Euroopan unionin
virallinen lehti

FI
L-sarja

2025/847

7.5.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/847,

annettu 6 päivänä toukokuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden tietoturvaloukkauksiin reagoinnin osalta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 23 päivänä heinäkuuta 2014 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) ja erityisesti sen 5 e artiklan 5 kohdan,

sekä katsoo seuraavaa:

(1) Asetuksella (EU) N:o 910/2014 perustettu eurooppalainen digitaalisen identiteetin kehys, jäljempänä 'kehys', on keskeinen osa turvallisen ja yhteentoimivan digitaalisen identiteetin ekosysteemin luomista kaikkialla unionissa. Kehyksen kulmakivenä ovat eurooppalaiset digitaalisen identiteetin lompakot, jäljempänä 'lompakot', ja sen tavoitteena on helpottaa palvelujen saatavuutta kaikissa jäsenvaltioissa ja varmistaa samalla henkilötietojen ja yksityisyyden suoja.

(2) Tämän asetuksen mukaisiin henkilötietojen käsittelytoimiin sovelletaan Euroopan parlamentin ja neuvoston asetuksia (EU) 2016/679 ([2]) ja (EU) 2018/1725 ([3]), ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY ([4]). Tässä asetuksessa vahvistetut arviointia ja tietojen antamista koskevat säännöt eivät vaikuta velvollisuuteen ilmoittaa henkilötietojen tietoturvaloukkauksista toimivaltaiselle valvontaviranomaiselle tapauksen mukaan asetuksen (EU) 2016/679 tai asetuksen (EU) 2018/1725 nojalla eikä velvollisuuteen ilmoittaa henkilötietojen tietoturvaloukkauksista tarvittaessa rekisteröidyille mainittujen asetusten nojalla.

(3) Komissio arvioi säännöllisesti uusia teknologioita, käytäntöjä, standardeja ja teknisiä eritelmiä. Jotta lompakoiden kehittämisessä ja sertifioinnissa voidaan varmistaa mahdollisimman suuri yhdenmukaistaminen jäsenvaltioiden kesken, tässä asetuksessa vahvistetut tekniset eritelmät perustuvat työhön, jota on tehty komission suosituksen (EU) 2021/946 ([5]) nojalla, ja erityisesti siihen kuuluvaan arkkitehtuuriin ja viitekehykseen. Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1183 ([6]) johdanto-osan 75 kappaleen mukaan komission olisi tarkasteltava uudelleen ja tarvittaessa päivitettävä tätä asetusta sen pitämiseksi maailmanlaajuisen kehityksen ja arkkitehtuurin ja viitekehyksen mukaisena sekä sisämarkkinoiden parhaiden käytäntöjen noudattamiseksi.

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

([2]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Komission suositus (EU) 2021/946, annettu 3 päivänä kesäkuuta 2021, unionin yhteisestä välineistöstä eurooppalaista digitaalisen identiteetin kehystä koskevaa koordinoitua lähestymistapaa varten (EUVL L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183, annettu 11 päivänä huhtikuuta 2024, asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta (EUVL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Jos lompakkoratkaisuihin tai asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettuihin validointimekanismeihin tai sähköisen tunnistamisen järjestelmään, jonka puitteissa lompakkoratkaisuja tarjotaan, kohdistuu tietoturvaloukkaus tai niiden turvallisuus vaarantuu, tällaisiin tietoturvaloukkauksiin ja turvallisuuden vaarantumisiin olisi reagoitava nopealla, koordinoidulla ja turvatulla tavalla kaikissa jäsenvaltioissa käyttäjien suojelemiseksi ja luottamuksen säilyttämiseksi digitaalisen identiteetin ekosysteemiin. Tämä ei rajoita Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2555 ([7]), Euroopan parlamentin ja neuvoston asetusten (EU) 2019/881 ([8]) ja (EU) 2024/2847 ([9]) soveltamista, etenkään siltä osin kun on kyse poikkeamien tai haavoittuvuuksien käsittelystä ja niiden huomioon ottamisesta tietoturvaloukkauksina. Sen vuoksi jäsenvaltioiden olisi varmistettava, että lompakoiden, joihin kohdistuu tietoturvaloukkaus tai joiden turvallisuus on vaarantunut, tarjoaminen ja käyttö keskeytetään viipymättä tai ne poistetaan tarvittaessa käytöstä.

