Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2025/847

7.5.2025.

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2025/847

(2025. gada 6. maijs),

kas nosaka noteikumus par Eiropas Parlamenta un Padomes Regulas (ES) Nr. 910/2014 piemērošanu reaģēšanā uz Eiropas digitālās identitātes maku drošības pārkāpumiem

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) 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.e panta 5. punktu,

tā kā:

(1) Eiropas digitālās identitātes satvars ("satvars"), kas noteikts Regulā (ES) Nr. 910/2014, ir būtisks drošas un sadarbspējīgas visas Savienības digitālās identitātes ekosistēmas izveides elements. Eiropas digitālās identitātes maki ("maki") ir satvara stūrakmens, kura mērķis ir atvieglot 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 Regulas (ES) 2016/679 ([2]), (ES) 2018/1725 ([3]) un – attiecīgā gadījumā – Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([4]). Šīs regulas noteikumi par informācijas novērtēšanu un sniegšanu neskar pienākumu attiecīgā gadījumā saskaņā ar Regulu (ES) 2016/679 vai Regulu (ES) 2018/1725 paziņot kompetentajai uzraudzības iestādei par personas datu aizsardzības pārkāpumiem un attiecīgā gadījumā pienākumu paziņot datu subjektiem par personas datu aizsardzības pārkāpumiem saskaņā ar šīm regulām.

(3) Komisija regulāri novērtē jaunas tehnoloģijas, praksi, standartus un tehniskas specifikācijas. Lai panāktu pašu augstāko saskaņotību starp dalībvalstīm attiecībā uz maku izstrādi un sertifikāciju, šajā regulā izklāstīto tehnisko specifikāciju pamats ir darbs, kas veikts atbilstoši Komisijas Ieteikumam (ES) 2021/946 ([5]), it īpaši tajā ietilpstošajai arhitektūrai un atsauces sistēmai. Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2024/1183 ([6]) 75. apsvērumu Komisijai šī regula būtu jāpārskata un vajadzības gadījumā jāatjaunina, to pieskaņojot pasaules norisēm un arhitektūrai un atsauces satvaram un sekojot iekšējā tirgus paraugpraksei.

([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 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).
([4]) 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).
([5]) Komisijas Ieteikums (ES) 2021/946 (2021. gada 3. jūnijs) par kopīgu Savienības rīkkopu koordinētai pieejai Eiropas digitālās identitātes satvaram (OV L 210, 14.6.2021., 51. lpp., ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([6]) 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).

(4) Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minēto maka risinājumu vai validācijas mehānismu, vai elektroniskās identifikācijas shēmas, kurās tiek nodrošināti maka risinājumi, drošības pārkāpuma vai aizskāruma gadījumā ir ātri, koordinēti un droši jāreaģē uz šādiem drošības pārkāpumiem un aizskārumiem visās dalībvalstīs, lai aizsargātu lietotājus un saglabātu uzticēšanos digitālās identitātes ekosistēmai. Tas neskar Eiropas Parlamenta un Padomes Direktīvu (ES) 2022/2555 ([7]), Eiropas Parlamenta un Padomes Regulas (ES) 2019/881 ([8]) un (ES) 2024/2847 ([9]), it īpaši attiecībā uz incidentu vai vājo vietu izskatīšanu un pieskaitīšanu pie drošības pārkāpumiem. Tāpēc dalībvalstīm būtu jānodrošina drošības pārkāpuma vai aizskāruma ietekmēta maka nodrošināšanas un lietošanas laicīga apturēšana vai – attiecīgā gadījumā – maka atcelšana.

