2025/847

7.5.2025

KOMISJONI RAKENDUSMÄÄRUS (EL) 2025/847,

6. mai 2025,

millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses reageerimisega Euroopa digiidentiteedikukrute turvarikkumistele

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrust (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ), ([1]) eriti selle artikli 5e lõiget 5,

ning arvestades järgmist:

(1) Euroopa digiidentiteedi raamistik (edaspidi „raamistik“), mis kehtestati määrusega (EL) nr 910/2014, on kogu liitu hõlmava turvalise ja koostöövõimelise digiidentiteedisüsteemi loomisel üks keskseid elemente. Raamistik, mille nurgakivi on Euroopa digiidentiteedikukkur (edaspidi „kukkur“), taotleb eesmärki hõlbustada teenuste kättesaadavust kõigis liikmesriikides, tagades samal ajal isikuandmete ja privaatsuse kaitse.

(2) Isikuandmete sellise töötlemise suhtes, mis toimub käesoleva määruse raames, kohaldatakse Euroopa Parlamendi ja nõukogu määrusi (EL) 2016/679 ([2]) ja (EL) 2018/1725 ([3]) ning vajaduse korral Euroopa Parlamendi ja nõukogu direktiivi 2002/58/EÜ ([4]). Käesoleva määruse alusel kehtestatud normid teabe hindamise ja esitamise kohta ei piira kohustust teatada pädevale järelevalveasutusele isikuandmetega seotud rikkumistest, kui see on kohaldatav määruse (EL) 2016/679 või määruse (EL) 2018/1725 alusel, ega kohustust teatada andmesubjektidele isikuandmetega seotud rikkumistest, kui see on nimetatud määruste alusel kohaldatav.

(3) Komisjon hindab regulaarselt uusi tehnoloogialahendusi, tavasid, standardeid ja tehnilisi spetsifikatsioone. Selleks et kukrute arendamine ja sertifitseerimine oleksid liikmesriikide vahel kõrgeimal tasemel ühtlustatud, tuginevad käesolevas rakendusmääruses esitatud tehnilised spetsifikatsioonid tööle, mida on tehtud komisjoni soovituse (EL) 2021/946 ([5]) põhjal, ning eeskätt selle osaks olevale arhitektuurile ja võrdlusraamistikule. Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1183 ([6]) põhjendusele 75 peaks komisjon käesoleva määruse läbi vaatama ja vajaduse korral seda ajakohastama, et tagada kooskõla üleilmsete arengusuundumustega, arhitektuuriga ja võrdlusraamistikuga ja järgida siseturu parimaid tavasid.

([1]) ELT L 257, 28.8.2014, lk 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).
([4]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([5]) Komisjoni 3. juuni 2021. aasta soovitus (EL) 2021/946, mis käsitleb ühiseid liidu tööriistu Euroopa digiidentiteedi raamistiku koordineeritud käsitlusviisi jaoks (ELT L 210, 14.6.2021, lk 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([6]) Euroopa Parlamendi ja nõukogu 11. aprilli 2024. aasta määrus (EL) 2024/1183, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega (ELT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Kukrulahenduste, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud valideerimismehhanisme või kukrulahenduste pakkumise aluseks olevat e-identimise süsteemi puudutava turvarikkumise või kahjustamise korral tuleb sellistele rikkumistele ja kahjustamistele reageerida kõigis liikmesriikides kiiresti, kooskõlastatult ja turvaliselt, et kaitsta kasutajaid ja säilitada digiidentiteedisüsteemi usaldusväärsus. See ei piira Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ([7]) ning Euroopa Parlamendi ja nõukogu määruste (EL) 2019/881 ([8]) ja (EL) 2024/2847 ([9]) kohaldamist, eelkõige seoses intsidentide või nõrkuste käsitlemisega ja nende käsitamisega turvarikkumistena. Seepärast peaksid liikmesriigid turvarikkumisest või kahjustamisest mõjutatud kukrute pakkumise ja kasutamise õigeaegselt peatama või vajaduse korral need kasutuselt kõrvaldama.

