nosaka elektroniskās identifikācijas līdzekļu uzticamības līmeņu minimālās tehniskās specifikācijas un procedūras

(Dokuments attiecas uz EEZ)

1. pants

1. Izziņotas elektroniskās identifikācijas shēmas ietvaros izdoto elektroniskās identifikācijas līdzekļu zemo, būtisko un augsto uzticamības līmeni nosaka ar atsauci uz pielikumā izklāstītajām specifikācijām un procedūrām.

2. Pielikumā izklāstītās specifikācijas un procedūras izmanto, lai izraudzītos elektroniskās identifikācijas shēmas ietvaros izdoto elektroniskās identifikācijas līdzekļu uzticamības līmeni, nosakot šādu elementu drošu izmantojamību un kvalitāti:

a) uzņemšana – kā izklāstīts šīs regulas pielikuma 2.1. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta a) apakšpunktu;

b) elektroniskās identifikācijas līdzekļu pārvaldība – kā izklāstīts šīs regulas pielikuma 2.2. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta b) un f) apakšpunktu;

c) autentifikācija – kā izklāstīts šīs regulas pielikuma 2.3. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta c) apakšpunktu;

d) pārvaldība un organizācija – kā izklāstīts šīs regulas pielikuma 2.4. punktā saskaņā ar Regulas (ES) Nr. 910/2014 8. panta 3. punkta d) un e) apakšpunktu.

3. Ja izziņotas elektroniskās identifikācijas shēmas ietvaros izdotais elektroniskās identifikācijas līdzeklis atbilst prasībai, kas minēta pie augstāka uzticamības līmeņa, uzskatāms, ka tas apmierina līdzvērtīgu zemāka uzticamības līmeņa prasību.

4. Ja attiecīgajā pielikuma daļā nav noteikts citādi, tad, lai panāktu pieprasīto uzticamības līmeni, ir jāapmierina visi elementi, kas pielikumā norādīti pie elektroniskās identifikācijas shēmas ietvaros izdota elektroniskās identifikācijas līdzekļa konkrēta uzticamības līmeņa.

2. pants

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

▼B

PIELIKUMS

Izziņotas elektroniskās identifikācijas shēmas ietvaros izdoto elektroniskās identifikācijas līdzekļu zema, būtiska un augsta uzticamības līmeņa tehniskās specifikācijas un procedūras

1. **Piemērojamās definīcijas**

Šajā pielikumā piemēro šādas definīcijas:

1) "autoritatīvs avots" – jebkura veida avots, uz kuru var paļauties, ka tas sniedz precīzus datus, informāciju un/vai pierādījumu, ko var izmantot identitātes pierādīšanai;

2) "autentifikācijas faktors" – faktors, kas apstiprināts par saistītu ar personu un ietilpst kādā no šīm kategorijām:

a) *"turējumā balstīts autentifikācijas faktors"* – autentifikācijas faktors, kurā subjektam ir jāpierāda, ka tas ir viņa turējumā;

b) *"zināšanā balstīts autentifikācijas faktors"* – autentifikācijas faktors, kurā subjektam ir jāpierāda, ka viņš to zina;

c) *"piemitīgs autentifikācijas faktors"* – autentifikācijas faktors, kas balstās uz fiziskas personas fizisku īpašību un par kuru subjektam ir jāpierāda, ka viņam piemīt šī fiziskā īpašība;

3) "dinamiskā autentifikācija" – elektronisks process, kurā izmanto kriptogrāfiju vai citas metodes, kas dod iespēju pēc pieprasījuma izveidot elektronisku pierādījumu tam, ka subjekta pārziņā vai turējumā ir identifikācijas dati, un kas mainās līdzi katrai autentifikācijai starp subjektu un sistēmu, kura verificē subjekta identitāti;

4) "informācijas drošības pārvaldības sistēma" – procesu un procedūru kopums, kura uzdevums ir informācijas drošības apdraudējumu noturēt pieņemamā līmenī.

2. **Tehniskās specifikācijas un procedūras**

Šajā pielikumā izklāstīto tehnisko specifikāciju un procedūru elementus izmanto, lai noteiktu, kā Regulas (ES) Nr. 910/2014 8. panta prasības un kritērijus piemērot elektroniskās identifikācijas shēmas ietvaros izsniegtiem elektroniskās identifikācijas līdzekļiem.