(5) Lai nodrošinātu pienācīgu reaģēšanu uz drošības pārkāpumu vai aizskārumu, dalībvalstīm būtu jānovērtē, vai maka risinājuma, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minēto validācijas mehānismu vai elektroniskās identifikācijas shēmas, kurās nodrošina maka risinājumu, drošības pārkāpums vai aizskārums ietekmē minētā maka risinājuma vai citu maka risinājumu uzticamību. Novērtējumam būtu jābalstās uz vienotiem kritērijiem, piemēram, ietekmēto maka lietotāju skaitu un kategoriju, fizisku personu un maka atkarīgo pušu skaitu un kategoriju, ietekmēto datu raksturu, drošības aizskāruma vai pārkāpuma ilgumu, ierobežoto pakalpojuma pieejamību un finansiāliem zaudējumiem, kā arī personas datu varbūtēju aizskārumu. Šiem kritērijiem būtu jānodrošina dalībvalstīm samērīga elastība un rīcības brīvība noteikt, vai ir ietekmēta maka risinājuma uzticamība un vai pienākas maka risinājumu apturēt vai, ja pamats ir pārkāpuma vai aizskāruma smagums, atcelt. Šiem kritērijiem nebūtu jāizraisa maka risinājuma atcelšana vai automātiska nodrošināšanas un lietošanas apturēšana, bet dalībvalstīm tie pienācīgi jāņem vērā, lemjot, vai maka risinājumu atcelt vai nodrošināšanu un lietošanu apturēt ir nepieciešams.

(6) Ņemot vērā ietekmi un neērtības, ko rada maka risinājumu izmantošanas apturēšana, dalībvalstīm vajadzēs izvērtēt, vai nepieciešams atsaukt maka vienības apliecinājumus vai veikt citus papildu pasākumus, lai pienācīgi reaģētu uz drošības pārkāpumu vai aizskārumu.

(7) Lai maka lietotājus pastāvīgi informētu par maka statusu, jāsniedz viņiem pienācīga informācija par drošības pārkāpumiem vai aizskārumiem, kas ietekmē viņu makus. Tā kā drošības pārkāpumi un aizskārumi var ietekmēt arī Savienībā reģistrētās maka atkarīgās puses, ar tām ir arī jādalās attiecīgā informācijā par drošības pārkāpumiem un aizskārumiem.

(8) Lai uzlabotu pārredzamību un vairotu uzticēšanos digitālās identitātes ekosistēmai, informācijā par drošības pārkāpumiem vai aizskārumiem un to sekām būtu iekļaujama vismaz šajā regulā prasītā informācija. Tomēr informācija par drošības pārkāpumiem vai aizskārumiem, kurā dalās ar maka lietotājiem un maka atkarīgajām pusēm, būtu rūpīgi jāvērtē, lai neļautu to ļaunprātīgi izmantot uzbrucējiem un tādas briesmas minimalizētu.

([7]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) (OV L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Lai lietotāji varētu atkal piekļūt savām maka vienībām, kad drošības pārkāpums vai aizskārums izlabots, dalībvalstij, kura nodrošinājusi maka risinājumus, vajadzēs bez liekas kavēšanās atjaunot minēto maka risinājumu nodrošināšanu un lietošanu. To var izdarīt, atjaunojot maka vienības, izdodot maka vienības, ko nodrošina ar jaunu maka risinājumu versiju, vai atkalizdodot derīgus maka vienības apliecinājumus. Attiecīgi jāinformē ietekmētie maka lietotāji, maka atkarīgās puses, vienotie kontaktpunkti, kas izraudzīti atbilstoši Regulas (ES) Nr. 910/2014 46.c panta 1. punktam, un Komisija.

(10) Lai nodrošinātu maku atcelšanu, kad drošības pārkāpums vai aizskārums nav novērsts trīs mēnešu laikā pēc apturēšanas vai ja par attaisnojumu ir drošības pārkāpuma vai aizskāruma smagums, dalībvalstij būtu jānodrošina, ka attiecīgie maka vienības apliecinājumi tiek atsaukti un ka nevar ne atjaunot to derīgumu, ne tos izdot vai nodrošināt pastāvošām maka vienībām. Vēl vairāk, nedrīkstētu nodrošināt jaunas maka vienības ar ietekmētā maka risinājumu. Pārredzamības labad par atcelšanu būtu informējami lietotāji, atkarīgās puses, vienotie kontaktpunkti, kas izraudzīti atbilstoši Regulas (ES) Nr. 910/2014 46.c panta 1. punktam, un Komisija. Tas nozīmē arī aprakstīt iespējamo ietekmi uz maku lietotājiem, īpaši uz izdoto apliecinājumu pārvaldību vai maka atkarīgajām pusēm.

