Europos Sąjungos
oficialusis leidinys

LT
L serija

2025/847

2025 5 7

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2025/847

2025 m. gegužės 6 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl reagavimo į europinių skaitmeninės tapatybės dėklių saugumo pažeidimus taikymo taisyklės

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB ([1]), ypač į jo 5e straipsnio 5 dalį,

kadangi:

(1) Reglamentu (ES) Nr. 910/2014 nustatyta Europos skaitmeninės tapatybės sistemai (toliau – sistema) tenka labai svarbus vaidmuo kuriant saugią ir sąveikią skaitmeninės tapatybės ekosistemą visoje Sąjungoje. Sistema, kurios pagrindas – europinės skaitmeninės tapatybės dėklės (toliau – dėklės), siekiama palengvinti prieigą prie paslaugų visose valstybėse narėse, kartu užtikrinant asmens duomenų ir privatumo apsaugą;

(2) asmens duomenų tvarkymo veiklai pagal šį reglamentą taikomi Europos Parlamento ir Tarybos reglamentai (ES) 2016/679 ([2]), (ES) 2018/1725 ([3]) ir, kai aktualu, Europos Parlamento ir Tarybos direktyva 2002/58/EB ([4]). Pagal šį reglamentą nustatytomis informacijos vertinimo ir teikimo taisyklėmis nedaromas poveikis pareigai pranešti apie asmens duomenų saugumo pažeidimus kompetentingai priežiūros institucijai, kai taikytina pagal Reglamentą (ES) 2016/679 arba Reglamentą (ES) 2018/1725, ir pareigai pranešti apie asmens duomenų saugumo pažeidimus duomenų subjektams, kai taikytina pagal šiuos reglamentus;

(3) Komisija reguliariai vertina naujas technologijas, praktiką, standartus ir technines specifikacijas. Siekiant užtikrinti aukščiausią valstybių narių suderinimo lygį kuriant ir sertifikuojant dėkles, šiame reglamente nustatytos techninės specifikacijos grindžiamos darbu, atliktu remiantis Komisijos rekomendacija (ES) 2021/946 ([5]), visų pirma jos architektūra ir pamatine sistema. Pagal Europos Parlamento ir Tarybos reglamento (ES) 2024/1183 ([6]) 75 konstatuojamąją dalį, Komisija turėtų šį reglamentą peržiūrėti ir prireikus atnaujinti, kad jis atitiktų pasaulinius pokyčius, architektūrą ir pamatinę sistemą ir būtų laikomasi geriausios vidaus rinkos praktikos;

([1]) OL L 257, 2014 8 28, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39, ELI: http://data. europa.eu/eli/reg/2018/1725/oj).

([4]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) 2021 m. birželio 3 d. Komisijos rekomendacija (ES) 2021/946 dėl bendro Sąjungos priemonių rinkinio darniam Europos skaitmeninės tapatybės sistemos kūrimui užtikrinti (OL L 210, 2021 6 14, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu, (OL L, 2024/1183, 2024 4 30, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) dėklės sprendinių arba Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų patvirtinimo mechanizmų, arba elektroninės atpažinties schemos, pagal kurią teikiami dėklės sprendiniai, saugumo arba patikimumo pažeidimo atveju reikia greitai, koordinuotai ir užtikrinant saugumą reaguoti į tokius saugumo ir patikimumo pažeidimus visose valstybėse narėse, kad būtų apsaugoti naudotojai ir išlaikytas pasitikėjimas skaitmeninės tapatybės ekosistema. Tai nedaro poveikio Europos Parlamento ir Tarybos direktyvai (ES) 2022/2555 ([7]) ir Europos Parlamento ir Tarybos reglamentams (ES) 2019/881 ([8]) ir (ES) 2024/2847 ([9]), visų pirma tam, kaip valdomi incidentai arba pažeidžiamumo atvejai ir kodėl jie laikomi saugumo pažeidimais. Todėl valstybės narės turėtų užtikrinti, kad būtų laiku sustabdytas dėklių, kurias paveikė saugumo arba patikimumo pažeidimas, teikimas ir naudojimas arba, kai tinkama, jos būtų pašalintos;