(5) Sen varmistamiseksi, että tietoturvaloukkaukseen tai turvallisuuden vaarantumiseen reagoidaan asianmukaisesti, jäsenvaltioiden olisi arvioitava, vaikuttaako lompakkoratkaisun, asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettujen validointimekanismien tai sähköisen tunnistamisen järjestelmän, jonka puitteissa lompakkoratkaisua tarjotaan, tietoturvaloukkaus tai turvallisuuden vaarantuminen kyseisen lompakkoratkaisun tai muiden lompakkoratkaisujen luotettavuuteen. Tällaisen arvioinnin olisi perustuttava yhdenmukaisiin kriteereihin, kuten niiden lompakon käyttäjien, luonnollisten henkilöiden ja lompakkoon luottavien osapuolten määrään ja luokkaan, joihin vaikutus kohdistuu, niiden tietojen luonteeseen, joihin vaikutus kohdistuu, turvallisuuden vaarantumisen tai tietoturvaloukkauksen kestoon, palvelun rajalliseen saatavuuteen ja taloudellisiin menetyksiin sekä henkilötietojen mahdolliseen vaarantumiseen. Näiden kriteerien olisi jätettävä jäsenvaltioille joustovaraa ja harkintavaltaa, jotta ne voivat määrittää oikeasuhteisella tavalla, onko lompakkoratkaisun luotettavuus vaarantunut ja onko tarkoituksenmukaista keskeyttää lompakkoratkaisun käyttö tai poistaa se käytöstä, jos se on tietoturvaloukkauksen tai turvallisuuden vaarantumisen vakavuuden vuoksi perusteltua. Näiden kriteerien ei pitäisi automaattisesti johtaa lompakkoratkaisun käytöstä poistamiseen tai sen tarjonnan ja käytön keskeyttämiseen, vaan jäsenvaltioiden olisi punnittava kriteerejä huolellisesti päättäessään, onko aiheellista poistaa lompakkoratkaisu käytöstä tai keskeyttää sen tarjonta ja käyttö.

(6) Lompakkoratkaisujen käytön keskeyttämisestä aiheutuvien vaikutusten ja hankaluuksien vuoksi jäsenvaltioiden olisi arvioitava, ovatko lompakkoyksikkötodistusten peruuttaminen tai jotkin muut lisätoimenpiteet tarpeen, jotta tietoturvaloukkaukseen tai turvallisuuden vaarantumiseen voidaan reagoida riittävällä tavalla.

(7) Jotta lompakon käyttäjät olisivat tietoisia lompakoidensa tilasta, heille olisi annettava riittävästi tietoa heidän lompakkoihinsa vaikuttavista tietoturvaloukkauksista tai turvallisuuden vaarantumisista. Koska tietoturvaloukkaukset ja turvallisuuden vaarantumiset voivat vaikuttaa myös unionissa rekisteröityihin lompakkoon luottaviin osapuoliin, myös niille olisi jaettava asiaankuuluvat tiedot tietoturvaloukkauksista ja turvallisuuden vaarantumisista.

(8) Avoimuuden parantamiseksi ja luottamuksen lisäämiseksi digitaalisen identiteetin ekosysteemiin tietoturvaloukkauksista tai turvallisuuden vaarantumisista ja niiden seurauksista annettaviin tietoihin olisi sisällyttävä ainakin tämän asetuksen nojalla vaaditut tiedot. Lompakon käyttäjille ja lompakkoon luottaville osapuolille tietoturvaloukkauksista tai turvallisuuden vaarantumisista jaettuja tietoja olisi kuitenkin arvioitava huolellisesti, jotta ehkäistään ja minimoidaan riski siitä, että hyökkääjät hyödyntävät niitä.

([7]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös) (EUVL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Jotta käyttäjät voisivat käyttää lompakkoyksikköjään uudelleen sen jälkeen, kun tietoturvaloukkaus tai turvallisuuden vaarantuminen on korjattu, lompakkoratkaisuja tarjonneen jäsenvaltion olisi aloitettava uudelleen kyseisten lompakkoratkaisujen tarjoaminen ja käyttö ilman aiheetonta viivytystä. Tämä voidaan tehdä ottamalla lompakkoyksiköt uudelleen käyttöön, myöntämällä lompakkoyksikköjä lompakkoratkaisun uuden version mukaisesti tai antamalla uusia voimassa olevia lompakkoyksikkötodistuksia. Asiasta olisi ilmoitettava vaikutuksen kohteena oleville lompakon käyttäjille, lompakkoon luottaville osapuolille, asetuksen (EU) N:o 910/2014 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille ja komissiolle.

(10) Jotta voidaan varmistaa lompakoiden poistaminen käytöstä, jos tietoturvaloukkausta tai turvallisuuden vaarantumista ei ole korjattu kolmen kuukauden kuluessa käytön keskeyttämisestä tai jos tämä on perusteltua tietoturvaloukkauksen tai turvallisuuden vaarantumisen vakavuuden vuoksi, jäsenvaltion olisi varmistettava, että asiaankuuluvat lompakkoyksikkötodistukset peruutetaan ja että niitä ei voida palauttaa voimassa olevaan tilaan eikä niitä voida myöntää tai tarjota olemassa oleville lompakkoyksiköille. Kyseisen lompakkoratkaisun puitteissa ei myöskään pitäisi tarjota uusia lompakkoyksiköitä. Avoimuuden vuoksi käytöstä poistamisesta olisi ilmoitettava käyttäjille, lompakkoon luottaville osapuolille, asetuksen (EU) N:o 910/2014 46 c artiklan 1 kohdan mukaisesti nimetyille keskitetyille yhteyspisteille ja komissiolle. Ilmoitukseen olisi sisällyttävä kuvaus mahdollisista vaikutuksista lompakon käyttäjiin ja erityisesti myönnettyjen todistusten hallinnointiin tai lompakkoon luottaviin osapuoliin.