2.1. *Uzņemšana*

2.1.1. Pieteikšanās un reģistrēšanās

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Nodrošina, ka pieteikuma iesniedzējs zina noteikumus, kas saistīti ar elektroniskās identifikācijas līdzekļu lietošanu. 2. Nodrošina, ka pieteikuma iesniedzējs zina ieteiktos piesardzības pasākumus, kas saistīti ar elektroniskās identifikācijas līdzekļiem. 3. Vāc attiecīgos personas datus, kas vajadzīgi identitātes pierādīšanai un verificēšanai.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

▼B

2.1.2. Identitātes pierādīšana un verificēšana (fiziskai personai)

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Var pieņemt, ka personai ir pierādījums, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, un tas atspoguļo uzdoto identitāti. 2. Pierādījumus var uzskatīt par patiesiem vai tādiem, kas pastāv pēc autoritatīva avota ziņām, un pierādījumi šķiet derīgi. 3. Autoritatīvais avots zina, ka uzdotā identitāte pastāv, un var tikt uzskatīts, ka persona, kura uzdod identitāti, ir tā pati.
Būtisks	Jāizpilda zemais līmenis plus viena no alternatīvām 1.–4. punktā: 1. Ir verificēts, ka personai ir pierādījums, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, un tā atbilst uzdotajai identitātei, un ir pārbaudīts pierādījuma patiesums; vai pēc autoritatīva avota ziņām tas pastāv un attiecas uz īstu personu, un ir veikti pasākumi, lai minimalizētu risku, ka personas identitāte nav uzdotā identitāte, ņemot vērā risku, ka var būt, piemēram, nozaudēts, nozagts, apturēts, anulēts vai notecējis pierādījums. vai 2. Reģistrēšanās laikā tiek iesniegts personas dokuments dalībvalstī, kurā šis dokuments izdots, un šķiet, ka dokuments attiecas uz tā uzrādītāju, un ir veikti pasākumi, lai minimalizētu risku, ka personas identitāte nav uzdotā identitāte, ņemot vērā risku, ka var būt, piemēram, nozaudēti, nozagti, apturēti, anulēti vai notecējuši dokumenti. vai 3. Ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.2. punktā attiecībā uz būtisku uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Eiropas Parlamenta un Padomes Regulas (EK) Nr. 765/2008 ([1]) 2. panta 13. punktā, vai līdzvērtīga struktūra. vai 4. Ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir būtisks vai augsts, un ņem vērā personas identifikācijas datu maiņas riskus, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, būtiskais vai augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai.

▼B

Uzticamības līmenis	Nepieciešamie elementi
Augsts	Jāizpilda 1. vai 2. punkta prasības: 1. Jāizpilda būtiskais līmenis plus viena no alternatīvām a)–c) apakšpunktā: a) ja ir verificēts, ka personai ir fotogrāfiskās vai biometriskās identifikācijas pierādījums, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, un minētais pierādījums atspoguļo uzdoto identitāti, pierādījumu pārbauda, lai noteiktu, vai tas ir derīgs pēc autoritatīva avota ziņām, un pieteikuma iesniedzējs tiek identificēts ar uzdoto identitāti, salīdzinot vienu vai vairākas personas fiziskās īpašības ar autoritatīvu avotu; vai b) ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.2. punktā attiecībā uz augstu uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīga struktūra, un tiek veikti pasākumi, kas pierāda, ka agrākās procedūras rezultāti vēl ir derīgi, vai c) ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir augsts, un ņem vērā personas identifikācijas datu maiņas riskus, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai, un tiek veikti pasākumi, kas pierāda, ka iepriekšējās šā izziņotā elektroniskās identifikācijas līdzekļa izdošanas procedūras rezultāti vēl ir derīgi. VAI 2. Ja pieteikuma iesniedzējs neuzrāda atzītu fotogrāfiskās vai biometriskās identifikācijas pierādījumu, piemēro tieši tās pašas procedūras, ko tāda atzīta fotogrāfiskās vai biometriskās identifikācijas pierādījuma iegūšanai valsts līmenī izmanto par reģistrāciju atbildīgās dalībvalsts vienība.