(5) Selleks et tagada asjakohane reageerimine turvarikkumisele või kahjustamisele, peaksid liikmesriigid hindama, kas kukrulahenduse, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud valideerimismehhanismide või kukrulahenduse pakkumise aluseks oleva e-identimise süsteemi turvarikkumine või kahjustamine mõjutab selle kukrulahenduse või muude kukrulahenduste usaldusväärsust. Selline hindamine peaks põhinema ühtsetel kriteeriumidel, nagu mõjutatud kukrukasutajate, füüsiliste isikute ja kukrule tuginevate isikute arv ja kategooria, mõjutatud andmete laad, kahjustamise või turvarikkumise kestus, teenuse piiratud kättesaadavus ja rahaline kahju ning võimalik isikuandmete kaitstuse rikkumine. Need kriteeriumid peaksid andma liikmesriikidele paindlikkuse ja kaalutlusõiguse, et teha proportsionaalsel viisil kindlaks, kas kukrulahenduse usaldusväärsust on mõjutatud ja kas kukrulahenduse peatamine või, kui see on rikkumise või kahjustamise tõsiduse tõttu põhjendatud, kasutuselt kõrvaldamine on asjakohane. Need kriteeriumid ei tohiks kaasa tuua kukrulahenduse automaatset kasutuselt kõrvaldamist või kukrulahenduse pakkumise ja kasutamise automaatset peatamist, kuid liikmesriigid peaksid neid kriteeriume nõuetekohaselt kaaluma, kui on tarvis otsustada, kas kukrulahenduse kasutuselt kõrvaldamine või selle pakkumise ja kasutamise peatamine on vajalik.

(6) Kukrulahenduste kasutamise peatamise mõju ja sellest tuleneva ebamugavuse tõttu peavad liikmesriigid hindama, kas turvarikkumisele või kahjustamisele asjakohaselt reageerimiseks on vajalik kukrukomplekti tõendite kehtetuks tunnistamine või mõni muu lisameede

(7) Selleks et teavitada kukrukasutajaid nende kukru staatusest, tuleb neile anda piisavat teavet nende kukrut mõjutavate turvarikkumiste või kahjustamiste kohta. Kuna turvarikkumised ja kahjustamised võivad mõjutada ka selliseid kukrule tuginevaid isikuid, kes on registreeritud liidus, tuleb turvarikkumisi ja kahjustamisi puudutavat teavet jagada ka nendega.

(8) Selleks et suurendada läbipaistvust ja usaldust digiidentiteedisüsteemi vastu, peaks turvarikkumiste või kahjustamiste ja nende tagajärgede kohta esitatav teave sisaldama vähemalt käesoleva määruse alusel nõutavat teavet. Kukrukasutajate ja kukrule tuginevate isikutega jagatavat teavet turvarikkumiste või kahjustamiste kohta tuleks siiski hoolikalt hinnata, et vältida ja minimeerida ohtu, et ründajad seda ära kasutavad.

([7]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Selleks et kasutajad pärast turvarikkumise või kahjustamise kõrvaldamist oma kukrukomplektidele uuesti juurde pääseksid, peab kukrulahendusi pakkunud liikmesriik nende kukrulahenduste pakkumise ja kasutamise ilma põhjendamatu viivituseta taastama. Seda saab teha kukrukomplektide taastamise, kukrulahenduste uue versiooni alusel pakutavate kukrukomplektide väljastamise või uute kehtivate kukrukomplekti tõendite väljastamise kaudu. Mõjutatud kukrukasutajatele, kukrule tuginevatele isikutele, määruse (EL) nr 910/2014 artikli 46c lõike 1 kohaselt määratud ühtsetele kontaktpunktidele ja komisjonile tuleb kasutuselt kõrvaldamisest teatada.

(10) Selleks et kukrud kasutuselt kõrvaldada, kui turvarikkumist või kahjustamist ei ole kolme kuu jooksul pärast peatamist kõrvaldatud või kui kasutuselt kõrvaldamine on põhjendatud turvarikkumise või kahjustamise tõsidusega, peaks liikmesriik tagama, et vastavad kukrukomplektide tõendid tunnistatakse kehtetuks ja et kehtivat staatust ei saa ennistada ega väljastada või pakkuda olemasolevatele kukrukomplektidele. Lisaks ei tohiks mõjutatud kukrulahenduse raames pakkuda uusi kukrukomplekte. Läbipaistvuse huvides tuleb kasutajatele, tuginevatele isikutele, määruse (EL) nr 910/2014 artikli 46c lõike 1 kohaselt määratud ühtsetele kontaktpunktidele ja komisjonile kasutuselt kõrvaldamisest teatada. Seejuures tuleb kirjeldada võimalikku mõju kukrukasutajatele, sh väljastatud tõendite haldamisele, või kukrule tuginevatele isikutele.

