Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/2982

4.12.2024.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2024/2982

(2024. gada 28. novembris),

ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes satvara atbalstāmajiem protokoliem un saskarnēm

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2014. gada 23. jūlija Regulu (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK ([1]), un jo īpaši tās 5.a panta 23. punktu,

tā kā:

(1) Eiropas digitālās identitātes satvars, kas izveidots ar Regulu (ES) Nr. 910/2014, ir būtisks drošas un sadarbspējīgas digitālās identitātes ekosistēmas izveides elements visā Savienībā. Eiropas digitālās identitātes maki ("maki") ir satvara stūrakmens, un tā mērķis ir atvieglot fizisku un juridisku personu piekļuvi pakalpojumiem visās dalībvalstīs, vienlaikus nodrošinot personas datu un privātuma aizsardzību.

(2) Visām šajā regulā paredzētajām personas datu apstrādes darbībām piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([2]) un, attiecīgā gadījumā, Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([3]).

(3) Regulas (ES) Nr. 910/2014 5.a panta 23. punktā Komisija ir pilnvarota vajadzības gadījumā noteikt attiecīgās specifikācijas un procedūras. To panāk ar četrām īstenošanas regulām, kuras attiecas uz: protokoliem un saskarnēm – Komisijas Īstenošanas regula (ES) 2024/2982 ([4]); integritāti un pamatfunkcijām – Komisijas Īstenošanas regula (ES) 2024/2979 ([5]); personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem – Komisijas Īstenošanas regula (ES) 2024/2977 ([6]), kā arī paziņojumiem Komisijai – Komisijas Īstenošanas regula (ES) 2024/2980 ([7]). Šajā regulā ir noteiktas attiecīgās prasības protokoliem un saskarnēm.

([1]) (OV L 257, 28.8.2014., 73. lpp., ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([2]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Komisijas Īstenošanas regula (ES) 2024/2982 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes satvara atbalstāmajiem protokoliem un saskarnēm (OV L, 2024/2982, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Komisijas Īstenošanas regula (ES) 2024/2979 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes maku integritāti un pamatfunkcijām (OV L, 2024/2979, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Komisijas Īstenošanas regula (ES) 2024/2977 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes makiem izsniegtajiem personas identifikācijas datiem un atribūtu elektroniskajiem apliecinājumiem (OV L, 2024/2977, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Komisijas Īstenošanas regula (ES) 2024/2980 (2024. gada 28. novembris), ar ko paredz noteikumus par to, kā Eiropas Parlamenta un Padomes Regula (ES) Nr. 910/2014 piemērojama attiecībā uz paziņojumiem Komisijai par Eiropas digitālās identitātes maku ekosistēmu (OV L, 2024/2980, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komisija regulāri novērtē jaunās tehnoloģijas, praksi, standartus un tehniskās specifikācijas. Lai nodrošinātu visaugstāko saskaņotības līmeni starp dalībvalstīm attiecībā uz maku izstrādi un sertifikāciju, šajā regulā izklāstīto tehnisko specifikāciju pamatā ir darbs, kas veikts, pamatojoties uz Komisijas 2021. gada 3. jūnija Ieteikumu (ES) 2021/946 par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālās identitātes satvaram ([8]) un jo īpaši arhitektūru un atsauces sistēmu. Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2024/1183 ([9]) 75. apsvērumu Komisijai šī īstenošanas regula vajadzības gadījumā būtu jāpārskata un jāatjaunina, lai tā atbilstu globālajām norisēm, arhitektūrai un atsauces sistēmai un tajā būtu ņemta vērā paraugprakse iekšējā tirgū.

(5) Lai nodrošinātu maka atkarīgo pušu pārredzamību un uzticamību attiecībā pret maka lietotājiem, maka risinājumu izmantotajiem protokoliem un saskarnēm būtu jānodrošina maka lietotājiem uzticams mehānisms, lai autentificētu maka atkarīgās puses un citas maka vienības. Savukārt maka nodrošinātājiem būtu jānodrošina mehānisms maka vienību autentificēšanai un validēšanai, lai atkarīgās puses varētu saņemt apliecinājumu par maka vienību uzticamību un autentiskumu. Turklāt maku tehniskā infrastruktūra būtu arī jāizstrādā tā, lai nodrošinātu, ka tikai minimāls nepieciešamais datu apjoms tiek pārsūtīts tikai pilnvarotajām atkarīgajām pusēm, vienlaikus saglabājot dažādu darījumu nesasaistāmību. Lai atvieglotu personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanu, visiem maka risinājumiem būtu jāatbalsta vismaz noteikts protokolu un saskarņu minimums.