([1]) Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Regula (EK) Nr. 765/2008, ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93 (OV L 218, 13.8.2008., 30. lpp.).

2.1.3. Identitātes pierādīšana un verificēšana (juridiskai personai)

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Juridiskās personas uzdoto identitāti apliecina uz tādu pierādījumu pamata, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli.

▼B

Uzticamības līmenis	Nepieciešamie elementi
	2. Pierādījumi šķietami ir derīgi un tos var uzskatīt par patiesiem vai pastāvošiem pēc autoritatīvu avota ziņām, ja juridiskas personas iekļāvums autoritatīvajā avotā ir brīvprātīgs un to reglamentē juridiskās personas un autoritatīvā avota vienošanās. 3. Autoritatīvam avotam nav zināms, ka juridiskā persona būtu statusā, kas tai neļauj rīkoties kā šai juridiskajai personai.
Būtisks	Jāizpilda zemais līmenis plus viena no alternatīvām 1.–3. punktā: 1. Juridiskās personas uzdoto identitāti apliecina uz tādu pierādījumu pamata, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, ieskaitot juridiskās personas nosaukumu, juridisko formu un (attiecīgā gadījumā) reģistrācijas numuru, un pierādījumus pārbauda, lai noteiktu, vai tie ir patiesi vai pastāv pēc autoritatīva avota ziņām, ja juridiskajai personai ir jābūt iekļautai autoritatīvajā informācijas avotā, lai darbotos savā nozarē, un ir veikti pasākumi, lai minimalizētu risku, ka juridiskās personas identitāte nav uzdotā identitāte, ņemot vērā risku, ka var būt, piemēram, nozaudēti, nozagti, apturēti, anulēti vai notecējuši dokumenti. vai 2. Ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.3. punktā attiecībā uz būtisku uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīga struktūra. vai 3. Ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir būtisks vai augsts, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, būtiskais vai augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai.
Augsts	Jāizpilda būtiskais līmenis plus viena no alternatīvām 1.–3. punktā: 1. Juridiskās personas uzdoto identitāti apliecina uz tādu pierādījumu pamata, ko atzīst dalībvalsts, kurā tiek iesniegts pieteikums uz elektroniskās identifikācijas līdzekli, ieskaitot juridiskās personas nosaukumu, juridisko formu un vismaz vienu unikālu identifikatoru, kas atspoguļo juridisko personu un ko lieto valsts vajadzībām, un ir pārbaudīts pierādījuma derīgums pēc autoritatīva avota ziņām. vai

▼B

Uzticamības līmenis	Nepieciešamie elementi
	2. Ja procedūras, ko publiska vai privāta vienība agrāk izmantojusi tajā pašā dalībvalstī citam nolūkam, nevis elektroniskās identifikācijas līdzekļu izdošanai, nodrošina uzticamību, kas līdzvērtīga tai, kas minēta 2.1.3. punktā attiecībā uz augstu uzticamības līmeni, tad vienībai, kas atbild par reģistrāciju, nav jāatkārto iepriekšējās procedūras, ja šādu līdzvērtīgu uzticamību apstiprina atbilstības novērtēšanas struktūra, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīga struktūra, un tiek veikti pasākumi, kas pierāda, ka agrākās procedūras rezultāti vēl ir derīgi. vai 3. Ja elektroniskās identifikācijas līdzekļus izdod uz tāda derīga izziņota elektroniskās identifikācijas līdzekļa pamata, kura uzticamības līmenis ir augsts, nav vajadzīgs atkārtot identitātes pierādīšanas un verifikācijas procesus. Ja elektroniskās identifikācijas līdzeklis, kas ir par pamatu, nav izziņots, augstais uzticamības līmenis ir jāapstiprina atbilstības novērtēšanas struktūrai, kas minēta Regulas (EK) Nr. 765/2008 2. panta 13. punktā, vai līdzvērtīgai struktūrai, un tiek veikti pasākumi, kas pierāda, ka iepriekšējās šā izziņotā elektroniskās identifikācijas līdzekļa izdošanas procedūras rezultāti vēl ir derīgi.