(11) Lompakkoratkaisun tarjonnan ja käytön keskeyttämistä seuraavan kolmen kuukauden ajanjakson, jonka aikana keskeyttämiseen johtanut tietoturvaloukkaus tai turvallisuuden vaarantuminen on korjattava, olisi muodostettava määräaika, jonka jälkeen lompakkoratkaisu olisi poistettava käytöstä, ellei asianmukaista korjaustoimenpidettä ole toteutettu. Jäsenvaltiot voivat kuitenkin vapaasti vaatia, että tietoturvaloukkaus tai turvallisuuden vaarantuminen korjataan kolmea kuukautta lyhyemmässä määräajassa, ottaen erityisesti ja tarvittaessa huomioon kyseisen tietoturvaloukkauksen tai turvallisuuden vaarantumisen laajuus, kesto ja seuraukset. Jos tietoturvaloukkausta tai turvallisuuden vaarantumista ei korjata tai ei voida korjata jäsenvaltion asettamassa määräajassa, jäsenvaltio voi vaatia, että lompakkoratkaisu poistetaan käytöstä ennen kolmen kuukauden määräajan päättymistä. Jäsenvaltioiden olisi käytettävä tätä ajanjaksoa, jonka aikana tietoturvaloukkaus tai turvallisuuden vaarantuminen, joka johti lompakkoratkaisun tarjonnan ja käytön keskeyttämiseen, on korjattava, kyseisen lompakkoratkaisun mahdollisen käytöstä poistamisen ja siitä johtuvaa viestinnän valmisteluun.

(12) Jotta voidaan vähentää hallinnollista taakkaa, joka jäsenvaltioille aiheutuu tämän asetuksen mukaisesti komissiolle ja muille jäsenvaltioille annettavista tiedoista, jäsenvaltioiden olisi käytettävä olemassa olevia ilmoitusvälineitä, kuten Euroopan unionin kyberturvallisuusviraston (ENISA) ylläpitämää kyberpoikkeamien raportointi- ja analysointijärjestelmää (CIRAS). Lompakon käyttäjille, joihin tietoturvaloukkaus tai turvallisuuden vaarantuminen vaikuttaa, ja lompakkoon luottaville osapuolille tiedottamiseen käytettävien vaihtoehtoisten kanavien tai keinojen osalta jäsenvaltioiden olisi varmistettava, että asiaankuuluvat tiedot annetaan selkeällä, kattavalla ja helposti saatavilla olevalla tavalla. Kanaviin, joilla tällaisia tietoja annetaan asianomaisille lompakon käyttäjille ja lompakkoon luottaville osapuolille, olisi sisällyttävä asianmukaisia ratkaisuja verkkosivustopohjaista tiedottamista, verkkosivustojen päivitysten reaaliaikaista seurantaa ja uutiskoostepalveluja varten.

(13) Euroopan tietosuojavaltuutettua on kuultu asetuksen (EU) 2018/1725 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 31 päivänä tammikuuta 2025.

(14) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) N:o 910/2014 48 artiklalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Kohde

Tässä asetuksessa vahvistetaan säännöt reagoimisesta tietoturvaloukkauksiin, jotka kohdistuvat lompakoihin, asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettuihin validointimekanismeihin sekä sähköisen tunnistamisen järjestelmään, jonka puitteissa lompakoita tarjotaan.

2 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) ’lompakkoratkaisulla’ ohjelmistojen, laitteiden, palvelujen, asetusten ja konfiguraatioiden yhdistelmää, mukaan lukien lompakon ilmentymät, yksi tai useampi lompakon suojattu salaussovellus ja yksi tai useampi lompakon suojattu salauslaite;

2) ’lompakon käyttäjällä’ käyttäjää, jonka hallinnassa lompakkoyksikkö on;

3) ’lompakkoon luottavalla osapuolella’ luottavaa osapuolta, joka aikoo luottaa lompakkoyksikköihin julkisten tai yksityisten palvelujen tarjoamiseksi digitaalisen vuorovaikutuksen avulla;

4) ’lompakon ilmentymällä’ sovellusta, joka on asennettu ja konfiguroitu lompakon käyttäjän laitteeseen tai ympäristöön ja on osa lompakkoyksikköä ja jota lompakon käyttäjä käyttää ollakseen vuorovaikutuksessa lompakkoyksikön kanssa;

5) ’lompakon suojatulla salaussovelluksella’ sovellusta, joka hallitsee kriittisiä resursseja linkittymällä lompakon suojatun salauslaitteen tarjoamiin salausteknisiin ja muihin toimintoihin ja käyttämällä näitä toimintoja;

6) ’lompakon suojatulla salauslaitteella’ väärinkäytöltä suojattua laitetta, joka tarjoaa lompakon suojattuun salaussovellukseen liitetyn ja sen käyttämän ympäristön kriittisten resurssien suojaamiseksi ja salaustoimintojen tarjoamiseksi kriittisten toimintojen turvallista suorittamista varten;

7) ’lompakon tarjoajalla’ lompakkoratkaisuja tarjoavaa luonnollista henkilöä tai oikeushenkilöä;

8) ’lompakkoyksiköllä’ lompakkoratkaisun ainutlaatuista konfiguraatiota, johon kuuluvat lompakon ilmentymät, lompakon suojatut salaussovellukset ja lompakon suojatut salauslaitteet ja jonka lompakon tarjoaja tarjoaa yksittäiselle lompakon käyttäjälle;

9) ’kriittisillä resursseilla’ lompakkoyksikössä olevia tai siihen liittyviä resursseja, jotka ovat niin merkittäviä, että niiden saatavuuden, luottamuksellisuuden tai eheyden vaarantuminen erittäin vakavasti heikentäisi kykyä luottaa lompakkoyksikköön;

10) ’lompakkoyksikkötodistuksella’ dataobjektia, jossa kuvataan lompakkoyksikön komponentit tai joka mahdollistaa näiden komponenttien todentamisen ja validoinnin.