(6) Lai nodrošinātu maka risinājumu izmantojamību visās dalībvalstīs, visiem maku risinājumiem būtu jāatbalsta vienotas tehniskās specifikācijas, kad, izmantojot makus, atkarīgajām pusēm tiek uzrādīti personas identifikācijas dati un atribūtu elektroniskie apliecinājumi gan attālinātā, gan tuva attāluma scenārijā. Turklāt maka vienības īpašos lietošanas gadījumos var atbalstīt citus protokolus un saskarnes.

(7) Lai panāktu integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, makiem būtu jānodrošina vairāki privātuma uzlabošanas elementi, novēršot to, ka elektroniskās identifikācijas līdzekļu un atribūtu elektroniskā apliecinājuma sniedzēji apvieno personas datus, kas iegūti, sniedzot citus pakalpojumus, ar personas datiem, kas apstrādāti, lai sniegtu Regulas (ES) Nr. 910/2014 darbības jomā esošus pakalpojumus. Kā noteikts Regulā (ES) Nr. 910/2014, atkarīgajām pusēm nav jāpieprasa lietotājiem sniegt nekādus citus datus, izņemot tos, kas norādīti reģistrācijas procesā attiecībā uz maku paredzēto izmantošanu. Maka lietotājiem vajadzētu būt iespējai jebkurā brīdī verificēt atkarīgo pušu reģistrācijas datus. Turklāt maka vienībām vajadzētu iespējot funkciju, ka atribūtu pieprasījuma ietvaros lietotājiem parāda maka atkarīgo pušu reģistrācijas sertifikātus, ja tie ir pieejami. Tam vajadzētu ļaut maka lietotājiem verificēt, ka maka atkarīgās puses pieprasītie atribūti ir viņu reģistrēto atribūtu tvērumā, nodrošinot pārliecību, ka pieprasījums ir likumīgs un uzticams.

(8) Lai aizsargātu maka lietotāju datus, maka nodrošinātājiem būtu jānodrošina, ka maka vienības pirms jebkādu datu sniegšanas validē maka atkarīgo pušu vai citu maka vienību pieprasījumus. Tā paša iemesla dēļ un saskaņā ar Regulas (ES) Nr. 910/2014 5.a panta 4. punkta d) apakšpunkta ii) punktu maka nodrošinātājiem būtu jānodrošina, ka maka vienības ļauj maka lietotājiem iesniegt datu dzēšanas pieprasījumus maka atkarīgajām pusēm.

(9) Lai būtu iespējams ātri reaģēt, rodoties jebkādām bažām par datu aizsardzību, kas saistītas ar Regulas (ES) Nr. 910/2014 5.a panta 4. punkta d) apakšpunkta iii) punktu, maka nodrošinātājiem būtu jānodrošina, ka maka risinājumi nodrošina mehānismus, ar kuriem par atkarīgo pusi ziņo kompetentajai valsts datu aizsardzības iestādei. Maka nodrošinātājiem un datu aizsardzības iestādēm būtu jādod pienācīga elastība izveidot piemērotus mehānismus mijiedarbībai ar dalībvalstu datu aizsardzības iestādēm.

(10) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([10]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2024. gada 30. septembrī sniedza savu atzinumu.

([8]) OV L 210, 14.6.2021., 51. lpp., ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2024/1183 (2024. gada 11. aprīlis), ar ko groza Regulu (ES) Nr. 910/2014 attiecībā uz Eiropas digitālās identitātes satvara izveidi (OV L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([10]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(11) Šajā regulā paredzētie pasākumi ir saskaņā ar Regulas (ES) Nr. 910/2014 48. pantā minētās komitejas atzinumu,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Priekšmets un darbības joma

Šajā regulā ir paredzēti noteikumi par maka risinājumu protokoliem un saskarnēm, kuri paredzēti:

1) personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanai maka vienībām;

2) personas identifikācijas datu un atribūtu elektronisko apliecinājumu uzrādīšanai maka atkarīgajām pusēm un citām maka vienībām;