2.1.4. Fizisku un juridisku personu elektroniskās identifikācijas līdzekļu saistījums

Attiecīgos gadījumos uz starp fiziskas personas elektroniskās identifikācijas līdzekļa un juridiskas personas elektroniskās identifikācijas līdzekļa saistījumu (“saistījumu”) attiecas šādi nosacījumi:

1. Jābūt iespējai saistījumu apturēt un/vai anulēt. Saistījuma darbības ciklu (piemēram, aktivizēšanu, apturēšanu, atjaunošanu, anulēšanu) pārvalda saskaņā ar valsts atzītām procedūrām.

2. Fiziska persona, kuras elektroniskās identifikācijas līdzeklis ir saistīts ar juridiskās personas elektroniskās identifikācijas līdzekli, var deleģēt saistījuma īstenošanu citai fiziskai personai, pamatojoties uz valsts atzītām procedūrām. Tomēr atbildība paliek deleģējošajai fiziskajai personai.

3. Saistījums veidojams šādi:

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Fiziskas personas, kas darbojas juridiskās personas vārdā, identitātes pierādīšanu verificē kā veiktu zemajā līmenī vai augstākā. 2. Saistījums ir izveidots, pamatojoties uz valsts atzītām procedūrām. 3. Autoritatīvam avotam nav zināms, ka fiziskā persona būtu statusā, kas tai neļauj rīkoties juridiskās personas vārdā.
Būtisks	Zemā līmeņa 3. punkts plus: 1. Fiziskas personas, kas darbojas juridiskās personas vārdā, identitātes pierādīšanu verificē kā veiktu būtiskajā vai augstajā līmenī. 2. Saistījums ir izveidots, pamatojoties uz valsts atzītām procedūrām, kuru rezultātā saistījums reģistrēts autoritatīvā avotā. 3. Saistījums ir verificēts, pamatojoties uz informāciju no autoritatīva avota.

▼B

Uzticamības līmenis	Nepieciešamie elementi
Augsts	Zemā līmeņa 3. punkts un būtiskā līmeņa 2. punkts plus: 1. Fiziskas personas, kas darbojas juridiskās personas vārdā, identitātes pierādīšanu verificē kā veiktu augstajā līmenī. 2. Saistījums ir verificēts, pamatojoties uz unikālu identifikatoru, kas apzīmē juridisko personu un ko lieto valsts vajadzībām, un pamatojoties uz autoritatīva avota informāciju, kas unikāli apzīmē fizisko personu.

2.2. *Elektroniskās identifikācijas līdzekļu pārvaldība*

2.2.1. Elektroniskās identifikācijas līdzekļu īpašības un izveids

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Elektroniskās identifikācijas līdzeklis izmanto vismaz vienu autentifikācijas faktoru. 2. Elektroniskās identifikācijas līdzeklis ir veidots tā, ka izdevējs veic piemērotus pasākumus, lai pārliecinātos, ka to izmanto tikai tās personas kontrolē vai turējumā, kurai tas pieder.
Būtisks	1. Elektroniskās identifikācijas līdzeklis izmanto vismaz divus dažādu kategoriju autentifikācijas faktorus. 2. Elektroniskās identifikācijas līdzeklis ir veidots tā, lai var pieņemt, ka to izmanto tikai tad, ja tas ir tās personas kontrolē vai turējumā, kurai tas pieder.
Augsts	Būtiskais līmenis plus: 1. Elektroniskās identifikācijas līdzeklis sargā no dublēšanas un viltošanas, kā arī no uzbrucējiem ar augstu uzbrukuma potenciālu. 2. Elektroniskās identifikācijas līdzeklis ir veidots tā, lai persona, kurai tas pieder, to varētu droši aizsargāt tā, ka to neizmanto citi.

2.2.2. Izdošana, piegāde un aktivizācija

Uzticamības līmenis	Nepieciešamie elementi
Zems	Pēc izdošanas elektroniskās identifikācijas līdzekli piegādā ar mehānismu, kura izmantošana ļauj pieņemt, ka tas nonāk tikai pie personas, kam tas paredzēts.
Būtisks	Pēc izdošanas elektroniskās identifikācijas līdzekli piegādā ar mehānismu, kura izmantošana ļauj pieņemt, ka tas nonāk tikai tās personas turējumā, kam tas pieder.
Augsts	Aktivizēšanas process verificē, vai elektroniskās identifikācijas līdzeklis ir nonācis tikai tās personas turējumā, kurai tas pieder.