(11) Trīs mēnešu laikā pēc maka risinājuma nodrošināšanas un izmantošanas apturēšanas, kuros jāizlabo drošības pārkāpums vai aizskārums, kas novedis pie apturēšanas, būtu jānoliek termiņš, pēc kura maka risinājums ir jāatceļ, ja nav īstenots pienācīgs tiesiskas aizsardzības līdzeklis. Tomēr dalībvalstīm ir ļauts pieprasīt, lai drošības pārkāpums vai aizskārums tiek izlabots termiņā, kas ir īsāks par trim mēnešiem, sevišķi un attiecīgi ņemot vērā minētā drošības pārkāpuma vai aizskāruma apmēru, ilgumu un sekas. Ja drošības pārkāpums vai aizskārums netiek izlabots vai nav izlabojams dalībvalsts noteiktajā termiņā, dalībvalsts var pieprasīt atcelt maka risinājumu pirms trīs mēnešu termiņa notecējuma. Šis laiks, kurā ir jāizlabo drošības pārkāpums vai aizskārums, kas novedis pie maka risinājuma nodrošināšanas un lietošanas apturēšanas, dalībvalstīm būtu jāizmanto, sagatavojot minētā maka risinājuma un no tā izrietošo paziņojumu varbūtējo atcelšanu.

(12) Lai mazinātu dalībvalstu administratīvo nastu sakarā ar informāciju, ko saskaņā ar šo regulu sniedz Komisijai un citām dalībvalstīm, dalībvalstīm būtu jāizmanto tādi pastāvoši paziņošanas rīki kā kiberincidentu ziņošanas un analīzes sistēma (*CIRAS*), ko pārvalda Eiropas Savienības Kiberdrošības aģentūra (*ENISA*). Attiecībā uz alternatīviem kanāliem vai līdzekļiem, kas izmantojami drošības pārkāpuma vai aizskāruma ietekmēto lietotāju un maka atkarīgo pušu informēšanai, dalībvalstīm būtu jāgādā, lai attiecīgā informācija tiek sniegta skaidri, vispusīgi un viegli piekļūstami. Kanāliem tādas informācijas sniegšanai ietekmētajiem maka lietotājiem un maka atkarīgajām personām būtu jāietver piemēroti risinājumi vietnēs balstītai apraidei, vietņu atjauninājumu izsekošanai reāllaikā un ziņu apkopošanai.

(13) Saskaņā ar Regulas (ES) 2018/1725 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2025. gada 31. janvārī sniedza atzinumu.

(14) Šajā regulā noteiktie pasākumi saskan ar atzinumu, ko sniegusi ar Regulas (ES) Nr. 910/2014 48. pantu izveidotā komiteja,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Priekšmets

Šī regula nosaka noteikumus par reaģēšanu uz drošības pārkāpumiem makos, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minētajos validācijas mehānismos un elektroniskās identifikācijas shēmā, kurā maki tiek nodrošināti.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "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;

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

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

4) "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;

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

6) "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 kritiskus aktīvus un nodrošinātu kriptogrāfijas funkcijas kritisku operāciju drošai izpildei;

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

8) "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;

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

10) "maka vienības apliecinājums" ir datu objekts, kas apraksta maka vienības komponentus vai ļauj šos komponentus autentificēt un validēt.

3. pants

Drošības pārkāpuma vai aizskāruma konstatēšana

1. Neskarot Direktīvu (ES) 2022/2555 un Regulas (ES) 2019/881 un (ES) 2024/2847, dalībvalstis pienācīgi ievēro šīs regulas I pielikumā izklāstītos kritērijus, novērtējot, vai maka risinājuma, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minēto validācijas mehānismu vai elektroniskās identifikācijas shēmas, kurā tiek nodrošināts maka risinājums, drošības pārkāpums vai aizskārums ietekmē to uzticamību vai citu maka risinājumu uzticamību.

2. Ja uz 1. punktā noteikto novērtējuma pamata dalībvalsts konstatē, ka drošības pārkāpums vai aizskārums ietekmē maka risinājuma uzticamību, un aptur minētā maka risinājuma nodrošināšanu un lietošanu, minētā dalībvalsts veic 4. un 5. pantā izklāstītos pasākumus. Ja dalībvalsts atceļ maka risinājumu, minētā dalībvalsts veic 8. un 9. pantā izklāstītos pasākumus.