3) paziņošanai par datu dzēšanas pieprasījumiem maka atkarīgajām pusēm;

4) ziņošanai par maka atkarīgajām pusēm uzraudzības iestādēm, kas izveidotas saskaņā ar Regulas (ES) 2016/679 51. pantu;

tie ir regulāri jāatjaunina, lai nodrošinātu atbilstību tehnoloģiju un standartu attīstībai un darbam, kas veikts, pamatojoties uz Komisijas Ieteikumu (ES) 2021/946 un jo īpaši arhitektūru un atsauces sistēmu.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "maka atkarīgā puse" ir atkarīgā puse, kas, izmantojot digitālu mijiedarbību, plāno paļauties uz maka vienībām, lai sniegtu publiskus vai privātus pakalpojumus;

2) "maka lietotājs" ir lietotājs, kas kontrolē maka vienību;

3) "maka risinājums" ir programmatūras, aparatūras, pakalpojumu, iestatījumu un konfigurāciju kombinācija, kas ietver maka instances, vienu vai vairākas maka drošas kriptogrāfijas lietojumprogrammas un vienu vai vairākas maka drošas kriptogrāfijas ierīces;

4) "maka vienība" ir maka risinājuma unikāla konfigurācija, kas ietver maka instances, maka drošas kriptogrāfijas lietojumprogrammas un maka drošas kriptogrāfijas ierīces, ko maka nodrošinātājs nodrošina individuālam maka lietotājam;

5) "maka nodrošinātājs" ir fiziska vai juridiska persona, kas nodrošina maka risinājumus;

6) "maka instance" ir lietojumprogramma, kas uzstādīta un konfigurēta maka lietotāja ierīcē vai vidē, tā ir daļa no maka vienības un maka lietotājs to izmanto, lai mijiedarbotos ar maka vienību;

7) "maka drošas kriptogrāfijas lietojumprogramma" ir lietojumprogramma, kura sasaistē ar kriptogrāfiskām un nekriptogrāfiskām funkcijām, ko nodrošina maka drošas kriptogrāfijas ierīce, un, izmantojot šīs funkcijas, pārvalda kritiski svarīgus aktīvus;

8) "maka drošas kriptogrāfijas ierīce" ir pret nesankcionētām manipulācijām noturīga ierīce, kas nodrošina vidi, kura ir sasaistīta ar maka drošas kriptogrāfijas lietojumprogrammu, kas šo vidi izmanto, lai aizsargātu kritiski svarīgus aktīvus un nodrošinātu kriptogrāfijas funkcijas kritiski svarīgu operāciju drošai izpildei;

9) "kritiski svarīgi aktīvi" ir aktīvi maka vienībā vai saistībā ar to, kas ir tik ārkārtīgi svarīgi, ka, ja to pieejamība, konfidencialitāte vai integritāte tiktu kompromitēta, tas ļoti nopietni un negatīvi ietekmētu spēju paļauties uz maka vienību;

10) “maka atkarīgās puses piekļuves sertifikāts” ir elektronisko zīmogu vai parakstu sertifikāts, ar ko autentificē un validē maka atkarīgo pusi un ko izdevis maka atkarīgās puses piekļuves sertifikātu nodrošinātājs;

11) “maka atkarīgās puses piekļuves sertifikātu nodrošinātājs” ir fiziska vai juridiska persona, ko dalībvalsts pilnvarojusi izdot atkarīgās puses piekļuves sertifikātus minētajā dalībvalstī reģistrētām maka atkarīgajām pusēm;

12) “maka vienības apliecinājums” ir datu objekts, kas apraksta maka vienības komponentus vai ļauj šos komponentus autentificēt un validēt;

13) “iegultā informācijas izpaušanas procedūra” ir noteikumu kopums, kuru atribūtu elektroniskajā apliecinājumā iegūlis tā izsniedzējs un kurā norādīti nosacījumi, kas maka atkarīgajai pusei ir jāizpilda, lai piekļūtu atribūtu elektroniskajam apliecinājumam;

14) “maka atkarīgās puses reģistrācijas sertifikāts” ir datu objekts, kas norāda, kurus atribūtus atkarīgā puse ir reģistrējusi kā tādus, kurus tā grasās pieprasīt no lietotājiem;

15) “personas identifikācijas datu sniedzējs” ir fiziska vai juridiska persona, kas atbild par personas identifikācijas datu izdošanu un atsaukšanu un nodrošina, ka lietotāja personas identifikācijas dati ir kriptogrāfiski saistīti ar maka vienību;

16) “kriptogrāfiska saistīšana” ir metode, ar ko personas identifikācijas datus vai atribūtu elektroniskos apliecinājumus sasaista ar maka vienībām, izmantojot kriptogrāfiskus līdzekļus.