(11) Kolm kukrulahenduse pakkumise ja kasutamise peatamise järgset kuud, mille jooksul tuleb kõrvaldada peatamise tinginud turvarikkumine või kahjustamine, peaks olema tähtaeg, mille möödumisel tuleb kukrulahendus kasutuselt kõrvaldada, välja arvatud juhul, kui on rakendatud asjakohast parandusmeedet. Liikmesriigid võivad aga nõuda, et turvarikkumine või kahjustamine kõrvaldataks vähem kui kolmekuulise tähtaja jooksul, võttes eelkõige ja vajaduse korral arvesse kõnealuse turvarikkumise või kahjustamise ulatust, kestust ja tagajärgi. Kui turvarikkumist või kahjustamist ei kõrvaldata või kui seda ei saa kõrvaldada liikmesriigi määratud tähtaja jooksul, võib liikmesriik nõuda kukrulahenduse kasutuselt kõrvaldamist enne kolme kuu möödumist. Liikmesriigid peaksid kasutama seda ajavahemikku, mille jooksul kukrulahenduse pakkumise ja kasutamise peatamiseni viinud turvarikkumine või kahjustamine tuleb kõrvaldada, et valmistuda selle kukrulahenduse võimalikuks kasutuselt kõrvaldamiseks ja sellest tulenevate teadete saatmiseks.

(12) Selleks et vähendada liikmesriikide halduskoormust seoses teabega, mis tuleb käesoleva määruse kohaselt esitada komisjonile ja teistele liikmesriikidele, peaksid liikmesriigid kasutama olemasolevaid teavitamisvahendeid, nagu küberintsidentidest teatamise ja nende analüüsi süsteem, mida haldab Euroopa Liidu Küberturvalisuse Amet (edaspidi „ENISA“). Mis puutub alternatiivsetesse kanalitesse või vahenditesse, mida kasutatakse turvarikkumisest või kahjustamisest mõjutatud kukrukasutajate ja kukrule tuginevate isikute teavitamiseks, peaksid liikmesriigid tagama asjakohase teabe esitamise selgel, arusaadaval ja kergesti kättesaadaval viisil. Kanalid sellise teabe esitamiseks mõjutatud kukrukasutajatele ja kukrule tuginevatele isikutele peaksid hõlmama asjakohaseid lahendusi veebipõhise ringhäälingu, veebisaitide ajakohastamise reaalajas jälgimise ja uudiste agregeerimise näol.

(13) Vastavalt määruse (EL) 2018/1725 artikli 42 lõikele 1 on konsulteeritud Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 31. jaanuaril 2025.

(14) Käesoleva määrusega ette nähtud meetmed on kooskõlas määruse (EL) nr 910/2014 artikliga 48 loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Reguleerimisese

Käesoleva määrusega kehtestatakse eeskirjad, mille alusel reageerida kukrute, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud valideerimismehhanismide ja kukrute pakkumise aluseks oleva e-identimise süsteemi turvarikkumistele.

Artikkel 2

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „kukrulahendus“ – tarkvara, riistvara, teenuste, seadete ja konfiguratsioonide kombinatsioon, sealhulgas kukrueksemplar, üks või mitu kukru turvalist krüptorakendust ja üks või mitu kukru turvalist krüptoseadet;

2) „kukrukasutaja“ – kasutaja, kelle kontrolli all kukrukomplekt on;

3) „kukrule tuginev isik“ – tuginev isik, kes kavatseb tugineda kukrukomplektidele avalike või erateenuste osutamiseks digitaalse suhtluse kaudu;

4) „kukrueksemplar“ – kukrukasutaja seadmesse või keskkonda paigaldatud ja seal konfigureeritud rakendus, mis on kukrukomplekti osa ja mida kukrukasutaja kasutab kukrukomplektiga toimuva interaktsiooni jaoks;

5) „kukru turvaline krüptorakendus“ – rakendus, mis haldab kriitilise tähtsusega vara selle kaudu, et on lingitud kukru turvalise krüptoseadme pakutavate krüptofunktsioonide ja muude funktsioonidega ning kasutab neid;

6) „kukru turvaline krüptoseade“ – muukimiskindel seade, mis pakub keskkonda, mis on lingitud kukru turvalise krüptorakendusega, mis seda seadet kasutab, et kaitsta kriitilise tähtsusega vara ja pakkuda krüptofunktsioone kriitilise tähtsusega toimingute turvaliseks teostamiseks;

7) „kukruteenuse pakkuja“ – füüsiline või juriidiline isik, kes pakub kukrulahendusi;

8) „kukrukomplekt“ – kukrulahenduse kordumatu konfiguratsioon, mis sisaldab kukrueksemplare, kukru turvalisi krüptorakendusi ja kukru turvalisi krüptoseadmeid ning mida kukruteenuse pakkuja pakub individuaalsele kukrukasutajale;

9) „kriitilise tähtsusega vara“ – kukrukomplektis olev või kukrukomplektiga seotud vara, mis on nii oluline, et selle käideldavuse, konfidentsiaalsuse või tervikluse rikkumine avaldaks väga tõsist nõrgestavat mõju suutlikkusele tugineda sellele kukrukomplektile;

10) „kukrukomplekti tõend“ – andmeobjekt, mis kirjeldab kukrukomplekti komponente või lubab nimetatud komponentide autentsust ja kehtivust kinnitada.