3 artikla

Tietoturvaloukkauksen tai turvallisuuden vaarantumisen toteaminen

1. Jäsenvaltioiden on otettava asianmukaisesti huomioon liitteessä I vahvistetut kriteerit arvioidakseen, vaikuttaako lompakkoratkaisun, asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettujen validointimekanismien tai sähköisen tunnistamisen järjestelmän, jonka puitteissa lompakkoratkaisua tarjotaan, tietoturvaloukkaus tai turvallisuuden vaarantuminen niiden luotettavuuteen tai muiden lompakkoratkaisujen luotettavuuteen, sanotun kuitenkaan rajoittamatta direktiivin (EU) 2022/2555 ja asetusten (EU) 2019/881 ja (EU) 2024/2847 soveltamista.

2. Jos jäsenvaltio toteaa 1 kohdassa säädetyn arvioinnin perusteella, että tietoturvaloukkaus tai turvallisuuden vaarantuminen vaikuttaa lompakkoratkaisun luotettavuuteen, ja keskeyttää kyseisen lompakkoratkaisun tarjoamisen ja käytön, kyseisen jäsenvaltion on toteutettava 4 ja 5 artiklassa säädetyt toimenpiteet. Jos jäsenvaltio poistaa lompakkoratkaisun käytöstä, sen on toteutettava 8 ja 9 artiklassa säädetyt toimenpiteet.

3. Jos jäsenvaltio saa tietoonsa mahdollisen tietoturvaloukkauksen tai turvallisuuden vaarantumisen, joka saattaa vaikuttaa jonkin toisen jäsenvaltion tarjoaman yhden tai useamman lompakkoratkaisun luotettavuuteen, kyseisen jäsenvaltion on ilman aiheetonta viivytystä tiedotettava tästä komissiolle ja asetuksen (EU) N:o 910/2014 46 c artiklan 1 kohdan mukaisesti nimetyille asianomaisten jäsenvaltioiden keskitetyille yhteyspisteille. Tiedonannon on sisällettävä 5 artiklan 2 kohdassa esitetyt tiedot.

4. Jäsenvaltion, joka vastaanottaa 3 kohdan nojalla toimitetut tiedot, on toteutettava 1 ja 2 kohdassa säädetyt toimenpiteet ilman aiheetonta viivytystä.

4 artikla

Lompakoiden tarjoamisen ja käytön keskeyttäminen ja muut korjaavat toimenpiteet

1. Jäsenvaltioiden on varmistettava, ettei lompakkoyksiköitä tarjota, käytetä tai aktivoida sellaisen lompakkoratkaisun puitteissa, jonka käyttö on keskeytetty.

2. Jäsenvaltioiden on arvioitava, onko lompakkoyksikkötodistusten peruuttaminen lompakkoyksiköiltä, joihin lompakkoratkaisun käytön keskeyttäminen vaikuttaa, tai jokin muu korjaava toimenpide tarpeen, jotta tietoturvaloukkaukseen tai turvallisuuden vaarantumiseen voidaan reagoida riittävällä tavalla.

3. Edellä 1 ja 2 kohdassa säädetyt toimenpiteet on toteutettava ilman aiheetonta viivytystä ja joka tapauksessa viimeistään 24 tunnin kuluttua sen lompakkoratkaisun tarjonnan tai käytön keskeyttämisestä, johon tietoturvaloukkaus tai turvallisuuden vaarantuminen vaikuttaa.

4. Edellä 1 ja 2 kohdassa säädetyt toimenpiteet eivät saa estää asianomaisia lompakon käyttäjiä käyttämästä asetuksen (EU) N:o 910/2014 5 a artiklan 4 kohdan g alakohdassa tarkoitettua oikeutta tietojen siirtoon. Tämä edellyttää, että lompakon käyttäjät voivat käyttää tätä oikeutta heikentämättä asianomaisten lompakkoyksiköiden kriittisten resurssien turvallisuutta, erityisesti kun otetaan huomioon keskeyttämisen syyt ja tarve varmistaa kyseisten resurssien tehokas suojaaminen väärinkäytöksiltä.

5 artikla

Keskeyttämisiä ja korjaavia toimenpiteitä koskevat tiedot

1. Lompakkoratkaisun tarjoamisen ja käytön keskeyttämisestä on tiedotettava seuraaville tahoille selkeällä, kattavalla ja helposti saatavilla olevalla tavalla, ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluttua lompakkoratkaisun tarjoamisen ja käytön keskeyttämisestä:

a) asetuksen (EU) N:o 910/2014 46 c artiklan 1 kohdan mukaisesti nimetyt keskitetyt yhteyspisteet;

b) komissio;

c) lompakon käyttäjät, joihin asia vaikuttaa;

d) asetuksen (EU) N:o 910/2014 5 b artiklan mukaisesti rekisteröidyt lompakkoon luottavat osapuolet.