(5) kad saugumo arba patikimumo pažeidimai būtų šalinami tinkamai, valstybės narės turėtų įvertinti, ar dėklės sprendinio, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų patvirtinimo mechanizmų arba elektroninės atpažinties schemos, pagal kurią teikiamas dėklės sprendinys, saugumo arba patikimumo pažeidimas daro poveikį to dėklės sprendinio arba kitų dėklės sprendinių patikimumui. Toks vertinimas turėtų būti grindžiamas vienodais kriterijais, pvz., paveiktų dėklės naudotojų, fizinių asmenų ir dėklės pasikliaujančiųjų šalių skaičiumi ir kategorija, paveiktų duomenų pobūdžiu, saugumo arba patikimumo pažeidimo trukme, ribotu paslaugos prieinamumu ir finansiniais nuostoliais, taip pat galimu asmens duomenų pažeidimu. Šiais kriterijais valstybėms narėms turėtų būti suteikta lankstumo ir veiksmų laisvės proporcingai nustatyti, ar daromas poveikis dėklės sprendinio patikimumui ir ar dėklės sprendinio sustabdymas arba, kai tai pagrįsta saugumo arba patikimumo pažeidimo sunkumu, dėklės sprendinio atšaukimas yra tikslingas. Pagal šiuos kriterijus neturėtų būti automatiškai atšaukiamas dėklės sprendinys arba automatiškai sustabdomas dėklės sprendinio teikimas ir naudojimas, bet valstybės narės į juos turėtų tinkamai atsižvelgti spręsdamos, ar būtina dėklės sprendinį atšaukti ar sustabdyti jo teikimą ir naudojimą;

(6) dėl poveikio ir nepatogumų, kuriuos sukelia dėklės sprendinių naudojimo sustabdymas, valstybės narės turės įvertinti, ar būtina atšaukti dėklės vieneto liudijimus arba imtis bet kokių kitų papildomų priemonių, kad būtų galima tinkamai reaguoti į saugumo arba patikimumo pažeidimą;

(7) kad dėklės naudotojai būtų informuojami apie jų dėklių statusą, jiems turi būti suteikta tinkama informacija apie jų dėklėms poveikį darančius saugumo arba patikimumo pažeidimus. Saugumo arba patikimumo pažeidimai taip pat gali paveikti Sąjungoje registruotas dėklės pasikliaujančiąsias šalis, todėl su jomis taip pat turi būti dalijamasi atitinkama informacija apie saugumo arba patikimumo pažeidimus;

(8) siekiant padidinti skaidrumą ir pasitikėjimą skaitmeninės tapatybės ekosistema, informacija apie saugumo arba patikimumo pažeidimus ir apie jų pasekmes turėtų apimti bent informaciją, kurios reikalaujama pagal šį reglamentą. Tačiau informacija apie saugumo arba patikimumo pažeidimus, kuria dalijamasi su dėklės naudotojais ir dėklės pasikliaujančiosiomis šalimis, turėtų būti atidžiai įvertinta, kad jais negalėtų pasinaudoti išpuolių vykdytojai ir kad tokia rizika būtų kuo mažesnė;

([7]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828, (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) kad pašalinus saugumo pažeidimą arba atkūrus patikimumą naudotojai galėtų vėl turėti prieigą prie savo dėklės vienetų, dėklės sprendinius pateikusi valstybė narė turės nepagrįstai nedelsdama atkurti tų dėklės sprendinių teikimą ir naudojimą. Tai galima padaryti atkuriant dėklės vienetus, išduodant dėklės vienetus, pateiktus pagal naują dėklės sprendinių versiją, arba iš naujo išduodant naujus galiojančius dėklės vieneto liudijimus. Paveikti dėklės naudotojai, dėklės pasikliaujančiosios šalys, bendrieji kontaktiniai punktai, paskirti pagal Reglamento (ES) Nr. 910/2014 46c straipsnio 1 dalį, ir Komisija turi būti atitinkamai informuojami;

(10) siekiant užtikrinti, kad dėklės būtų pašalintos, kai saugumo pažeidimas nepašalinamas arba patikimumas neatkuriamas per tris mėnesius nuo sustabdymo arba kai tai pagrįsta saugumo arba patikimumo pažeidimo sunkumu, valstybė narė turėtų užtikrinti, kad atitinkami dėklės vieneto liudijimai būtų atšaukti, kad jie nebūtų padaryti vėl galiojančiais ir jų nebūtų galima išduoti ar pateikti esamiems dėklės vienetams. Be to, pagal paveiktą dėklės sprendinį neturėtų būti teikiami jokie nauji dėklės vienetai. Skaidrumo tikslais apie pašalinimą turi būti informuojami naudotojai, pasikliaujančiosios šalys, bendrieji kontaktiniai punktai, paskirti pagal Reglamento (ES) Nr. 910/2014 46c straipsnio 1 dalį, ir Komisija. Be kita ko, aprašomas galimas poveikis dėklės naudotojams, visų pirma išduotų liudijimų administravimo požiūriu, arba dėklės pasikliaujančiosioms šalims;