Artikkel 3

Turvarikkumise või kahjustamise kindlakstegemine

1. Ilma et see piiraks direktiivi (EL) 2022/2555 ning määruste (EL) 2019/881 ja (EL) 2024/2847 kohaldamist, võtavad liikmesriigid selleks, et hinnata, kas kukrulahenduse, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud valideerimismehhanismide või kukrulahenduse pakkumise aluseks oleva e-identimise süsteemi turvarikkumine või kahjustamine mõjutab nimetatute usaldusväärsust või muude kukrulahenduste usaldusväärsust, nõuetekohaselt arvesse I lisas sätestatud kriteeriume.

2. Kui liikmesriik teeb lõikes 1 sätestatud hindamise põhjal kindlaks, et turvarikkumine või kahjustamine mõjutab kukrulahenduse usaldusväärsust, ning peatab asjaomase kukrulahenduse pakkumise ja kasutamise, võtab see liikmesriik artiklites 4 ja 5 sätestatud meetmed. Kui liikmesriik kõrvaldab kukrulahenduse kasutuselt, võtab ta artiklites 8 ja 9 sätestatud meetmed.

3. Kui liikmesriigini jõuab teave seoses võimaliku turvarikkumise või kahjustamisega, mis võib mõjutada teise liikmesriigi pakutava ühe või mitme kukrulahenduse usaldusväärsust, teatab see liikmesriik sellest asjaolust põhjendamatu viivituseta komisjonile ja mõjutatud liikmesriikide ühtsetele kontaktpunktidele, mis on määratud määruse (EL) nr 910/2014 artikli 46c lõike 1 kohaselt. Selline teade peab sisaldama artikli 5 lõikes 2 loetletud teavet.

4. Liikmesriik, kes saab lõike 3 kohaselt esitatud teabe, võtab ilma põhjendamatu viivituseta lõigetes 1 ja 2 sätestatud meetmed.

Artikkel 4

Kukrute pakkumise ja kasutamise peatamine ning muud parandusmeetmed

1. Liikmesriigid tagavad, et peatatud kukrulahenduse raames ei pakuta, kasutata ega aktiveerita kukrukomplekte.

2. Liikmesriigid hindavad, kas turvarikkumisele või kahjustamisele asjakohaselt reageerimiseks on vaja tunnistada kehtetuks kukrulahenduse peatamisest mõjutatud kukrukomplekti tõendid või võtta muid parandusmeetmeid.

3. Lõigetes 1 ja 2 sätestatud meetmed võetakse ilma põhjendamatu viivituseta ja igal juhul hiljemalt 24 tunni jooksul pärast turvarikkumisest või kahjustamisest mõjutatud kukrulahenduse pakkumise ja kasutamise peatamist.

4. Lõigetes 1 ja 2 sätestatud meetmed ei tohi takistada mõjutatud kukrukasutajatel määruse (EL) nr 910/2014 artikli 5a lõike 4 punktis g sätestatud andmete ülekantavuse õiguse kasutamist. See kehtib tingimusel, et kukrukasutajad võivad seda õigust kasutada, kui nad ei kahjusta mõjutatud kukrukomplektide kriitilise tähtsusega varade turvalisust, võttes eelkõige arvesse peatamise põhjuseid ja vajadust tagada nende varade tulemuslik kaitse väärkasutamise eest.

Artikkel 5

Teave peatamiste ja parandusmeetmete kohta

1. Põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul pärast kukrulahenduse pakkumise ja kasutamise peatamist esitatakse selge, põhjalik ja kergesti kättesaadav teave kukrulahenduse pakkumise ja kasutamise peatamise kohta:

a) määruse (EL) nr 910/2014 artikli 46c lõike 1 kohaselt määratud ühtsetele kontaktpunktidele;

b) komisjonile;

c) mõjutatud kukrukasutajatele;

d) kukrule tuginevatele isikutele, kes on registreeritud määruse (EL) nr 910/2014 artikli 5b kohaselt.