2. Tämän artiklan 1 kohdan mukaisesti annettuihin tietoihin on sisällyttävä vähintään seuraavat:

a) sen lompakkoratkaisun tarjoajan nimi, jonka lompakkoratkaisun tarjoaminen ja käyttö on keskeytetty;

b) kyseisen lompakkoratkaisun nimi ja viitetunniste, sellaisena kuin ne on ilmoitettu asetuksen (EU) N:o 910/2014 5 d artiklan nojalla laaditussa sertifioitujen lompakoiden luettelossa, ja tarvittaessa asianomaiset versiot;

c) päivämäärä ja kellonaika, jolloin tietoturvaloukkaus tai turvallisuuden vaarantuminen havaittiin;

d) jos tiedossa, päivämäärä ja kellonaika, jolloin tietoturvaloukkauksen tai turvallisuuden vaarantumisen vaikutus alkoi, verkon tai järjestelmän lokitietojen tai muiden tietolähteiden perusteella;

e) lompakkoratkaisun käytön keskeyttämisen päivämäärä ja kellonaika;

f) yhteystiedot, mukaan lukien vähintään sähköpostiosoite ja puhelinnumero ilmoittavalle jäsenvaltiolle, ja jos se ei ole sama, a alakohdassa tarkoitetulle lompakon tarjoajalle;

g) kuvaus tietoturvaloukkauksesta tai turvallisuuden vaarantumisesta;

h) kuvaus vaarantuneista tiedoista, mukaan lukien tarvittaessa asetuksen (EU) 2016/679 9 artiklan 1 kohdassa ja 10 artiklassa määritellyt henkilötietoryhmät;

i) mahdollisuuksien mukaan arvio niiden lompakon käyttäjien ja muiden luonnollisten henkilöiden lukumäärästä, joihin asia vaikuttaa;

j) kuvaus mahdollisista vaikutuksista lompakkoon luottaviin osapuoliin tai lompakon käyttäjiin, ja jälkimmäisessä tapauksessa tarvittaessa tiedot toimenpiteistä, joita lompakon käyttäjät voivat toteuttaa näiden mahdollisten vaikutusten lieventämiseksi;

k) kuvaus tietoturvaloukkauksen tai turvallisuuden vaarantumisen korjaamiseksi toteutetuista tai suunnitelluista toimenpiteistä sekä tällaisen korjaavien toimenpiteiden suunnittelu ja määräaika;

l) jos mahdollista ja asianmukaista, kuvaus toteutetuista tai suunnitelluista toimenpiteistä niiden lompakon käyttäjien, joihin vaikutukset kohdistuvat, siirtämiseksi vaihtoehtoisiin lompakkoratkaisuihin tai -palveluihin.

6 artikla

Lompakoiden tarjoamisen ja käytön aloittaminen uudelleen

Jos se on tarpeen lompakkoratkaisun tarjoamisen, aktivoinnin ja käytön uudelleen aloittamisen varmistamiseksi, jäsenvaltioiden on ilman aiheetonta viivytystä

1) aloitettava uudelleen kyseisen lompakkoratkaisun puitteissa tarjottujen lompakkoyksiköiden tarjoaminen ja käyttö myöntämällä lompakkoratkaisun uuden version puitteissa tarjottu lompakkoyksikkö kaikille käyttäjille, joita asia koskee;

2) myönnettävä uusia lompakkoyksikkötodistuksia uusille lompakkoyksiköille tai tapauksen mukaan aiemmin myönnetyille lompakkoyksiköille edellyttäen, että kyseiset lompakkoyksiköt täyttävät tietoturvavaatimukset, jotka ovat voimassa sen jälkeen, kun tietoturvaloukkaus tai turvallisuuden vaarantuminen on korjattu;

3) kumottava kaikki 4 artiklan nojalla toteutetut toimenpiteet, jotka estävät uusien lompakkoyksikköjen tarjoamisen asianomaisen lompakkoratkaisun puitteissa, jos kyseinen toimenpide liittyi yksinomaan nyt korjattuun tietoturvaloukkaukseen tai turvallisuuden vaarantumiseen.

7 artikla

Uudelleen käyttöön ottamista koskevat tiedot

Jos jäsenvaltio ottaa lompakkoratkaisun uudelleen käyttöön, sen on varmistettava, että

1) tieto tästä annetaan ilman aiheetonta viivytystä kaikille osapuolille, jotka ovat saaneet tiedon kyseisen lompakkoratkaisun tarjoamisen ja käytön keskeyttämisestä 5 artiklan 1 mukaisesti.

2) Tämän artiklan 1 kohdan mukaisesti annettujen tietojen on sisällettävä vähintään 5 artiklan 2 kohdan a, b ja f–h alakohdassa tarkoitetut tiedot sekä seuraavat tiedot:

   a) päivämäärä ja kellonaika, jolloin tietoturvaloukkaus tai turvallisuuden vaarantuminen korjattiin;

   b) päivämäärä ja kellonaika, jolloin kyseinen lompakkoratkaisu ja tarvittaessa kyseisen lompakkoratkaisun puitteissa tarjotut lompakkoyksiköt, joihin vaikutus kohdistui, otettiin uudelleen käyttöön;

   c) kuvaus tietoturvaloukkauksen tai turvallisuuden vaarantumisen korjaamiseksi toteutetuista toimenpiteistä;

   d) kuvaus mahdollisista jäännösvaikutuksista lompakkoon luottaviin osapuoliin tai lompakon käyttäjiin, ja jälkimmäisessä tapauksessa tarvittaessa tiedot toimenpiteistä, joita lompakon käyttäjät voivat toteuttaa näiden mahdollisten jäännösvaikutusten lieventämiseksi.