2.2.3. Apturēšana, anulēšana un reaktivizācija

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Elektroniskās identifikācijas līdzekli ir iespējams laicīgi un efektīvi apturēt un/vai anulēt. 2. Ir veikti pasākumi, kas novērš neautorizētu apturēšanu, anulēšanu un/vai reaktivizāciju. 3. Reaktivizācija notiek tikai tad, ja joprojām tiek apmierinātas tādas pašas uzticamības prasības, kādas izvirzītas pirms apturēšanas vai anulēšanas.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

▼B

2.2.4. Atjaunošana un aizstāšana

Uzticamības līmenis	Nepieciešamie elementi
Zems	Ņemot vērā risku, ka var mainīties personas identifikācijas dati, atjaunošanai vai aizstāšanai jāizpilda tādas pašas uzticamības prasības kā sākotnējā identitātes pierādīšanā un verifikācijā vai ir jābūt balstītai uz derīgu tāda paša vai augstāka uzticamības līmeņa elektroniskās identifikācijas līdzekli.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Zemais līmenis plus: ja atjaunošana vai aizstāšana ir balstīta uz elektroniskās identifikācijas līdzekli, identitātes datus verificē pēc autoritatīva avota.

2.3. *Autentifikācija*

Šajā punktā uzmanība veltīta briesmām, kas saistās ar autentifikācijas mehānisma lietošanu, un uzskaitītas prasības katrā uzticamības līmenī. Šajā punktā tiek uzskatīts, ka kontrole ir samērīga ar riskiem dotajā līmenī.

2.3.1. Autentifikācijas mehānisms

Tabulā ir izklāstītas prasības katrā uzticamības līmenī attiecībā uz autentifikācijas mehānismu, kurā fiziskā vai juridiskā persona izmanto elektroniskās identifikācijas līdzekli, lai apstiprinātu savu identitāti pārbaudītājam.

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Pirms personas identifikācijas datu izlaišanas tiek droši verificēts elektroniskās identifikācijas līdzeklis un tā derīgums. 2. Ja personas identifikācijas dati tiek glabāti kā daļa no autentifikācijas mehānisma, minētā informācija ir aizsargāta, lai nodrošinātos pret nozaudēšanu un drošības politikas pārkāpumiem, ieskaitot analīzi bezsaistē. 3. Autentifikācijas mehānisms īsteno drošības kontroli elektroniskās identifikācijas līdzekļu verifikācijai tā, ka ir maz ticams, ka tādas uzbrucēja ar vairāk nekā parastu uzbrukuma potenciālu darbības kā paziņojuma uzminēšana, pārtveršana, pārspēlēšana vai manipulācijas ar to spētu vājināt autentifikācijas mehānismus.
Būtisks	Zemais līmenis plus: 1. Pirms personas identifikācijas datu izlaišanas ar dinamisko autentifikāciju tiek droši verificēts elektroniskās identifikācijas līdzeklis un tā derīgums. 2. Autentifikācijas mehānisms īsteno drošības kontroli elektroniskās identifikācijas līdzekļu verifikācijai tā, ka ir maz ticams, ka tādas uzbrucēja ar vidēji augstu uzbrukuma potenciālu darbības kā paziņojuma uzminēšana, pārtveršana, pārspēlēšana vai manipulācijas ar to spētu vājināt autentifikācijas mehānismus.
Augsts	Būtiskais līmenis plus: autentifikācijas mehānisms īsteno drošības kontroli elektroniskās identifikācijas līdzekļu verifikācijai tā, ka ir maz ticams, ka tādas uzbrucēja ar augstu uzbrukuma potenciālu darbības kā paziņojuma uzminēšana, pārtveršana, pārspēlēšana vai manipulācijas ar to spētu vājināt autentifikācijas mehānismus.