2. Lõike 1 kohaselt esitatav teave hõlmab vähemalt järgmist:

a) selle kukrulahenduse pakkuja nimi, mille pakkumine ja kasutamine on peatatud;

b) asjaomase kukrulahenduse nimi ja tunnus, nagu on märgitud määruse (EL) nr 910/2014 artikli 5d kohaselt koostatud sertifitseeritud kukrute loetelus, ja vajaduse korral versioonid, mida teade puudutab;

c) kuupäev ja kellaaeg, mil turvarikkumine või kahjustamine avastati;

d) kui see on teada, siis kuupäev ja kellaaeg, mil turvarikkumine või kahjustamine aset leidis, tuginedes võrgu- või süsteemilogidele või muudele andmeallikatele;

e) kukrulahenduse kehtivuse peatamise kuupäev ja kellaaeg;

f) kontaktandmed, sh vähemalt e-posti aadress ja telefoninumber teavitava liikmesriigi kohta ning punktis a osutatud kukruteenuse pakkuja e-posti aadress ja telefoninumber, kui need on erinevad;

g) turvarikkumise või kahjustamise kirjeldus;

h) ohtu sattunud andmete kirjeldus, sealhulgas määruse (EL) 2016/679 artikli 9 lõikes 1 ja artiklis 10 osutatud isikuandmete kategooriad, kui see on asjakohane;

i) võimaluse korral hinnang mõjutatud kukrukasutajate ja muude mõjutatud füüsiliste isikute ligikaudse arvu kohta;

j) kirjeldus võimalikust mõjust kukrule tuginevatele isikutele või kukrukasutajatele ning viimaste puhul vajaduse korral viited meetmetele, mida kukrukasutajad võivad võtta võimaliku mõju leevendamiseks;

k) turvarikkumise või kahjustamise kõrvaldamiseks võetud või kavandatud meetmete kirjeldus koos sellise kõrvaldamise kava ja tähtajaga;

l) kui see on asjakohane ja otstarbekas, siis nende meetmete kirjeldus, mis on võetud või kavandatud selleks, et korraldada mõjutatud kukrukasutajate üleminek alternatiivsetele kukrulahendustele või teenustele.

Artikkel 6

Kukrute pakkumise ja kasutamise taastamine

Kui see on vajalik kukrulahenduse taastamiseks, aktiveerimiseks ja kasutamiseks, teevad liikmesriigid ilma põhjendamatu viivituseta järgmist:

1) taastavad asjaomase kukrulahenduse raames pakutavate kukrukomplektide pakkumise ja kasutamise, väljastades kõigile mõjutatud kasutajatele kukrukomplekti, mida pakutakse kukrulahenduse uue versiooni alusel;

2) väljastavad uued kukrukomplekti tõendid uutele kukrukomplektidele või vajaduse korral varem väljastatud kukrukomplektidele, tingimusel et need vastavad pärast turvarikkumise või kahjustamise kõrvaldamist kehtivatele turvanõuetele;

3) tunnistavad kehtetuks kõik artikli 4 kohaselt rakendatud meetmed, mis takistavad uute kukrukomplektide pakkumist mõjutatud kukrulahenduse raames, kui see meede oli seotud üksnes nüüdseks kõrvaldatud turvarikkumise või kahjustamisega.

Artikkel 7

Teave taastamise kohta

Kui liikmesriik kukrulahenduse taastab, tagab ta järgmise:

1) sellekohane teave esitatakse põhjendamatu viivituseta kõigile isikutele, kes on saanud teavet kõnealuse kukrulahenduse pakkumise ja kasutamise peatamise kohta vastavalt artikli 5 lõikele 1;

2) punkti 1 kohaselt esitatud teave peab sisaldama vähemalt artikli 5 lõike 2 punktides a, b ja f–h osutatud elemente ning järgmist:

   a) kuupäev ja kellaaeg, mil turvarikkumine või kahjustamine kõrvaldati;

   b) mõjutatud kukrulahenduse taastamise kuupäev ja kellaaeg ning, kui see on asjakohane, selle kukrulahenduse raames pakutavate mõjutatud kukrukomplektide taastamise kuupäev ja kellaaeg;

   c) turvarikkumise või kahjustamise kõrvaldamiseks võetud meetmete kirjeldus;

   d) kirjeldus võimalikust jääkmõjust kukrule tuginevatele isikutele või kukrukasutajatele ning viimaste puhul vajaduse korral viited meetmetele, mida kukrukasutajad võivad võtta võimaliku jääkmõju leevendamiseks.