8 artikla

Lompakoiden poistaminen käytöstä

1. Jos lompakkoratkaisun tarjonnan ja käytön keskeyttämiseen johtanutta tietoturvaloukkausta tai turvallisuuden vaarantumista ei ole korjattu kolmen kuukauden kuluessa päivästä, jona kyseisen lompakkoratkaisun tarjoaminen ja käyttö on keskeytetty, kyseistä lompakkoratkaisua tarjoavan jäsenvaltion on varmistettava, että kyseinen lompakkoratkaisu poistetaan käytöstä ja sen voimassaolo peruutetaan ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa kolmen kuukauden määräajan päättymisestä.

2. Kun jäsenvaltio poistaa lompakkoratkaisun käytöstä, sen on varmistettava, että

a) asianomaisen lompakkoratkaisun lompakkoyksiköiden lompakkoyksikkötodistukset peruutetaan;

b) lompakkoyksikkötodistukset eivät voi palautua voimassa olevaan tilaan;

c) uutta lompakkoyksikkötodistusta ei voida myöntää asianomaisen lompakkoratkaisun puitteissa tarjotuille olemassa oleville lompakkoyksiköille;

d) asianomaisen lompakkoratkaisun puitteissa ei voida tarjota uusia lompakkoyksiköitä.

3. Edellä 1 ja 2 kohdassa säädetyt toimenpiteet eivät saa estää asianomaisia lompakon käyttäjiä käyttämästä asetuksen (EU) N:o 910/2014 5 a artiklan 4 kohdan g alakohdassa tarkoitettua oikeutta tietojen siirtoon. Tämä edellyttää, että lompakon käyttäjät voivat käyttää tätä oikeutta heikentämättä asianomaisten lompakkoyksiköiden kriittisten resurssien turvallisuutta, erityisesti kun otetaan huomioon käytöstä poistamisen syyt ja tarve varmistaa kyseisten resurssien tehokas suojaaminen väärinkäytöksiltä.

9 artikla

Käytöstä poistamista koskevat tiedot

1. Lompakkoratkaisun käytöstä poistamisesta on tiedotettava seuraaville tahoille selkeällä, kattavalla ja helposti saatavilla olevalla tavalla, ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluttua lompakkoratkaisun käytöstä poistamisesta:

a) asetuksen (EU) N:o 910/2014 46 c artiklan 1 kohdan mukaisesti nimetyt keskitetyt yhteyspisteet;

b) komissio;

c) lompakon käyttäjät, joihin asia vaikuttaa;

d) asetuksen (EU) N:o 910/2014 5 b artiklan mukaisesti rekisteröidyt lompakkoon luottavat osapuolet.

2. Tämän artiklan 1 kohdan mukaisesti annettuihin tietoihin on sisällyttävä vähintään seuraavat:

a) sen lompakkoratkaisun tarjoajan nimi, jonka lompakkoratkaisu on poistettu käytöstä;

b) kyseisen lompakkoratkaisun nimi ja viitetunniste, sellaisena kuin ne on ilmoitettu asetuksen (EU) N:o 910/2014 5 d artiklan nojalla laaditussa sertifioitujen lompakoiden luettelossa, ja tarvittaessa asianomaiset versiot;

c) päivämäärä ja kellonaika, jolloin havaittiin tietoturvaloukkaus tai turvallisuuden vaarantuminen, joka johti kyseisen lompakkoratkaisun käytöstä poistamiseen tietoturvaloukkauksen tai vaarantumisen vakavuuden vuoksi tai siksi, että sitä ei oltu korjattu kolmen kuukauden kuluessa;

d) jos tiedossa, päivämäärä ja kellonaika, jolloin tietoturvaloukkauksen tai turvallisuuden vaarantumisen vaikutus alkoi, verkon tai järjestelmän lokitietojen tai muiden tietolähteiden perusteella;

e) lompakkoratkaisun käytöstä poistamisen ja lompakkoratkaisun puitteissa tarjottujen lompakkoyksikköjen lompakkoyksikkötodistusten tosiasiallisen peruuttamisen päivämäärä ja kellonaika;

f) johtuuko käytöstä poistaminen tietoturvaloukkauksen tai turvallisuuden vaarantumisen vakavuudesta vai siitä, että tietoturvaloukkausta tai turvallisuuden vaarantumista ei ole korjattu;

g) yhteystiedot, mukaan lukien vähintään sähköpostiosoite ja puhelinnumero ilmoittavalle jäsenvaltiolle, ja jos se ei ole sama, a alakohdassa tarkoitetulle lompakon tarjoajalle;

h) kuvaus tietoturvaloukkauksesta tai turvallisuuden vaarantumisesta;

i) kuvaus vaarantuneista tiedoista, mukaan lukien tarvittaessa asetuksen (EU) 2016/679 9 artiklan 1 kohdassa ja 10 artiklassa määritellyt henkilötietoryhmät;

j) mahdollisuuksien mukaan arvio niiden lompakon käyttäjien ja muiden luonnollisten henkilöiden lukumäärästä, joihin asia vaikuttaa;

k) kuvaus mahdollisista vaikutuksista lompakkoon luottaviin osapuoliin tai lompakon käyttäjiin, ja jälkimmäisessä tapauksessa tarvittaessa tiedot toimenpiteistä, joita lompakon käyttäjät voivat toteuttaa näiden mahdollisten vaikutusten lieventämiseksi;

l) kuvaus toteutetuista tai suunnitelluista toimenpiteistä niiden lompakon käyttäjien, joihin vaikutukset kohdistuvat, siirtämiseksi vaihtoehtoisiin lompakkoratkaisuihin tai, jos se on mahdollista ja asianmukaista, vaihtoehtoisiin palveluihin.