(11) trijų mėnesių laikotarpiu nuo dėklės sprendinio teikimo ir naudojimo sustabdymo, per kurį turi būti pašalintas tokį sustabdymą lėmęs saugumo pažeidimas arba atkurtas patikimumas, turėtų būti numatytas terminas, po kurio dėklės sprendinys turi būti pašalintas, nebent būtų įgyvendinta tinkama taisomoji priemonė. Tačiau valstybės narės gali reikalauti, kad saugumo pažeidimas būtų pašalintas arba patikimumas būtų atkurtas per trumpesnį nei trijų mėnesių laikotarpį, visų pirma atsižvelgdamos, kai aktualu, į to saugumo arba patikimumo pažeidimo mastą, trukmę ir pasekmes. Jeigu per valstybės narės nustatytą laikotarpį saugumo pažeidimo pašalinti arba patikimumo atkurti negalima, valstybė narė gali reikalauti, kad dėklės sprendinys būtų atšauktas nepasibaigus trijų mėnesių laikotarpiui. Valstybės narės turėtų pasinaudoti šiuo laikotarpiu, per kurį turi būti pašalintas dėklės sprendinio teikimo ir naudojimo sustabdymą lėmęs saugumo pažeidimas arba atkurtas patikimumas, kad būtų pasirengta galimam to dėklės sprendinio atšaukimui ir su tuo susijusiems pranešimams;

(12) siekiant sumažinti valstybėms narėms dėl informacijos, kuri pagal šį reglamentą turi būti pateikta Komisijai ir kitoms valstybėms narėms, tenkančią administracinę naštą, valstybės narės turėtų naudotis esamomis pranešimo priemonėmis, pvz., Europos Sąjungos kibernetinio saugumo agentūros (ENISA) valdoma Pranešimo apie kibernetinius incidentus ir jų analizės sistema (CIRAS). Alternatyvių kanalų ar priemonių, kurie turi būti naudojami siekiant informuoti dėklės naudotojus, kuriems padarė poveikį saugumo arba patikimumo pažeidimas, ir dėklės pasikliaujančiąsias šalis, atžvilgiu valstybės narės turėtų užtikrinti, kad atitinkama informacija būtų teikiama aiškiai, išsamiai ir suprantamai. Kanalai, kuriais tokia informacija teikiama paveiktiems dėklės naudotojams ir dėklės pasikliaujančiosioms šalims, turėtų apimti tinkamus transliavimo interneto svetainėse, interneto svetainių atnaujinimų stebėjimo tikruoju laiku ir naujienų agregavimo sprendimus;

(13) vadovaujantis Reglamento (ES) 2018/1725 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir 2025 m. sausio 31 d. jis pateikė nuomonę;

(14) šiame reglamente numatytos priemonės atitinka pagal Reglamento (ES) Nr. 910/2014 48 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Dalykas

Šiuo reglamentu nustatomos reagavimo į dėklių, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų patvirtinimo mechanizmų ir elektroninės atpažinties schemos, pagal kurią teikiamos dėklės, saugumo pažeidimus taisyklės.

2 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) dėklės sprendinys – programinės ir aparatinės įrangos, paslaugų, nuostačių ir konfigūracijų derinys, apimantis dėklės egzempliorius, vieną ar daugiau saugių dėklės šifravimo programų ir vieną ar daugiau saugių dėklės šifravimo įrenginių;

2) dėklės naudotojas – naudotojas, valdantis dėklės vienetą;

3) dėklės pasikliaujančioji šalis – pasikliaujančioji šalis, kuri skaitmenine sąveika teikdama viešąsias ar privačiąsias paslaugas, ketina kliautis dėklės vienetais;

4) dėklės egzempliorius – dėklės naudotojo įrenginyje arba aplinkoje įdiegta ir sukonfigūruota taikomoji programa, kuri yra dėklės vieneto dalis ir kurią dėklės naudotojas naudoja sąveikai su dėklės vienetu;

5) saugi dėklės šifravimo programa – taikomoji programa ypatingos svarbos turtui valdyti, susieta su saugiu dėklės šifravimo įrenginiu ir naudojanti jo teikiamas šifravimo ir kitas funkcijas;

6) saugus dėklės šifravimo įrenginys – manipuliavimui atsparus įrenginys, suteikiantis aplinką, kuri susieta su saugia dėklės šifravimo programa ir kurią ši programa naudoja ypatingos svarbos turtui apsaugoti ir šifravimo funkcijoms atlikti, kad būtų galima saugiai vykdyti ypatingos svarbos operacijas;

7) dėklės teikėjas – fizinis arba juridinis asmuo, teikiantis dėklės sprendinius;

8) dėklės vienetas – unikalios konfigūracijos dėklės sprendinys, apimantis dėklės egzempliorius, saugias dėklės šifravimo programas ir saugius dėklės šifravimo įrenginius, kuriuos dėklės teikėjas teikia atskiram dėklės naudotojui;

9) ypatingos svarbos turtas – dėklės vienetui priklausantis arba su juo susijęs turtas, kurio svarba tokia didelė, kad pažeistas jo prieinamumas, konfidencialumas ar vientisumas turėtų labai didelį neigiamą poveikį patikimam dėklės vieneto naudojimui;

10) dėklės vieneto liudijimas – duomenų objektas, kuris apibūdina dėklės vieneto komponentus arba leidžia nustatyti tų komponentų tapatumą ir juos patvirtinti.