Artikkel 8

Kukrute kasutuselt kõrvaldamine

1. Kui turvarikkumist või kahjustamist, mis on põhjustanud kukrulahenduse pakkumise ja kasutamise peatamise, ei kõrvaldata kolme kuu jooksul pärast selle kukrulahenduse pakkumise ja kasutamise peatamise kuupäeva, tagab kukrulahendust pakkuv liikmesriik, et mõjutatud kukrulahendus kõrvaldatakse kasutuselt ja tunnistatakse kehtetuks, tehes seda ilma põhjendamatu viivituseta ning igal juhul 72 tunni jooksul pärast kolmekuulise tähtaja möödumist.

2. Kui liikmesriik kukrulahenduse kasutuselt kõrvaldab, tagab ta järgmise:

a) mõjutatud kukrulahenduse kukrukomplekti tõendid tunnistatakse kehtetuks;

b) kukrukomplekti tõendite kehtivust ei saa ennistada;

c) uut kukrukomplekti tõendit ei saa väljastada mõjutatud kukrulahenduse raames pakutavatele olemasolevatele kukrukomplektidele;

d) mõjutatud kukrulahenduse raames ei saa pakkuda uut kukrukomplekti.

3. Lõigetes 1 ja 2 sätestatud meetmed ei tohi takistada mõjutatud kukrukasutajatel kasutada määruse (EL) nr 910/2014 artikli 5a lõike 4 punktis g sätestatud andmete ülekantavuse õigust. See kehtib tingimusel, et kukrukasutajad võivad seda õigust kasutada, kui nad ei kahjusta mõjutatud kukrukomplektide kriitilise tähtsusega varade turvalisust, võttes eelkõige arvesse kasutuselt kõrvaldamise põhjuseid ja vajadust tagada nende varade tõhus kaitse väärkasutamise eest.

Artikkel 9

Teave kasutuselt kõrvaldamise kohta

1. Selge, terviklik ja kergesti kättesaadav teave kukrulahenduse kasutuselt kõrvaldamisest esitatakse põhjendamatu viivituseta ja hiljemalt 24 tunni jooksul pärast kukrulahenduse kasutuselt kõrvaldamist:

a) määruse (EL) nr 910/2014 artikli 46c lõike 1 kohaselt määratud ühtsetele kontaktpunktidele;

b) komisjonile;

c) mõjutatud kukrukasutajatele;

d) kukrule tuginevatele isikutele, kes on registreeritud määruse (EL) nr 910/2014 artikli 5b kohaselt.

2. Lõike 1 kohaselt esitatav teave hõlmab vähemalt järgmist:

a) kõrvaldatud kukrulahenduse pakkuja nimi;

b) asjaomase kukrulahenduse nimi ja tunnus, nagu on märgitud määruse (EL) nr 910/2014 artikli 5d kohaselt koostatud sertifitseeritud kukrute loetelus, ja vajaduse korral versioonid, mida teade puudutab;

c) sellise turvarikkumise või kahjustamise avastamise kuupäev ja kellaaeg, mis viis mõjutatud kukrulahenduse kasutuselt kõrvaldamiseni turvarikkumise või kahjustamise tõsiduse tõttu või põhjusel, et seda ei kõrvaldatud kolme kuu jooksul;

d) kui see on teada, siis kuupäev ja kellaaeg, mil turvarikkumine või kahjustamine aset leidis, tuginedes võrgu- või süsteemilogidele või muudele andmeallikatele;

e) kukrulahenduse kasutuselt kõrvaldamise kuupäev ja kellaaeg ning kukrulahenduse raames pakutud kukrukomplektide tõendite tegelik kehtetuks tunnistamine;

f) teave selle kohta, kas kasutuselt kõrvaldamine on tingitud turvarikkumise või kahjustamise tõsidusest või on kõrvaldamata jäetud turvarikkumise või kahjustamise tagajärg;

g) kontaktandmed, sh vähemalt e-posti aadress ja telefoninumber teavitava liikmesriigi kohta ning punktis a osutatud kukruteenuse pakkuja e-posti aadress ja telefoninumber, kui need on erinevad;

h) turvarikkumise või kahjustamise kirjeldus;

i) ohtu sattunud andmete kirjeldus, sealhulgas määruse (EL) 2016/679 artikli 9 lõikes 1 ja artiklis 10 nimetatud isikuandmete kategooriad, kui see on asjakohane;

j) võimaluse korral hinnang mõjutatud kukrukasutajate ja muude mõjutatud füüsiliste isikute ligikaudse arvu kohta;

k) kirjeldus võimalikust mõjust kukrule tuginevatele isikutele või kukrukasutajatele ning viimaste puhul vajaduse korral viited meetmetele, mida kukrukasutajad võivad võtta võimaliku mõju leevendamiseks;

l) nende meetmete kirjeldus, mis on võetud või kavandatud selleks, et korraldada mõjutatud kukrukasutajate üleminek alternatiivsetele kukrulahendustele või, kui see on asjakohane, alternatiivsetele teenustele.