10 artikla

Tietojärjestelmä

Jäsenvaltioiden on lähetettävä 3, 5, 7 ja 9 artiklassa tarkoitetut tiedot komissiolle ja asetuksen (EU) N:o 910/2014 46 c artiklan 1 kohdan mukaisesti nimetyille jäsenvaltioiden keskitetyille yhteyspisteille ENISAn ylläpitämän CIRAS-järjestelmän tai jäsenvaltioiden ja komission hyväksymän vastaavan järjestelmän kautta.

11 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa, lukuun ottamatta 10 artiklaa, jota sovelletaan 7 päivästä toukokuuta 2026.

Tehty Brysselissä 6 päivänä toukokuuta 2025.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE

Tietoturvaloukkauksen tai turvallisuuden vaarantumisen arviointiperusteet

1. Jäsenvaltioiden on perustettava tietoturvaloukkauksen tai turvallisuuden vaarantumisen arviointinsa seuraaviin kriteereihin:

a) Tietoturvaloukkaus tai turvallisuuden vaarantuminen on aiheuttanut tai voi aiheuttaa luonnollisen henkilön kuoleman tai huomattavaa vahinkoa luonnollisen henkilön terveydelle.

b) On tapahtunut tai voi tapahtua onnistunut, epäillysti vihamielinen ja luvaton tunkeutuminen lompakon tarjoajan, asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettujen validointimekanismien tarjoajan tai sen sähköisen tunnistamisen järjestelmän tarjoajan, jonka puitteissa lompakkoratkaisua tarjotaan, jäljempänä 'asianomaiset toimijat', verkko- ja tietojärjestelmiin, mikä voi aiheuttaa vakavia toimintahäiriöitä, ja kyseiset järjestelmät ovat asianomaisen lompakkoratkaisun, asianomaisten asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettujen validointimekanismien tai asianomaisen sähköisen tunnistamisen järjestelmän, jonka puitteissa lompakkoratkaisua tarjotaan, kriittisiä komponentteja.

c) Lompakkoratkaisu, asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettu validointimekanismi tai sähköisen tunnistamisen järjestelmä, jonka puitteissa lompakkoratkaisua tarjotaan, tai jokin niiden osa

— on täysin tai sen ennustetaan olevan täysin poissa lompakon käyttäjien tai lompakkoon luottavien osapuolten käytöstä yli 12 peräkkäisen tunnin ajan

— on täysin tai sen ennustetaan olevan täysin poissa lompakon käyttäjien tai lompakkoon luottavien osapuolten käytöstä yli 16 tunnin ajan kalenteriviikon aikana.

d) Epäillään, että lompakkoratkaisun tai asianomaisten toimijoiden tarjoamien lompakkoratkaisuun liittyvien palveluiden rajallinen käytettävyys vaikuttaa tai ennustetusti vaikuttaa yli yhteen prosenttiin lompakon käyttäjistä tai lompakkoon luottavista osapuolista.

e) On mahdollista, että fyysinen pääsy, joka on rajoitettu asiaankuuluvien toimijoiden luotettuun henkilöstöön, tai tällaisen fyysisen pääsyn suojaaminen voi vaarantua tai on vaarantunut yhteen tai useampaan sellaisten verkko- ja tietojärjestelmien sijaintipaikkaan, joilla tuetaan lompakkoratkaisua, lompakkoratkaisuun liittyvien asetuksen (EU) N:o 910/2014 5 a artiklan 8 kohdassa tarkoitettujen validointimekanismien tarjontaa tai sähköisen tunnistamisen järjestelmää, jonka puitteissa lompakkoratkaisua tarjotaan.

f) Lompakkoratkaisussa tallennettujen, siirrettyjen tai käsiteltyjen tietojen yksityisyys, eheys, luottamuksellisuus tai aitous on vaarantuvat tai voi vaarantua yhdellä tai useammalla seuraavista tavoista:

— se vaikuttaa yli yhteen prosenttiin asianomaisen lompakkoratkaisun mukaisen lompakon käyttäjistä tai yli 100 000:een kyseisistä lompakon käyttäjistä sen mukaan, kumpi määrä on pienempi

— se on seurausta onnistuneesta epäillystä vihamielisestä toiminnasta

— se on seurausta tai on todennäköisesti seurauksena yhdestä tai useammasta tunnetusta haavoittuvuudesta, mukaan lukien komission täytäntöönpanoasetuksen (EU) 2024/2981 ([1]) mukaisesti käsitellyt haavoittuvuudet

— se todennäköisesti vaikuttaa henkilötietoihin tavalla, joka todennäköisesti aiheuttaa riskin asianomaisten luonnollisten henkilöiden oikeuksille ja vapauksille, erityisesti kun on kyse asetuksen (EU) 2016/679 9 artiklan 1 kohdassa ja 10 artiklassa määriteltyjen henkilötietojen tietoturvaloukkauksesta