3. pants

Vispārīgie noteikumi

Attiecībā uz 4. un 5. pantā minētajiem protokoliem un saskarnēm maka nodrošinātāji nodrošina, ka maka vienības:

1) autentificē un validē maka atkarīgās puses piekļuves sertifikātus, ja tie mijiedarbojas ar maka atkarīgajām pusēm;

2) autentificē un validē maka vienības apliecinājumus par citām maka vienībām, ja tie mijiedarbojas ar citām maka vienībām;

3) attiecīgā gadījumā autentificē un validē pieprasījumus, kas iesniegti, izmantojot maka atkarīgās puses piekļuves sertifikātus vai maka vienības apliecinājumus no citām maka vienībām;

4) attiecīgā gadījumā autentificē un validē maka atkarīgās puses reģistrācijas sertifikātu;

5) parāda maka lietotājiem informāciju, kas iekļauta maka atkarīgās puses piekļuves sertifikātos vai maka vienības apliecinājumos;

6) attiecīgā gadījumā parāda maka lietotājiem atribūtus, kas maka lietotājiem jāuzrāda;

7) attiecīgā gadījumā parāda maka lietotājiem informāciju, kas ietverta maka atkarīgās puses reģistrācijas sertifikātā;

8) sniedz maka vienības apliecinājumus maka atkarīgajām pusēm vai maka vienībām, kas to pieprasa;

9) nesniedz nekādus pieprasītos atribūtus maka atkarīgajām pusēm vai maka vienībām, kamēr nav izpildītas šādas prasības:

   a) ir verificēts, ka maka drošas kriptogrāfijas lietojumprogramma ir autentificējusi maka lietotāja identitāti,

   b) attiecīgā gadījumā – ir verificēts, ka maka vienībās ir apstrādātas iegultās informācijas izpaušanas procedūras saskaņā ar Īstenošanas regulas (ES) 2024/2979 11. pantu;

   c) ir verificēts, ka maka lietotāji ir daļēji vai pilnībā apstiprinājuši uzrādīšanu;

(10) iespējo privātuma saglabāšanas paņēmienus, kas nodrošina nesasaistāmību, ja atribūtu elektroniskajiem apliecinājumiem nav nepieciešama maka lietotāja identifikācija, uzrādot apliecinājumus vai personas identifikācijas datus dažādām maka atkarīgajām pusēm.

4. pants

Personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošana maka vienībām

1. Maka nodrošinātāji nodrošina, ka maka risinājumi atbalsta protokolus un saskarnes personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanai maka vienībām.

2. Maka nodrošinātāji nodrošina, ka maka vienības pieprasa personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanu tikai no pusēm, kurām ir autentisks un derīgs maka atkarīgās puses piekļuves sertifikāts, kas apliecina, ka šīs puses ir:

a) personas identifikācijas datu sniedzējs;

b) atribūtu kvalificēta elektroniskā apliecinājuma sniedzējs;

c) tāda atribūtu elektroniskā apliecinājuma sniedzējs, ko izdevusi par autentisku avotu atbildīga publiska iestāde vai kas izdots tās vārdā; vai

d) atribūtu nekvalificētu elektronisko apliecinājumu sniedzējs.

3. Attiecībā uz personas identifikācijas datu un atribūtu elektronisko apliecinājumu izdošanu maka vienībai maka nodrošinātāji nodrošina, ka tiek ievērotas šādas prasības:

a) ja maka lietotāji savu maka vienību izmanto, lai pieprasītu personas identifikācijas datu vai atribūtu elektronisko apliecinājumu izdošanu no personas identifikācijas datu vai atribūtu elektronisko apliecinājumu sniedzējiem, kas ļauj izdot personas identifikācijas datus vai elektroniskos apliecinājumus vairāk nekā vienā formātā, maka vienība to pieprasa visos formātos, kas minēti Īstenošanas regulas (ES) 2024/2979, ar ko paredz noteikumus par to, kā Regula (ES) Nr. 910/2014 piemērojama attiecībā uz Eiropas digitālās identitātes maku integritāti un pamatfunkcijām, 8. pantā;