3. Ja dalībvalstij kļūst zināma informācija par iespējamu drošības pārkāpumu vai aizskārumu, kas spēj ietekmēt viena vai vairāku citas dalībvalsts nodrošināto maka risinājumu uzticamību, dalībvalsts to bez liekas kavēšanās dara zināmu Komisijai un skarto dalībvalstu vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar Regulas (ES) Nr. 910/2014 46.c panta 1. punktu. Paziņojumā ietilpst 5. panta 2. punktā noteiktā informācija.

4. Dalībvalsts, kas saņem saskaņā ar 3. punktu sniegtu informāciju, bez liekas kavēšanās veic 1. un 2. punktā noteiktos pasākumus.

4. pants

Maku un citu tiesiskas aizsardzības līdzekļu nodrošināšanas un lietošanas apturēšana

1. Dalībvalstis gādā, lai netiek nodrošinātas, lietotas un aktivizētas maka vienības ar apturētā maka risinājumu.

2. Dalībvalstis izvērtē, vai pienācīgai reaģēšanai uz drošības pārkāpumu vai aizskārumu ir nepieciešams atsaukt maka vienības apliecinājumus, ko ietekmē maka risinājuma apturēšana, vai noteikt citus papildinošus tiesiskās aizsardzības līdzekļus.

3. 1. un 2. punktā noteiktos pasākumus veic bez liekas kavēšanās un nekādā gadījumā vēlāk kā 24 stundas pēc drošības pārkāpuma vai aizskāruma ietekmētā maka risinājuma nodrošināšanas un lietošanas apturējuma.

4. Šā panta 1. un 2. punktā izklāstītie pasākumi neliedz ietekmētajiem maka lietotājiem īstenot tiesību uz datu pārnešanu, kas noteikta Regulas (ES) Nr. 910/2014 5.a panta 4. punkta g) apakšpunktā. Tam ir nosacījums, ka maka lietotāji šo tiesību var izmantot, nemazinot ietekmēto maka vienību kritisko aktīvu drošību, īpaši ņemot vērā apturēšanas iemeslus un vajadzību gādāt par minēto aktīvu efektīvu aizsardzību pret ļaunprātīgu izmantošanu.

5. pants

Informācija par apturēšanu un tiesiskās aizsardzības līdzekļiem

1. Informāciju par maka risinājuma nodrošināšanas un lietošanas apturēšanu skaidrā, izsmeļošā un viegli pieejamā veidā bez liekas kavēšanās un ne vēlāk kā 24 stundas pēc maka risinājuma apturēšanas sniedz:

a) vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar Regulas (ES) Nr. 910/2014 46.c panta 1. punktu;

b) Komisijai;

c) ietekmētajiem maka lietotājiem;

d) maka atkarīgajām pusēm, kas reģistrētas saskaņā ar Regulas (ES) Nr. 910/2014 5.b pantu.

2. Saskaņā ar 1. punktu sniegtajā informācijā iekļaujamas vismaz šādas ziņas:

a) maka risinājuma, kura nodrošināšana un izmantošana ir apturēta, nodrošinātāja nosaukums;

b) minētā maka risinājuma nosaukums un atsauces identifikators, kas norādīts sertificēto maku sarakstā, kurš izveidots saskaņā ar Regulas (ES) Nr. 910/2014 5.d pantu, un – attiecīgā gadījumā – relevantās versijas;

c) drošības pārkāpuma vai aizskāruma konstatēšanas datums un laiks;

d) ja zināms, datums un laiks, kad drošības pārkāpums vai aizskārums īstenojies, pēc tīkla vai sistēmas žurnāliem vai citiem datu avotiem;

e) maka risinājuma apturēšanas datums un laiks;

f) paziņotājas dalībvalsts un (ja atšķiras) (a) punktā norādītā maka nodrošinātāja kontaktinformācija, ieskaitot vismaz e-pasta adresi un tālruņa numuru;

g) drošības pārkāpuma vai aizskāruma apraksts;