▼B

2.4. *Pārvaldība un organizācija*

Visiem dalībniekiem, kas ar elektronisko identifikāciju saistītu pakalpojumu sniedz pārrobežu kontekstā (“pakalpojuma sniedzēji”), ir jābūt dokumentētai informācijas drošības pārvaldības praksei, rīcības politikai, riska pārvaldības pieejām un citiem atzītiem kontroles līdzekļiem, lai attiecīgām elektroniskās identifikācijas shēmu vadības struktūrām attiecīgajās dalībvalstīs sniegtu pārliecību, ka pastāv efektīva prakse. Visā 2.4. punktā visas prasības/elementus uzskata par samērīgiem ar dotā līmeņa riskiem.

2.4.1. Vispārīgi noteikumi

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Pakalpojuma sniedzēji, kas nodrošina darbības pakalpojumus, uz ko attiecas šī regula, ir publiska iestāde vai juridiska vienība, ko par tādu atzīst kādas dalībvalsts tiesību akti un kam ir izveidota organizatoriskā struktūra un pilnībā darbojas visas daļas, kas vajadzīgas pakalpojumu sniegšanai. 2. Pakalpojumu sniedzēji ievēro juridiskās prasības, kas tiem izvirzītas sakarā ar darbību un pakalpojuma sniegšanu, ieskaitot jautājumos par pieprasāmās informācijas veidiem, identitātes pierādīšanas veidu, par to, kāda informāciju drīkst paturēt un cik ilgi. 3. Pakalpojumu sniedzēji spēj pierādīt spēju uzņemties risku sakarā ar atbildību par zaudējumiem, kā arī to, ka viņiem pietiek finanšu resursu nepārtrauktai darbībai un pakalpojumu sniegšanai. 4. Pakalpojumu sniedzēji atbild par citām vienībām ārpakalpojumu veidā nodoto saistību izpildi un par to, lai shēmas politika būtu ievērota tā, it kā pienākumus būtu pildījuši paši pakalpojumu sniedzēji. 5. Elektroniskās identifikācijas shēmām, kas nav izveidotas ar valsts tiesību aktiem, ir jābūt efektīvam darbības izbeigšanas plānam. Plānā jābūt noteiktai kārtībai, kā pakalpojums tiek izbeigts vai kā to turpina cits pakalpojumu sniedzējs, kā informējamas attiecīgās iestādes un galalietotāji, kā arī ziņas par to, kā uzskaites dati ir jāaizsargā, jāsaglabā un jāiznīcina saskaņā ar shēmas politiku.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.4.2. Publicētie paziņojumi un informācija lietotājiem

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Ir publicēta pakalpojuma definīcija, kas aptver visus piemērojamos noteikumus un maksas, ieskaitot tā izmantošanas ierobežojumus (ja tādi ir). Pakalpojuma definīcijā ietilpst privātuma politika. 2. Ir jāievieš atbilstoša politika un procedūras, lai nodrošinātu, ka pakalpojuma lietotāji laicīgi un droši tiek informēti par izmaiņām pakalpojuma definīcijā un piemērojamajos noteikumos un privātuma politikā. 3. Ir jāievieš atbilstoša rīcības politika un procedūras, kas nodrošina pilnīgas un pareizas atbildes uz informācijas pieprasījumiem.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

▼B

2.4.3. Informācijas drošības pārvaldība

Uzticamības līmenis	Nepieciešamie elementi
Zems	Pastāv efektīva informācijas drošības pārvaldības sistēma informācijas drošības risku pārvaldībai un kontrolei.
Būtisks	Zemais līmenis plus: informācijas drošības pārvaldības sistēma ievēro pārbaudītus informācijas drošības risku pārvaldības un kontroles standartus vai principus.
Augsts	Tāpat kā būtiskajā līmenī.