3 straipsnis

Saugumo arba patikimumo pažeidimo nustatymas

1. Nedarant poveikio Direktyvai (ES) 2022/2555 ir reglamentams (ES) 2019/881 ir (ES) 2024/2847, kad įvertintų, ar dėklės sprendinio, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų patvirtinimo mechanizmų arba elektroninės atpažinties schemos, pagal kurią teikiamas dėklės sprendinys, saugumo arba patikimumo pažeidimas daro poveikį jų arba kitų dėklės sprendinių patikimumui, valstybės narės tinkamai atsižvelgia į šio reglamento I priede nustatytus kriterijus.

2. Jei valstybė narė, remdamasi 1 dalyje nurodytu vertinimu, nustato, kad saugumo arba patikimumo pažeidimas daro poveikį dėklės sprendinio patikimumui, ir dėl šios priežasties sustabdo to dėklės sprendinio teikimą ir naudojimą, ta valstybė narė imasi 4 ir 5 straipsniuose nustatytų priemonių. Jei valstybė narė dėklės sprendinį pašalina, ta valstybė narė imasi 8 ir 9 straipsniuose nustatytų priemonių.

3. Jei valstybė narė gavo informaciją, susijusią su galimu saugumo arba patikimumo pažeidimu, galinčiu daryti poveikį vieno ar daugiau kitos valstybės narės pateiktų dėklės sprendinių patikimumui, ta valstybė narė nepagrįstai nedelsdama apie tai praneša Komisijai ir paveiktų valstybių narių bendriesiems kontaktiniams punktams, paskirtiems pagal Reglamento (ES) Nr. 910/2014 46c straipsnio 1 dalį. Šiame pranešime pateikiama 5 straipsnio 2 dalyje nustatyta informacija.

4. Pagal 3 dalį pateiktą informaciją gavusi valstybė narė nepagrįstai nedelsdama imasi 1 ir 2 dalyse nustatytų priemonių.

4 straipsnis

Dėklių teikimo ir naudojimo sustabdymas ir kitos taisomosios priemonės

1. Valstybės narės užtikrina, kad pagal dėklės sprendinį, kurio galiojimas sustabdytas, nebūtų teikiami, naudojami ar aktyvuojami jokie dėklės vienetai.

2. Valstybės narės įvertina, ar siekiant tinkamai reaguoti į saugumo arba patikimumo pažeidimą, būtina atšaukti dėklės vienetų, kuriuos paveikė dėklės sprendinio galiojimo sustabdymas, dėklės vieneto liudijimus arba taikyti bet kokią kitą papildomą taisomąją priemonę.

3. 1 ir 2 dalyse nustatytų priemonių imamasi nepagrįstai nedelsiant ir bet kuriuo atveju ne vėliau kaip per 24 valandas nuo dėklės sprendinio, kurį paveikė saugumo arba patikimumo pažeidimas, teikimo ir naudojimo sustabdymo.

4. 1 ir 2 dalyse nustatytos priemonės netrukdo paveiktiems dėklės naudotojams pasinaudoti Reglamento (ES) Nr. 910/2014 5a straipsnio 4 dalies g punkte nustatyta teise į duomenų perkeliamumą. Turi būti laikomasi sąlygos, kad dėklės naudotojai šia teise gali naudotis nepakenkdami paveiktų dėklės vienetų ypatingos svarbos turto saugumui, visų pirma atsižvelgiant į sustabdymo priežastis ir būtinybę užtikrinti veiksmingą to turto apsaugą nuo netinkamo naudojimo.

5 straipsnis

Informacija apie sustabdymą ir taisomąsias priemones

1. Nepagrįstai nedelsiant ir ne vėliau kaip per 24 valandas nuo dėklės sprendinio teikimo ir naudojimo sustabdymo pateikiama aiški, išsami ir lengvai prieinama informacija apie dėklės sprendinio teikimo ir naudojimo sustabdymą:

a) pagal Reglamento (ES) Nr. 910/2014 46c straipsnio 1 dalį paskirtiems bendriesiems kontaktiniams punktams;

b) Komisijai;

c) paveiktiems dėklės naudotojams;

d) pagal Reglamento (ES) Nr. 910/2014 5b straipsnį užregistruotoms dėklės pasikliaujančiosioms šalims.