h) aizskarto datu apraksts, attiecīgā gadījumā iekļaujot personas datu kategorijas, kas noteiktas Regulas (ES) 2016/679 9. panta 1. punktā un 10. pantā;

i) ja iespējams – ietekmēto maka lietotāju un citu ietekmēto fizisko personu aptuvenā skaita aplēse;

j) apraksts par potenciālo ietekmi uz maka lietotājiem vai maka atkarīgajām pusēm, otrajā gadījumā – norādes uz pasākumiem, ko maka lietotāji var veikt, lai mazinātu potenciālo ietekmi;

k) veikto vai plānoto drošības pārkāpuma vai aizskāruma izlabošanas pasākumu apraksts, kā arī izlabošanas plāns un termiņš;

l) ja ir piemērojams un pienākas – apraksts par pasākumiem, kas veikti vai plānoti, lai ietekmētie maka lietotāji pārietu uz alternatīviem maka risinājumiem vai pakalpojumiem.

6. pants

Maku nodrošināšanas un lietošanas atjaunošana

Ja maka risinājuma nodrošināšanas, aktivizēšanas un lietošanas atjaunošanai nepieciešams, dalībvalstis bez liekas kavēšanās:

1) atjauno maka vienību nodrošināšanu un lietošanu saskaņā ar minēto maka risinājumu, visiem ietekmētajiem lietotājiem izdodot maka vienību, ko nodrošina saskaņā ar jaunu maka risinājuma versiju;

2) izdod jaunus maka vienības apliecinājumus jaunām maka vienībām vai – attiecīgā gadījumā – agrāk izdotām maka vienībām, ar noteikumu, ka maka vienības atbilst pēc drošības pārkāpuma vai aizskāruma izbeigšanas spēkā esošajām drošības prasībām;

3) atceļ pasākumus, kas īstenoti atbilstīgi 4. pantam un traucē jaunu maka vienību nodrošināšanai saskaņā ar ietekmēto maka risinājumu, ja minētais pasākums bijis saistīts tikai ar nu jau izlaboto drošības pārkāpumu vai aizskārumu.

7. pants

Informācija par atjaunošanu

Ja dalībvalsts atjauno maka risinājumu, tā gādā, lai:

1) informācija par minēto faktu bez liekas kavēšanās tiek sniegta visām pusēm, kas saņēmušas informāciju par minētā maka risinājuma nodrošināšanas un lietošanas apturēšanu saskaņā ar 5. panta 1. punktu;

2) saskaņā ar 1) punktu sniegtā informācijā ietilpst vismaz 5. panta 2. punkta a), b) un f)–h) apakšpunktā norādītie un šie elementi:

   a) drošības pārkāpuma vai aizskāruma izlabošanas datums un laiks;

   b) ietekmētā maka risinājuma un – attiecīgā gadījumā – ietekmēto maka vienību, kas tiek nodrošinātas ar minēto maka risinājumu, atjaunošanas datums un laiks;

   c) drošības pārkāpuma vai aizskāruma labošanai veikto pasākumu apraksts;

   d) apraksts par palikušo potenciālo ietekmi uz maka lietotājiem vai maka atkarīgajām pusēm, otrajā gadījumā – norādes uz pasākumiem, ko maka lietotāji var veikt, lai mazinātu palikušo potenciālo ietekmi.

8. pants

Maku atcelšana

1. Ja drošības pārkāpums vai aizskārums, kas novedis pie maka risinājuma nodrošināšanas un lietošanas apturēšanas, nav izlabots trīs mēnešus pēc dienas, kad apturēta minētā maka risinājuma nodrošināšana un lietošana, dalībvalsts, kas nodrošina minēto maka risinājumu, bez liekas kavēšanās un katrā gadījumā 72 stundu laikā pēc minētā trīs mēnešu termiņa gādā, lai ietekmētais maka risinājums tiek atcelts un tā derīgums atsaukts.

2. Ja dalībvalsts atceļ maka risinājumu, tā gādā, lai:

a) tiek atsaukti attiecīgā maka risinājuma maka vienības apliecinājumi;

b) maka vienības apliecinājumi nevar atgūt derīgumu;

c) pastāvošām maka vienībām, ko nodrošina ar ietekmētā maka risinājumu, nevar izdot jaunu maka vienības apliecinājumu;

d) ar ietekmēto maka risinājumu netiek nodrošinātas jaunas maka vienības.