Artikkel 10

Infosüsteem

Liikmesriigid saadavad artiklites 3, 5, 7 ja 9 sätestatud teabe komisjonile ja määruse (EL) nr 910/2014 artikli 46c lõike 1 kohaselt määratud liikmesriikide ühtsetele kontaktpunktidele ENISA hallatava küberintsidentidest teatamise ja nende analüüsi süsteemi või liikmesriikide ja komisjoni vahel kokku lepitud samaväärse süsteemi kaudu.

Artikkel 11

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides, välja arvatud artikkel 10, mida kohaldatakse alates 7. maist 2026.

Brüssel, 6. mai 2025

Komisjoni nimel
president
Ursula VON DER LEYEN

LISA

Turvarikkumise või kahjustamise hindamise kriteeriumid

1. Liikmesriigid võtavad turvarikkumise või kahjustamise hindamisel aluseks järgmised kriteeriumid.

a) Rikkumine või kahjustamine on põhjustanud või võib põhjustada füüsilise isiku surma või märkimisväärset kahju tema tervisele.

b) Edukas ning arvatavalt kuritahtlik või volitamata juurdepääs kukruteenuse pakkuja, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud valideerimismehhanismide pakkuja või kukrulahenduse pakkumist toetava e-identimise süsteemi pakkuja (edaspidi „asjaomased üksused“) võrgu- ja infosüsteemidele on toimunud või võib toimuda viisil, mis võib põhjustada tõsiseid talitlushäireid, ning need süsteemid on mõjutatud kukrulahenduse, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud mõjutatud valideerimismehhanismide või kukrulahenduse pakkumise aluseks oleva mõjutatud e-identimise süsteemi kriitilise tähtsusega komponendid.

c) Kukrulahendus, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud valideerimismehhanism või kukrulahenduse pakkumise aluseks olev e-identimise süsteem või nende osa:

— on kukrukasutajatele või kukrule tuginevatele isikutele enam kui 12 järjestikuse tunni jooksul täielikult kättesaamatu või prognoositavalt täielikult kättesaamatu;

— on kukrukasutajatele või kukrule tuginevatele isikutele kättesaamatu või prognoositavalt kättesaamatu rohkem kui 16 tunni vältel kalendrinädala kohta;

d) Kahtluste kohaselt on kukrulahenduse või sellega seotud asjaomaste üksuste pakutavate teenuste piiratud kättesaadavusel mõju või prognoositav mõju rohkem kui 1 % kukrukasutajatest või kukrule tuginevatest isikutest.

e) Olemas on võimalus kahjustada või on kahjustatud füüsilist juurdepääsu (mis on ainult asjaomaste üksuste usaldusväärsetel töötajatel) või sellise füüsilise juurdepääsu kaitset kukrulahendust toetavate võrgu- ja infosüsteemide, määruse (EL) nr 910/2014 artikli 5a lõikes 8 osutatud ja kukrulahendusega seotud valideerimismehhanismide või kukrulahenduse pakkumist toetavate e-identimise süsteemide ühes või mitmes asukohas.

f) Kukrulahenduses säilitatavate, edastatavate või töödeldavate andmete privaatsus, terviklus, konfidentsiaalsus või autentsus on kahjustatud või võib saada kahjustatud ühel või mitmel järgmisel viisil:

— see mõjutab rohkem kui 1 % mõjutatud kukrulahenduse kasutajatest või rohkem kui 100 000 neist kukrukasutajatest, olenevalt sellest, kumb arv on väiksem;

— see on eduka ning arvatavalt kuritahtliku tegevuse tulemus;

— see tuleneb või tõenäoliselt tuleneb ühest või mitmest teadaolevast nõrkusest, sealhulgas komisjoni rakendusmääruse (EL) 2024/2981 ([1]) kohaselt käideldavast nõrkusest;

— see mõjutab tõenäoliselt isikuandmeid viisil, mis võib ohustada asjaomaste füüsiliste isikute õigusi ja vabadusi, eelkõige määruse (EL) 2016/679 artikli 9 lõikes 1 ja artiklis 10 määratletud isikuandmetega seotud rikkumise korral;