2. Pagal 1 dalį pateikiama bent ši informacija:

a) dėklės sprendinio, kurio teikimas ir naudojimas sustabdytas, teikėjo pavadinimas;

b) to dėklės sprendinio pavadinimas ir nuorodos identifikatorius, nurodytas pagal Reglamento (ES) Nr. 910/2014 5d straipsnį sudarytame sertifikuotų dėklių sąraše, ir, kai taikytina, susijusios sprendinio versijos;

c) data ir laikas, kada buvo nustatytas saugumo arba patikimumo pažeidimas;

d) jei žinoma, data ir laikas, kada saugumo arba patikimumo pažeidimas buvo padarytas, remiantis tinklo ar sistemos žurnalais ar kitais duomenų šaltiniais;

e) dėklės sprendinio galiojimo sustabdymo data ir laikas;

f) pranešančiosios valstybės narės ir, jei skiriasi, a punkte nurodyto dėklės teikėjo kontaktiniai duomenys, įskaitant bent e. pašto adresą ir telefono numerį;

g) saugumo arba patikimumo pažeidimo aprašymas;

h) pažeistų duomenų aprašymas, įskaitant, kai taikytina, asmens duomenų kategorijas, apibrėžtas Reglamento (ES) 2016/679 9 straipsnio 1 dalyje ir 10 straipsnyje;

i) kai įmanoma – apytikslis paveiktų dėklės naudotojų ir kitų paveiktų fizinių asmenų skaičiaus įvertis;

j) galimo poveikio dėklės pasikliaujančiosioms šalims arba dėklės naudotojams aprašymas, o pastaruoju atveju, kai aktualu, nurodymai, kokių priemonių imtis dėklės naudotojams, kad sumažintų tą galimą poveikį;

k) priemonių, kurių imtasi arba planuojama imtis siekiant pašalinti saugumo pažeidimą arba atkurti patikimumą, aprašymas, taip pat tokio pašalinimo ar atkūrimo planas ir terminas;

l) kai taikytina ir tinkama, priemonių, kurių imtasi arba planuojama imtis siekiant, kad paveikti dėklės naudotojai pereitų prie alternatyvių dėklės sprendinių arba paslaugų, aprašymas.

6 straipsnis

Dėklių teikimo ir naudojimo atkūrimas

Kai būtina užtikrinti, kad būtų atkurtas dėklės sprendinio teikimas, aktyvavimas ir naudojimas, valstybės narės nepagrįstai nedelsdamos:

1) atkuria pagal tą dėklės sprendinį teikiamų dėklės vienetų teikimą ir naudojimą, visiems paveiktiems naudotojams išduodant dėklės vienetą, atitinkantį naujos versijos dėklės sprendinį;

2) išduoda naujus dėklės vieneto liudijimus naujiems dėklės vienetams arba, kai taikytina, anksčiau išduotiems dėklės vienetams, jei tie vienetai atitinka galiojančius saugumo reikalavimus pašalinus saugumo pažeidimą arba atkūrus patikimumą;

3) panaikina bet kokią pagal 4 straipsnį įgyvendintą priemonę, kuria trukdoma teikti naujus dėklės vienetus pagal paveiktą dėklės sprendinį, jei ta priemonė buvo susijusi tik su dabar pašalintu saugumo pažeidimu arba atkurtu patikimumu.

7 straipsnis

Informacija apie atkūrimą

Dėklės sprendinį atkūrusi valstybė narė užtikrina, kad:

1) informacija apie tą faktą nepagrįstai nedelsiant pateikiama visoms šalims, gavusioms informaciją apie to dėklės sprendinio teikimo ir naudojimo sustabdymą pagal 5 straipsnio 1 dalį;

2) pagal 1 punktą teikiama informacija apima bent 5 straipsnio 2 dalies a, b ir f–h punktuose nurodytus elementus ir šiuos dalykus:

   a) datą ir laiką, kada buvo pašalintas saugumo pažeidimas arba atkurtas patikimumas;

   b) paveikto dėklės sprendinio ir, kai tinkama, paveiktų dėklės vienetų, teikiamų pagal tą dėklės sprendinį, atkūrimo datą ir laiką;

   c) priemonių, kurių imtasi siekiant pašalinti saugumo pažeidimą arba atkurti patikimumą, aprašymą;

   d) galimo likutinio poveikio dėklės pasikliaujančiosioms šalims arba dėklės naudotojams aprašymą, o pastaruoju atveju, kai aktualu, nurodymus, kokių priemonių imtis dėklės naudotojams, kad sumažintų tą galimą likutinį poveikį;