([1]) Komission täytäntöönpanoasetus (EU) 2024/2981, annettu 28 päivänä marraskuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä eurooppalaisten digitaalisen identiteetin lompakoiden sertifioinnin osalta (EUVL L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— se todennäköisesti vaikuttaa henkilökohtaiseen sähköiseen viestintään

— se todennäköisesti aiheuttaa suuren riskin luonnollisten henkilöiden oikeuksille ja vapauksille

— se todennäköisesti vaikuttaa haavoittuvassa asemassa oleviin luonnollisiin henkilöihin.

g) Lompakkoratkaisun sertifiointi on peruutettu tai se ennustetaan peruutettavan.

h) Tietoturvaloukkaus tai turvallisuuden vaarantuminen on aiheuttanut tai voi aiheuttaa asianomaiselle toimijalle välittömiä taloudellisia tappioita, ja kyseinen tappio on yli 500 000 euroa tai tapauksen mukaan yli 5 prosenttia asianomaisen toimijan edeltävän tilikauden vuotuisesta kokonaisliikevaihdosta sen mukaan, kumpi on pienempi.

2. Jäsenvaltiot eivät saa ottaa huomioon asianomaisten toimijoiden suorittamien tai niiden puolesta suoritettujen huoltotöiden suunniteltuja seurauksia edellyttäen, että

a) tällaisista huoltotöistä on ilmoitettu etukäteen niille lompakon käyttäjille, lompakkoon luottaville osapuolille ja asiaankuuluville toimivaltaisille valvontaelimille, joihin vaikutukset voivat kohdistua;

b) huoltotyöt ei täytä mitään tämän liitteen 1 kohdassa esitetyistä kriteereistä.

3. Edellä olevan 1 kohdan c alakohdan osalta käytettävyyteen vaikuttavan poikkeaman kesto mitataan siitä hetkestä, jona kyseisen palvelun häiriötön tarjonta keskeytyy, siihen hetkeen, jona palvelu palautetaan ja otetaan uudelleen käyttöön. Jos asianomainen toimija ei pysty määrittämään poikkeaman alkamishetkeä, poikkeaman kesto mitataan siitä hetkestä, jona poikkeama havaittiin, tai siitä hetkestä, jona poikkeama kirjattiin verkko- tai järjestelmälokeihin tai muihin tietolähteisiin, sen mukaan, kumpi ajankohta on aikaisempi. Palvelun täydellinen käyttökatkos mitataan siitä hetkestä, jona palvelu ei ollut enää käyttäjien saatavilla, siihen hetkeen, jona säännöllinen toiminta tai toiminnot on palautettu poikkeamaa edeltävälle palvelutasolle. Jos asianomainen toimija ei pysty määrittämään palvelun täydellisen käyttökatkoksen alkamishetkeä, käyttökatkoksen kesto mitataan siitä hetkestä, jona kyseinen toimija havaitsi käyttökatkoksen.

4. Edellä olevan 1 kohdan d alakohdan osalta palvelun katsotaan olevan rajoitetusti käytettävissä silloin, kun palvelu toimii huomattavasti keskimääräistä vasteaikaa hitaammin tai kun kaikki palvelun toiminnot eivät ole käytettävissä. Vasteaikaviiveiden arvioinnin on mahdollisuuksien mukaan perustuttava objektiivisiin kriteereihin, jotka perustuvat palvelujen keskimääräisiin vasteaikoihin.

5. Edellä 1 kohdan h alakohdassa tarkoitettujen tietoturvaloukkauksesta tai turvallisuuden vaarantumisesta aiheutuneiden välittömien taloudellisten tappioiden määrittämiseksi asianomaisten toimijoiden on otettava huomioon kaikki poikkeaman seurauksena aiheutuneet taloudelliset tappiot, kuten ohjelmistojen, laitteistojen tai infrastruktuurin korvaamisesta tai siirtämisestä aiheutuneet kustannukset, henkilöstökustannukset, mukaan lukien kustannukset, jotka liittyvät henkilöstön korvaamiseen tai siirtämiseen, lisähenkilöstön palkkaamiseen, ylityökorvauksiin sekä menetettyjen tai heikentyneiden taitojen palauttamiseen, sopimusvelvoitteiden noudattamatta jättämisestä aiheutuneet maksut, asiakkaille maksettavista hyvityksistä ja korvauksista aiheutuneet kustannukset, menetetyistä tuloista aiheutuneet tappiot, sisäiseen ja ulkoiseen tiedottamiseen liittyvät kustannukset, neuvontakustannukset, mukaan lukien oikeudelliseen neuvontaan, rikosteknisiin palveluihin ja korjauspalveluihin liittyvät kustannukset. Poikkeamasta johtuviksi taloudellisiksi tappioiksi ei katsota päivittäisen liiketoiminnan kannalta välttämättömiä kustannuksia, kuten infrastruktuurin, laitteiden, laitteistojen ja ohjelmistojen yleisestä ylläpidosta, parannuksista ja riskinarviointihankkeista sekä vakuutusmaksuista aiheutuvia kustannuksia. Asianomaisten toimijoiden on laskettava taloudellisten tappioiden määrät saatavilla olevien tietojen perusteella, ja jos taloudellisten tappioiden tosiasiallisia määriä ei voida määrittää, toimijoiden on arvioitava kyseiset määrät.