3. Šā panta 1. un 2. punktā izklāstītie pasākumi neliedz ietekmētajiem maka lietotājiem īstenot tiesību uz datu pārnešanu, kas noteikta Regulas (ES) Nr. 910/2014 5.a panta 4. punkta g) apakšpunktā. Tam ir nosacījums, ka maka lietotāji šo tiesību var izmantot, nemazinot ietekmēto maka vienību kritisko aktīvu drošību, īpaši ņemot vērā atcelšanas iemeslus un vajadzību nodrošināt minēto aktīvu efektīvu aizsardzību pret ļaunprātīgu izmantošanu.

9. pants

Informācija par atcelšanu

1. Informāciju par maka risinājuma atcelšanu skaidrā, vispusīgā un viegli pieejamā veidā bez liekas kavēšanās un ne vēlāk kā 24 stundas pēc maka risinājuma atcelšanas sniedz:

a) vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar Regulas (ES) Nr. 910/2014 46.c panta 1. punktu;

b) Komisijai;

c) ietekmētajiem maka lietotājiem;

d) maka atkarīgajām pusēm, kas reģistrētas saskaņā ar Regulas (ES) Nr. 910/2014 5.b pantu.

2. Saskaņā ar 1. punktu sniegtajā informācijā iekļaujamas vismaz šādas ziņas:

a) atceltā maka risinājuma nodrošinātāja nosaukums;

b) minētā maka risinājuma nosaukums un atsauces identifikators, kas norādīts sertificēto maku sarakstā, kurš izveidots saskaņā ar Regulas (ES) Nr. 910/2014 5.d pantu, un – attiecīgā gadījumā – relevantās versijas;

c) datums un laiks, kad atklāts drošības pārkāpums vai aizskārums, kura dēļ ietekmētais maka risinājums atcelts tā smaguma dēļ vai tāpēc, ka trīs mēnešos nav izlabots;

d) ja zināms, datums un laiks, kad drošības pārkāpums vai aizskārums sācis darboties, pēc tīkla vai sistēmas žurnāliem vai citiem datu avotiem;

e) maka risinājuma un ar maka risinājumu sniegto maka vienību apliecinājumu atcelšanas un faktiskās atsaukšanas datums un laiks;

f) vai atcelšana ir drošības pārkāpuma vai aizskāruma smaguma rezultāts vai drošības pārkāpuma vai aizskāruma nenovēršanas sekas;

g) paziņotājas dalībvalsts un (ja atšķiras) a) punktā norādītā maka nodrošinātāja kontaktinformācija, ieskaitot vismaz e-pasta adresi un tālruņa numuru;

h) drošības pārkāpuma vai aizskāruma apraksts;

i) aizskarto datu apraksts, attiecīgā gadījumā iekļaujot personas datu kategorijas, kas noteiktas Regulas (ES) 2016/679 9. panta 1. punktā un 10. pantā;

j) ja iespējams – ietekmēto maka lietotāju un citu ietekmēto fizisko personu aptuvenā skaita aplēse;

k) apraksts par potenciālo ietekmi uz maka lietotājiem vai maka atkarīgajām pusēm, otrajā gadījumā – norādes uz pasākumiem, ko maka lietotāji var veikt, lai mazinātu potenciālo ietekmi;

l) apraksts par pasākumiem, kas veikti vai plānoti, lai ietekmētos maka lietotājus pārvestu uz alternatīviem maka risinājumiem, vai, kad attiecīgā gadījumā pienākas, uz alternatīviem pakalpojumiem.

10. pants

Informācijas sistēma

3., 5., 7. un 9. pantā noteikto informāciju dalībvalstis Komisijai un saskaņā ar Regulas (ES) Nr. 910/2014 46.c panta 1. punktu izraudzītajiem dalībvalstu vienotajiem kontaktpunktiem nosūta sistēmā *CIRAS*, ko apkalpo *ENISA*, vai līdzvērtīgā sistēmā, par ko vienojušās dalībvalstis un Komisija.