8 straipsnis

Dėklių pašalinimas

1. Jei per tris mėnesius nuo dėklės sprendinio teikimo ir naudojimo sustabdymo dienos tokį sustabdymą lėmęs saugumo pažeidimas nepašalinamas arba patikimumas neatkuriamas, tokį dėklės sprendinį teikianti valstybė narė užtikrina, kad nepagrįstai nedelsiant ir bet kuriuo atveju per 72 valandas nuo trijų mėnesių laikotarpio pabaigos paveiktas dėklės sprendinys būtų pašalintas ir jo galiojimas būtų atšauktas.

2. Dėklės sprendinį pašalinusi valstybė narė užtikrina, kad:

a) paveikto dėklės sprendinio dėklės vieneto liudijimai būtų atšaukti;

b) dėklės vieneto liudijimų negalima būtų padaryti vėl galiojančiais;

c) esamiems dėklėms vienetams, teikiamiems pagal paveiktą dėklės sprendinį, negali būti išduodamas joks naujas dėklės vieneto liudijimas;

d) pagal paveiktą dėklės sprendinį negali būti teikiamas joks naujas dėklės vienetas.

3. 1 ir 2 dalyse nustatytos priemonės netrukdo paveiktiems dėklės naudotojams pasinaudoti Reglamento (ES) Nr. 910/2014 5a straipsnio 4 dalies g punkte nustatyta teise į duomenų perkeliamumą. Turi būti laikomasi sąlygos, kad dėklės naudotojai šia teise gali naudotis nepakenkdami paveiktų dėklės vienetų ypatingos svarbos turto saugumui, visų pirma atsižvelgiant į pašalinimo priežastis ir būtinybę užtikrinti veiksmingą to turto apsaugą nuo netinkamo naudojimo.

9 straipsnis

Informacija apie pašalinimą

1. Nepagrįstai nedelsiant ir ne vėliau kaip per 24 valandas nuo dėklės sprendinio pašalinimo pateikiama aiški, išsami ir lengvai prieinama informacija apie dėklės sprendinio teikimo ir naudojimo sustabdymą:

a) pagal Reglamento (ES) Nr. 910/2014 46c straipsnio 1 dalį paskirtiems bendriesiems kontaktiniams punktams;

b) Komisijai;

c) paveiktiems dėklės naudotojams;

d) pagal Reglamento (ES) Nr. 910/2014 5b straipsnį užregistruotoms dėklės pasikliaujančiosioms šalims.

2. Pagal 1 dalį pateikiama bent ši informacija:

a) atšaukto dėklės sprendinio teikėjo pavadinimas;

b) to dėklės sprendinio nuorodos identifikatorius, nurodytas pagal Reglamento (ES) Nr. 910/2014 5d straipsnį sudarytame sertifikuotų dėklių sąraše, ir, kai taikytina, susijusios versijos;

c) saugumo arba patikimumo pažeidimo, dėl kurio paveiktas dėklės sprendinys dėl pažeidimo sunkumo buvo pašalintas, arba dėl to, kad pažeidimas nebuvo pašalintas per tris mėnesius, nustatymo data ir laikas;

d) jei žinoma, data ir laikas, kada saugumo arba patikimumo pažeidimas buvo padarytas, remiantis tinklo ar sistemos žurnalais ar kitais duomenų šaltiniais;

e) dėklės sprendinio pašalinimo ir faktinio dėklės vienetų liudijimų, teikiamų pagal tą dėklės sprendinį, atšaukimo data ir laikas;

f) ar dėklės sprendinys atšauktas dėl saugumo arba patikimumo pažeidimo sunkumo, ar dėl to, kad saugumo pažeidimas nebuvo pašalintas arba patikimumas nebuvo atkurtas;

g) pranešančiosios valstybės narės ir, jei skiriasi, a punkte nurodyto dėklės teikėjo kontaktiniai duomenys, įskaitant bent e. pašto adresą ir telefono numerį;

h) saugumo arba patikimumo pažeidimo aprašymas;

i) pažeistų duomenų aprašymas, įskaitant, kai taikytina, asmens duomenų kategorijas, nurodytas Reglamento (ES) 2016/679 9 straipsnio 1 dalyje ir 10 straipsnyje;

j) kai įmanoma – apytikslis paveiktų dėklės naudotojų ir kitų paveiktų fizinių asmenų skaičiaus įvertis;

k) galimo poveikio dėklės pasikliaujančiosioms šalims arba dėklės naudotojams aprašymas, o pastaruoju atveju, kai aktualu, nurodymai, kokių priemonių imtis dėklės naudotojams, kad sumažintų tą galimą poveikį;

l) priemonių, kurių imtasi arba planuojama imtis siekiant, kad paveikti dėklės naudotojai pereitų prie alternatyvių dėklės sprendinių arba, kai taikytina ir tinkama, prie alternatyvių paslaugų, aprašymas.