2.4.4. Uzskaite

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Reģistrē un uztur attiecīgu informāciju, izmantojot efektīvu uzskaitvedības sistēmu, ņemot vērā piemērojamos tiesību aktus un labu praksi, kas attiecas uz datu aizsardzību un datu saglabāšanu. 2. Saglabā, cik to ļauj valsts tiesību akti vai citi valsts administratīvi noteikumi, un aizsargā uzskaites datus tik ilgi, kamēr tie ir nepieciešami revīzijai un drošības pārkāpumu izmeklēšanai, un saglabāšanai, pēc kuras uzskaites datus drošā veidā iznīcina.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

2.4.5. Iekārtas un personāls

Tabulā ir norādītas prasības iekārtām un darbiniekiem un – attiecīgā gadījumā – apakšuzņēmējiem, kas uzņemas pienākumus, uz kuriem attiecas šī regula. Katras prasības izpilde ir proporcionāla riskam, kas saistās ar uzticamības līmeni.

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Pastāv procedūras, kas nodrošina, ka darbinieki un apakšuzņēmēji ir pietiekami apmācīti, kvalificēti un pieredzējuši prasmēs, kas nepieciešamas viņu funkciju pildīšanai. 2. Pietiek personāla un apakšuzņēmēju pakalpojuma pienācīgai sniegšanai un apgādei ar resursiem saskaņā ar tā politiku un procedūrām. 3. Iekārtas, ko izmanto pakalpojuma sniegšanai, pastāvīgi uzrauga un aizsargā pret dabas untumu nodarīto kaitējumu, neatļautu piekļuvi un citiem faktoriem, kas var ietekmēt pakalpojuma drošību. 4. Pakalpojuma sniegšanai izmantojamās iekārtas nodrošina piekļūšanu personas datu un kriptogrāfiskas vai citādas sensitīvas informācijas apstrādes zonām tikai pilnvarotiem darbiniekiem vai apakšuzņēmējiem.
Būtisks	Tāpat kā zemajā līmenī.
Augsts	Tāpat kā zemajā līmenī.

▼B

2.4.6. Tehniskā kontrole

Uzticamības līmenis	Nepieciešamie elementi
Zems	1. Samērīga tehniskā kontrole, aizsargādama apstrādātās informācijas konfidencialitāti, integritāti un pieejamību, pārvalda riskus, kas apdraud pakalpojumu drošību. 2. Elektronisko sakaru kanāli, ko izmanto personas datu vai sensitīvas informācijas apmaiņai, ir aizsargāti no pārtveršanas, manipulēšanas un pārspēlēšanas. 3. Piekļuve sensitīviem kriptogrāfiskiem materiāliem, ko izmanto elektroniskās identifikācijas līdzekļu izdošanai un autentifikācijai, tiek dota tikai funkcijām un lietojumiem, kam piekļuve noteikti nepieciešama. Ir jānodrošina, ka šādus materiālus nekad pastāvīgi neuzglabā kā vienkāršu tekstu. 4. Pastāv procedūras, kas nodrošina, ka drošība tiek uzturēta pastāvīgi un ka ir spēja reaģēt uz riska līmeņa maiņu, incidentiem un drošības pārkāpumiem. 5. Visus informācijas nesējus ar personas datiem, kriptogrāfisku vai citādu sensitīvu informāciju uzglabā, pārvadā un likvidē drošā un aizsargātā veidā.
Būtisks	Tāpat kā zemajā līmenī plus: sensitīvi kriptogrāfiskie materiāli, ko izmanto elektroniskās identifikācijas līdzekļu izdošanai un autentifikācijai, ir aizsargāti no viltošanas.
Augsts	Tāpat kā būtiskajā līmenī.

2.4.7. Atbilstība un revīzija

Uzticamības līmenis	Nepieciešamie elementi
Zems	Pastāv regulāra iekšējā revīzija, kas aptver visas daļas, kuras attiecas uz sniegto pakalpojumu piegādi, nodrošinot atbilstību attiecīgajai politikai.
Būtisks	Pastāv regulāra neatkarīga iekšējā revīzija vai ārējā revīzija, kas aptver visas daļas, kuras attiecas uz sniegto pakalpojumu piegādi, nodrošinot atbilstību attiecīgajai politikai.
Augsts	1. Pastāv regulāra neatkarīga ārējā revīzija, kas aptver visas daļas, kas attiecas uz sniegto pakalpojumu piegādi, nodrošinot atbilstību attiecīgajai politikai. 2. Ja shēmu tieši pārvalda valsts pārvaldes struktūra, shēmas revīziju veic saskaņā ar attiecīgās valsts tiesību aktiem.