11. 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, izņemot 10. pantu, ko piemēro no 2026. gada 7. maija.

Briselē, 2025. gada 6. maijā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

PIELIKUMS

Drošības pārkāpuma vai aizskāruma novērtēšanas kritēriji

1. Drošības pārkāpumu vai aizskārumu dalībvalstis novērtē pēc šādiem kritērijiem:

a) pārkāpums vai aizskārums ir izraisījis vai spēj izraisīt fiziskas personas nāvi vai būtisku kaitējumu fiziskas personas veselībai;

b) ir notikusi vai var notikt sekmīga varbūtēji ļaunprātīga vai neatļauta piekļuve maka nodrošinātāja, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā norādīta validācijas mehānismu nodrošinātāja vai elektroniskās identifikācijas shēmas, kurā tiek nodrošināts maka risinājums, nodrošinātāja ("attiecīgās vienības") tīkliem un informācijas sistēmām tādā veidā, kas var izraisīt nopietnus darbības traucējumus, un minētās sistēmas ir ietekmētā maka risinājuma, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minēto ietekmēto validācijas mehānismu vai ietekmētās elektroniskās identifikācijas shēmas, kurā tiek nodrošināts maka risinājums, kritiskie komponenti;

c) kāds maka risinājums, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minēts validācijas mehānisms vai elektroniskās identifikācijas shēma, kurā tiek nodrošināts maka risinājums, vai to daļa:

— ir pilnīgi nepieejami vai tiek prognozēts, ka būs pilnīgi nepieejami, maka lietotājiem vai maka atkarīgajām pusēm ilgāk ar 12 stundām no vietas,

— maka lietotājiem vai maka atkarīgajām pusēm nav pieejami vai tiek prognozēts, ka nebūs pieejami, vairāk nekā 16 stundas kalendāra nedēļu ilgā posmā;

d) ir aizdomas, ka vairāk nekā 1 % maka lietotāju vai maka atkarīgo pušu ietekmē vai tiek prognozēts, ka tos ietekmēs maka risinājuma ierobežotā pieejamība vai attiecīgo struktūru sniegtie pakalpojumi maka risinājuma sakarā;

e) pastāv spēja aizskart vai ir aizskarta fiziska piekļuve, kas ir tikai attiecīgo vienību uzticamam personālam, vai tādas fiziskas piekļuves aizsardzība vienai vai vairākām tīklu un informācijas sistēmu, kuras atbalsta maka risinājumu, atrašanās vietām, Regulas (ES) Nr. 910/2014 5.a panta 8. punktā minēto ar maka risinājumu saistīto validācijas mehānismu nodrošināšana vai elektroniskās identifikācijas shēma, kurā tiek nodrošināts maka risinājums;

f) vienā vai vairākos no šiem veidiem ir aizskarti vai var tikt aizskarti maka risinājumā glabāto, pārsūtīto vai apstrādāto datu privātums, veselums, konfidencialitāte vai autentiskums:

— ietekmē vairāk nekā 1 % attiecīgā maka lietotāju vai vairāk nekā 100 000 šo maku lietotāju, atkarā no tā, kurš skaits mazāks,

— ir sekmīgas varbūtēji ļaunprātīgas darbības rezultāts,

— ceļas vai var būt cēlies no vienas vai vairākām zināmām vājajām vietām, ieskaitot tādas, kuras risina saskaņā ar Komisijas Īstenošanas regulu (ES) 2024/2981 ([1]),

— tas var ietekmēt personas datus tādā veidā, kas var radīt briesmas attiecīgu fizisku personu tiesībām un brīvībām, sevišķi, ja pārkāpti personas dati, kā noteikts Regulas (ES) 2016/679 9. panta 1. punktā un 10. pantā,

([1]) Komisijas Īstenošanas regula (ES) 2024/2981 (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 sertifikāciju (OV L, 2024/2981, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— tas var ietekmēt personas elektronisko saziņu,

— tas var radīt augstu risku fizisku personu tiesībām un brīvībām,

— tas var ietekmēt mazaizsargātas fiziskas personas;

g) maka risinājuma sertificējums ir anulēts, vai tiek plānota tā anulēšana;

h) pārkāpums vai aizskārums ir radījis vai var radīt tiešus finansiālus zaudējumus attiecīgajai vienībai un minētie zaudējumi pārsniedz 500 000 EUR vai attiecīgā gadījumā 5 % attiecīgās vienības kopējā gada apgrozījuma iepriekšējā finanšu gadā, atkarā no tā, kura summa ir mazāka.