10 straipsnis

Informacinė sistema

3, 5, 7 ir 9 straipsniuose nurodytą informaciją valstybės narės siunčia Komisijai ir valstybių narių bendriesiems kontaktiniams punktams, paskirtiems pagal Reglamento (ES) Nr. 910/2014 46c straipsnio 1 dalį, per ENISA valdomą sistemą CIRAS arba lygiavertę sistemą, dėl kurios susitarė valstybės narės ir Komisija.

11 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse, išskyrus 10 straipsnį, kuris taikomas nuo 2026 m. gegužės 7 d.

Priimta Briuselyje 2025 m. gegužės 6 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

PRIEDAS

Saugumo arba patikimumo pažeidimo vertinimo kriterijai

1. Valstybės narės saugumo arba patikimumo pažeidimo vertinimą grindžia šiais kriterijais:

a) saugumo arba patikimumo pažeidimas sukėlė arba gali sukelti fizinio asmens mirtį arba padaryti didelę žalą fizinio asmens sveikatai;

b) sėkminga, kaip įtariama, piktavališka arba neteisėta prieiga prie dėklės teikėjo, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų patvirtinimo mechanizmų teikėjo arba elektroninės atpažinties schemos, pagal kurią teikiamas dėklės sprendinys, teikėjo (toliau – susiję subjektai) tinklų ir informacinių sistemų buvo arba gali būti įgyta tokiu būdu, kuris gali smarkiai sutrikdyti veiklą, ir tos sistemos yra esminiai paveikto dėklės sprendinio, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų paveiktų patvirtinimo mechanizmų arba paveiktos elektroninės atpažinties schemos, pagal kurią teikiamas dėklės sprendinys, komponentai;

c) dėklės sprendinys, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytas patvirtinimo mechanizmas arba elektroninės atpažinties schema, pagal kurią teikiamas dėklės sprendinys, arba jų dalis:

— daugiau kaip 12 valandų iš eilės dėklės naudotojams arba dėklės pasikliaujančiosioms šalims yra arba, numatoma, bus visiškai neprieinami,

— daugiau kaip 16 valandų per kalendorinę savaitę dėklės naudotojams arba dėklės pasikliaujančiosioms šalims yra arba, numatoma, bus visiškai neprieinami;

d) įtariama, kad riboto dėklės sprendinio arba su juo susijusių subjektų teikiamų paslaugų prieinamumo yra paveikti arba, numatoma, bus paveikti daugiau kaip 1 % dėklės naudotojų arba dėklės pasikliaujančiųjų šalių;

e) esama galimybės, kad fizinė prieiga (taikoma tik patikimiems susijusių subjektų darbuotojams) arba tokios fizinės prieigos prie vienos ar daugiau dėklės sprendinį palaikančių tinklo ir informacinių sistemų vietų apsauga, Reglamento (ES) Nr. 910/2014 5a straipsnio 8 dalyje nurodytų patvirtinimo mechanizmų, susijusių su dėklės sprendiniu, arba elektroninės atpažinties schemos, pagal kurią teikiamas dėklės sprendinys, teikimas gali būti arba buvo pažeisti;

f) dėklės sprendinyje saugomų, juo perduodamų ar tvarkomų duomenų privatumas, vientisumas, konfidencialumas ar autentiškumas yra arba gali būti pažeisti vienu ar keliais iš šių būdų:

— pažeidimas daro poveikį daugiau kaip 1 % paveikto dėklės sprendinio naudotojų arba daugiau kaip 100 000 tų dėklės naudotojų, priklausomai nuo to, kuris skaičius yra mažesnis,

— pažeidimas yra sėkmingai įgyvendintos piktavališkos veiklos rezultatas,

— pažeidimas yra arba, tikėtina, gali būti vieno ar daugiau žinomų pažeidžiamumo atvejų, įskaitant tvarkomus pagal Komisijos įgyvendinimo reglamentą (ES) 2024/2981 ([1]), rezultatas,

— pažeidimas gali asmens duomenis paveikti taip, kad galėtų kilti pavojus atitinkamų fizinių asmenų teisėms ir laisvėms, visų pirma asmens duomenų, apibrėžtų Reglamento (ES) 2016/679 9 straipsnio 1 dalyje ir 10 straipsnyje, pažeidimo atveju,