([1]) Komisjoni 28. novembri 2024. aasta rakendusmäärus (EL) 2024/2981, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 rakenduseeskirjad seoses Euroopa digiidentiteedikukrute sertifitseerimisega (ELT L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— see mõjutab tõenäoliselt isiklikku elektroonilist sidet;

— sellest tuleneb tõenäoliselt suur risk füüsiliste isikute õigustele ja vabadustele;

— see mõjutab tõenäoliselt haavatavaid füüsilisi isikuid;

g) Kukrulahenduse sertifitseerimine on tühistatud või eeldatavasti tühistatakse.

h) Rikkumine või kahjustamine on põhjustanud või võib põhjustada asjaomasele üksusele otsest rahalist kahju, mis on suurem kui 500 000 eurot või, kui see on asjakohane, 5 % asjaomase üksuse aastasest kogukäibest eelmisel majandusaastal olenevalt sellest, kumb summa on väiksem.

2. Liikmesriigid ei võta arvesse asjaomaste üksuste poolt või nende nimel tehtava hooldustöö kavakohaseid tagajärgi, tingimusel et:

a) sellisest hooldustööst on eelnevalt teatatud potentsiaalselt mõjutatud kukrukasutajatele, kukrule tuginevatele isikutele ja asjaomastele pädevatele järelevalveasutustele;

b) hooldustöö ei vasta ühelegi käesoleva lisa punktis 1 sätestatud kriteeriumile.

3. Lõike 1 punkti c puhul mõõdetakse kättesaadavust mõjutava intsidendi kestust alates sellest, kui mõjutatud teenuse nõuetekohane osutamine katkeb, kuni selleni, kui teenus taastatakse ja uuesti toimib. Kui asjaomane üksus ei suuda kindlaks teha teenuse katkemise hetke, mõõdetakse intsidendi kestust alates intsidendi avastamise hetkest või hetkest, mil võrgu või süsteemi logidesse või muudesse andmeallikatesse tekib intsidendi kohta kanne, olenevalt sellest, kumb leidis aset varem. Teenuse täielikku käideldamatust mõõdetakse alates hetkest, mil teenus on kasutaja jaoks täiesti käideldamatu, kuni hetkeni, mil tavapärane tegevus või töö on enne intsidenti pakutud teenuse tasemel taastatud. Kui asjaomane üksus ei suuda kindlaks teha, millal teenuse täielik käideldamatus algas, mõõdetakse käideldamatust alates hetkest, mil kõnealune üksus selle avastas.

4. Lõike 1 punkti d puhul loetakse teenuse kättesaadavus piiratuks eelkõige siis, kui teenus on keskmisest reageerimisajast märkimisväärselt aeglasem või kui kõik teenuse funktsioonid ei ole kättesaadavad. Reageerimisajas esinevate viivituste hindamiseks tuleb võimaluse korral kasutada objektiivseid kriteeriume, mis põhinevad osutatud teenuste keskmistel reageerimisaegadel.

5. Selleks et teha kindlaks otseselt lõike 1 punktis h osutatud rikkumisest või kahjustamisest tulenev rahaline kahju, peaksid asjaomased üksused arvesse võtma kogu rahalist kahju, mis neil intsidendi tulemusena tekkis, näiteks tarkvara, riistvara või taristu asendamise või teisaldamise kulusid, personalikulusid, kaasa arvatud kulusid, mis on seotud töötajate asendamise või ümberpaigutamise, lisatöötajate värbamise, ületunnitöö tasustamise ning kaotatud või vähenenud oskuste taastamisega, tasusid, mis tuleb maksta tulenevalt lepinguliste kohustuste täitmata jätmisest, kahju heastamise ja klientidele hüvitamise kulusid, saamata jäänud tulust tulenevat kahju, sise- ja välissuhtlusega seotud kulusid ning nõustamiskulusid, sealhulgas õigusnõustamise, kohtuekspertiisi ja parandusteenustega seotud kulusid. Intsidendist tuleneva rahalise kahjuna ei käsitata igapäevase äritegevuse toimimiseks vajaminevaid kulusid, nagu kulutused taristu, seadmete, riistvara ja tarkvara üldisele hooldusele, täiustustele, riskihindamistele ning kindlustusmaksetele. Asjaomased üksused arvutavad finantskahju summad kättesaadavate andmete põhjal ja kui finantskahju tegelikke summasid ei ole võimalik kindlaks teha, siis annavad need üksused oma hinnangu, millised need summad võiksid olla.