2. Dalībvalstis neņem vērā tehniskās apkopes darbības, ko veic attiecīgās struktūras vai kas tiek veiktas to vārdā, plānotās sekas, ja tehniskās apkopes darbība:

a) ir iepriekš izziņota potenciāli ietekmētajiem maku lietotājiem, maka atkarīgajām pusēm un attiecīgajām kompetentajām uzraudzības iestādēm;

b) neatbilst nevienam no šā pielikuma 1. punktā izklāstītajiem kritērijiem.

3. 1. punkta c) apakšpunkta sakarā tāda incidenta ilgumu, kas ietekmē pieejamību, mērī no brīža, kad aprauta ietekmētā pakalpojuma pienācīga sniegšana, līdz brīdim, kad pakalpojums atjaunots un atkal darbojas. Ja attiecīga vienība nespēj noteikt pārrāvuma sākuma brīdi, incidenta ilgums jāmērī no incidenta atklāšanas brīža vai no brīža, kad incidents reģistrēts tīkla vai sistēmas žurnālos vai citos datu avotos, atkarā no tā, kas notiek vispirms. Pakalpojuma pilnīga nepieejamība jāmērī no brīža, kad pakalpojums kļūst pilnīgi nepieejams lietotājiem, līdz brīdim, kad regulārā aktivitāte vai darbība ir atjaunota tādā pakalpojumu līmenī, kāds nodrošināts pirms incidenta. Ja attiecīga vienība nespēj noteikt, kad ir sākusies pakalpojuma pilnīga nepieejamība, nepieejamība jāmērī no brīža, kad vienība to konstatējusi.

4. Attiecībā uz 1. punkta d) apakšpunktu uzskata, ka pakalpojuma pieejamība ir ierobežota, īpaši tad, kad pakalpojums ir ievērojami lēnāks nekā vidējais atbildes laiks vai nav pieejamas visas pakalpojuma funkcijas. Kur iespējams, atbildes laika kavējuma noteikšanā jāizmanto objektīvi kritēriji, balstoties uz pakalpojumu vidējo reakcijas laiku.

5. 1. punkta h) apakšpunktā norādīta pārkāpuma vai aizskāruma nodarītu tiešu finansiālu zaudējumu noteikšanā attiecīgajām vienībām jāņem vērā visi finansiālie zaudējumi, kas tām radušies incidenta rezultātā, piemēram, programmatūras, aparatūras vai infrastruktūras nomaiņas vai pārvietošanas izmaksas, personāla izmaksas, to skaitā izmaksas, kas saistītas ar personāla nomaiņu vai pārcelšanu, papildu darbinieku pieņemšanu darbā, samaksu par virsstundu darbu un zaudēto vai vājināto prasmju atgūšanu, maksas par līgumsaistību neievērošanu, klientu zaudējumu atlīdzināšanas un kompensēšanas izmaksas, zaudējumi, kas radušies, negūstot ieņēmumus, izmaksas saistībā ar iekšējo un ārējo komunikāciju, konsultāciju izmaksas, to skaitā izmaksas, kas saistītas ar juridiskām konsultācijām, tiesu ekspertīzes pakalpojumiem un koriģēšanas pakalpojumiem. Izmaksas, kas nepieciešamas uzņēmuma ikdienējai darbībai, piemēram, infrastruktūras, aprīkojuma, aparatūras un programmatūras vispārējai uzturēšanai, uzlabošanai un riska novērtēšanas iniciatīvām un apdrošināšanas iemaksām, neuzskata par incidenta izraisītiem finansiāliem zaudējumiem. Attiecīgās vienības finansiālo zaudējumu summas aprēķina pēc pieejamiem datiem, un, ja finansiālo zaudējumu faktiskās summas nav iespējams noteikt, vienības tādas summas aplēš.