b) ja maka lietotāji izmanto savu maka vienību, lai mijiedarbotos ar personas identifikācijas datu vai atribūtu elektronisko apliecinājumu sniedzējiem, maka vienības ļauj autentificēt un validēt maka vienības komponentus, pēc pieprasījuma uzrādot šiem sniedzējiem maka vienības apliecinājumus;

c) maka risinājumi atbalsta mehānismus, kas ļauj personas identifikācijas datu sniedzējiem verificēt izdošanu, piegādi un aktivizēšanu saskaņā ar augsta uzticamības līmeņa prasībām, kas noteiktas Komisijas Īstenošanas regulā (ES) 2015/1502 ([11]);

d) maka vienības pārbauda personas identifikācijas datu un atribūtu elektronisko apliecinājumu autentiskumu un spēkā esību.

5. pants

Atribūtu uzrādīšana maka atkarīgajām pusēm

1. Maka nodrošinātāji nodrošina, ka maka risinājumi atbalsta protokolus un saskarnes atribūtu uzrādīšanai maka atkarīgajām pusēm attālināti un attiecīgā gadījumā tuvā attālumā saskaņā ar pielikumā noteikto standartu.

2. Maka nodrošinātāji nodrošina, ka pēc lietotāju pieprasījuma maka vienības atbild uz sekmīgi autentificētiem un validētiem 3. pantā minēto maka atkarīgo pušu pieprasījumiem saskaņā ar pielikumā noteikto standartu.

3. Maka nodrošinātāji nodrošina, ka maka vienības atbalsta tādu privātu atslēgu esības pierādīšanu, kas atbilst publiskām atslēgām, kuras izmanto kriptogrāfiskajā sasaistīšanā.

([11]) 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 (OV L 235, 9.9.2015., 7. lpp., ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

4. Maka nodrošinātāji nodrošina, ka maka risinājumi atbalsta personas identifikācijas datu atribūtu un atribūtu elektronisko apliecinājumu selektīvu izpaušanu.

5. Šā panta 1.–4. punktu *mutatis mutandis* piemēro mijiedarbībai starp divām tuvā attālumā esošām maka vienībām.

6. pants

Datu dzēšanas pieprasījumu paziņošana

1. Maka nodrošinātāji nodrošina, ka maka vienības atbalsta protokolus un saskarnes, kas ļauj maka lietotājiem pieprasīt no maka atkarīgajām pusēm, ar kurām tie mijiedarbojušies, izmantojot minētās maka vienības, dzēst viņu personas datus, kas sniegti, izmantojot minētās maka vienības, saskaņā ar Regulas (ES) 2016/679 17. pantu.

2. Protokoli un saskarnes, kas minētas 1. punktā, ļauj maka lietotājiem atlasīt maka atkarīgās puses, kurām ir jāiesniedz datu dzēšanas pieprasījumi.

3. Maka vienības parāda maka lietotājam iepriekš iesniegtus datu dzēšanas pieprasījumus, kas iesniegti, izmantojot minētās maka vienības.

7. pants

Ziņošana par maka atkarīgajām pusēm uzraudzības iestādēm, kas izveidotas saskaņā ar Regulas (ES) 2016/679 51. pantu

1. Maka nodrošinātāji nodrošina, ka maka vienības dod maka lietotājiem iespēju viegli ziņot par maka atkarīgajām pusēm uzraudzības iestādēm, kas izveidotas saskaņā ar Regulas (ES) 2016/679 51. pantu.

2. Maka nodrošinātāji īsteno protokolus un saskarnes, lai ziņotu par maka atkarīgajām pusēm saskaņā ar dalībvalstu procesuālajiem tiesību aktiem.

3. Maka nodrošinātāji nodrošina, ka maka vienības dod maka lietotājiem iespēju pamatot ziņojumus, tajā skaitā pievienojot attiecīgu informāciju, lai identificētu maka atkarīgās puses, un maka lietotāju prasības mašīnlasāmā formātā.

8. pants

Stāšanās spēkā

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

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

Briselē, 2024. gada 28. novembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

PIELIKUMS

5. PANTA 1. UN 2. PUNKTĀ MINĒTAIS STANDARTS

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024