([1]) 2024 m. lapkričio 28 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2981, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 nuostatų dėl europinių skaitmeninės tapatybės dėklių sertifikavimo taikymo taisyklės (OL L, 2024/2981, 2024 12 4, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— tikėtina, kad pažeidimas turės įtakos asmeniniams elektroniniams ryšiams,

— dėl pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms,

— tikėtina, kad pažeidimas paveiks pažeidžiamus fizinius asmenis;

g) dėklės sprendinio sertifikavimas buvo atšauktas arba numatoma, kad jis bus atšauktas;

h) dėl saugumo arba patikimumo pažeidimo susijęs subjektas patyrė arba gali patirti tiesioginių finansinių nuostolių, kurių suma viršija 500 000 EUR arba, kai taikytina, 5 % ankstesnių finansinių metų bendros metinės susijusio subjekto apyvartos, atsižvelgiant į tai, kuri suma yra mažesnė.

2. Valstybės narės neatsižvelgia į planines susijusių subjektų arba jų vardu atliekamos techninės priežiūros operacijos pasekmes, jeigu:

a) apie tokią techninės priežiūros operaciją buvo iš anksto pranešta galimai paveiksimiems dėklės naudotojams, dėklės pasikliaujančiosiomis šalims ir atitinkamoms kompetentingoms priežiūros įstaigoms;

b) ji neatitinka nė vieno iš šio priedo 1 dalyje nustatytų kriterijų.

3. Kiek tai susiję su 1 dalies c punktu, prieinamumui poveikį darančio incidento trukmė matuojama nuo to momento, kai sutrikdomas tinkamas paveiktos paslaugos teikimas, iki to momento, kai paslauga atkuriama ir vėl pradedama teikti. Tais atvejais, kai susijęs subjektas sutrikimo pradžios momento nustatyti negali, incidento trukmė skaičiuojama nuo ankstesnio iš šių momentų: incidento nustatymo momento arba incidento užregistravimo tinklo ar sistemos žurnaluose arba kituose duomenų šaltiniuose momento. Visiško paslaugos neprieinamumo trukmė skaičiuojama nuo momento, kurį paslauga tampa visiškai neprieinama naudotojams, iki momento, kurį įprasta veikla ar operacijos atkuriamos iki tokio paslaugų lygio, koks buvo užtikrinamas iki incidento. Kai susijęs subjektas negali nustatyti, kada paslauga tapo visiškai neprieinama, neprieinamumo trukmė skaičiuojama nuo momento, kurį tas subjektas nustatė, kad paslauga neprieinama.

4. Kiek tai susiję su 1 dalies d punktu, laikoma, kad paslauga prieinama tik iš dalies, visų pirma tais atvejais, kai ji veikia daug lėčiau, palyginti su vidutine atsako trukme, arba kai veikia ne visos jos funkcijos. Atsako delsai įvertinti, kai įmanoma, turėtų būti taikomi objektyvūs kriterijai, pagrįsti vidutine paslaugų atsako trukme.

5. Kad nustatytų dėl 1 dalies h punkte nurodyto saugumo arba patikimumo pažeidimo patirtus tiesioginius finansinius nuostolius, susiję subjektai atsižvelgia į visus dėl incidento patirtus finansinius nuostolius, tokius kaip programinės įrangos, aparatinės įrangos ar infrastruktūros keitimo ar perkėlimo išlaidos, išlaidos darbuotojams, įskaitant išlaidas, susijusias su darbuotojų pakeitimu ar perkėlimu, papildomų darbuotojų įdarbinimu, atlyginimu už viršvalandžius ir prarastų arba pablogėjusių įgūdžių atgavimu, mokesčiai, mokėtini dėl sutartinių įsipareigojimų nevykdymo, žalos atlyginimo ir kompensacijų klientams išlaidos, nuostoliai dėl negautų pajamų, su vidaus ir išorės komunikacija susijusios išlaidos, konsultavimosi išlaidos, įskaitant išlaidas, susijusias su teisinėmis konsultacijomis, teismo ekspertizės paslaugomis ir pažeidimų padarinių pašalinimo paslaugomis. Kasdienei verslo veiklai vykdyti būtinos išlaidos, pvz., infrastruktūros, įrenginių, aparatinės ir programinės įrangos bendrosios techninės priežiūros, patobulinimų ir rizikos vertinimo iniciatyvų išlaidos ir draudimo įmokos, nelaikomos dėl incidento patirtais finansiniais nuostoliais. Finansinių nuostolių sumas susiję subjektai apskaičiuoja remdamiesi turimais duomenimis, o tais atvejais, kai faktinių finansinių nuostolių sumų nustatyti neįmanoma, tie subjektai apskaičiuoja tų sumų įverčius.