PROVEDBENA UREDBA KOMISIJE (EU) 2025/847

od 6. svibnja 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu reakcija na povrede sigurnosti europskih lisnica za digitalni identitet

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ ([1]), a posebno njezin članak 5.e stavak 5.,

budući da:

(1) Europski okvir za digitalni identitet („okvir”) utvrđen Uredbom (EU) br. 910/2014 bitan je element za uspostavu sigurnog i interoperabilnog ekosustava digitalnog identiteta u cijeloj Uniji. Temelj okvira su europske lisnice za digitalni identitet („lisnice”), a cilj mu je olakšati pristup uslugama u svim državama članicama i zajamčiti zaštitu osobnih podataka i privatnosti.

(2) Na aktivnosti obrade osobnih podataka na temelju ove Uredbe primjenjuju se uredbe (EU) 2016/679 ([2]) i (EU) 2018/1725 ([3]) Europskog parlamenta i Vijeća i, prema potrebi, Direktiva 2002/58/EZ Europskog parlamenta i Vijeća ([4]). Pravilima o procjeni i pružanju informacija utvrđenima ovom Uredbom ne dovodi se u pitanje obveza izvješćivanja nadležnog nadzornog tijela o povredama osobnih podataka ako je to primjenjivo na temelju Uredbe (EU) 2016/679 ili Uredbe (EU) 2018/1725 ni obveza obavješćivanja ispitanika o povredama osobnih podataka ako je to primjenjivo na temelju tih uredbi.

(3) Komisija redovito ocjenjuje nove tehnologije, prakse, norme i tehničke specifikacije. Kako bi države članice u najvećoj mogućoj mjeri usklađeno razvijale i certificirale lisnice, tehničke specifikacije utvrđene u ovoj Uredbi temelje se na Preporuci Komisije (EU) 2021/946 ([5]), osobito na njezinu arhitekturnom i referentnom okviru. U skladu s uvodnom izjavom 75. Uredbe (EU) 2024/1183 Europskog parlamenta i Vijeća ([6]) Komisija bi ovu Provedbenu uredbu trebala preispitivati i, prema potrebi, ažurirati kako bi bila u skladu s globalnim kretanjima, arhitekturnim i referentnim okvirom te provjerenim praksama na unutarnjem tržištu.

([1]) SL L 257, 28.8.2014., str. 73., ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).
([4]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37., ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([5]) Preporuka Komisije (EU) 2021/946 od 3. lipnja 2021. o zajedničkom Unijinu paketu alata za koordinirani pristup europskom okviru za digitalni identitet (SL L 210, 14.6.2021., str. 51., ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([6]) Uredba (EU) 2024/1183 Europskog parlamenta i Vijeća od 11. travnja 2024. o izmjeni Uredbe (EU) br. 910/2014 u pogledu uspostave europskog okvira za digitalni identitet (SL L, 2024/1183, 30.4.2024., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) U slučaju povrede ili ugroženosti sigurnosti izvedbe lisnice ili mehanizama za validaciju iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 ili sustava elektroničke identifikacije u okviru kojeg se izvedbe lisnice stavljaju na raspolaganje, reakcije na takve povrede i ugroženost sigurnosti moraju u svim državama članicama uslijediti brzo, koordinirano i sigurno kako bi se zaštitili korisnici i održalo povjerenje u ekosustav digitalnog identiteta. Time se ne dovode u pitanje Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća ([7]), i uredbe (EU) 2019/881 ([8]) (EU) 2024/2847 ([9]) Europskog parlamenta i Vijeća, prije svega kad je riječ o postupanju s incidentima ili ranjivostima i njihovu svrstavanju među povrede sigurnosti. Države članice stoga bi se trebale pobrinuti da se stavljanje na raspolaganje i korištenje lisnica čija je sigurnost povrijeđena ili ugrožena pravodobno suspendiraju ili da se one prema potrebi povuku.

(5) Kako bi reakcije na povredu ili ugroženost sigurnosti bile primjerene, države članice trebale bi procijeniti utječe li povreda ili ugroženost sigurnosti izvedbe lisnice, mehanizama validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 ili sustava elektroničke identifikacije u okviru kojeg se izvedba lisnice stavlja na raspolaganje na pouzdanost te ili drugih izvedbi lisnice. Ta bi se procjena trebala temeljiti na jedinstvenim kriterijima kao što su broj i kategorija pogođenih korisnika lisnice, fizičkih osoba i pouzdajućih strana lisnice, priroda zahvaćenih podataka, trajanje ugroženosti ili povrede sigurnosti, ograničena dostupnost usluge i financijski gubici te moguća ugroženost osobnih podataka. Ti bi kriteriji državama članicama trebali omogućiti fleksibilnost i diskrecijsko pravo da na razmjeran način utvrde je li narušena pouzdanost izvedbe lisnice te je li izvedbu lisnice primjereno suspendirati ili, ako je to opravdano zbog ozbiljnosti povrede ili ugroženosti, povući. Na temelju tih kriterija ne bi trebalo uslijediti automatsko povlačenje izvedbe lisnice niti automatsko suspendiranje njezina stavljanja na raspolaganje ili korištenja, nego bi ih države članice trebale na odgovarajući način razmotriti kad odlučuju o potrebi povlačenja izvedbe lisnice ili suspendiranja njezina stavljanja na raspolaganje ili korištenja.

(6) Zbog posljedica i neugodnosti koje uzrokuje suspenzija korištenja izvedbi lisnice države članice morat će ocijeniti je li za odgovarajuću reakciju na povredu ili ugroženost sigurnosti potrebno opozvati potvrde jedinice lisnice ili poduzeti neke druge dodatne mjere.

(7) Kako bi korisnici bili upoznati sa statusom svojih lisnica, trebaju dobivati odgovarajuće informacije o povredama ili ugroženosti sigurnosti koje utječu na njihove lisnice. Budući da povrede i ugroženost sigurnosti mogu utjecati i na pouzdajuće strane lisnice registrirane u Uniji, relevantne informacije o povredama i ugroženosti sigurnosti treba prosljeđivati i njima.

(8) Radi veće transparentnosti i izgradnje povjerenja u ekosustav digitalnog identiteta, informacije o povredama ili ugroženosti sigurnosti i o njihovim posljedicama trebale bi sadržavati barem informacije koje se zahtijevaju na temelju ove Uredbe. Međutim, informacije o povredama ili ugroženosti sigurnosti koje se dijele s korisnicima lisnice i pouzdajućim stranama lisnice trebalo bi pažljivo procijeniti kako bi se spriječilo njihovo iskorištavanje i kako bi se rizik da ih iskoriste napadači sveo na minimum.

([7]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) (SL L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Kako bi korisnici nakon otklanjanja povrede ili ugroženosti sigurnosti mogli ponovno pristupiti svojim jedinicama lisnice, država članica koja je te izvedbe lisnice stavila na raspolaganje morat će bez nepotrebne odgode ponovno uspostaviti njihovo stavljanje na raspolaganje i korištenje. To se može učiniti ponovnom uspostavom jedinica lisnice, izdavanjem jedinica lisnice koje se stavljaju na raspolaganje u okviru nove verzije izvedbi lisnice ili ponovnim izdavanjem novih valjanih potvrda jedinice lisnice. O tome treba obavijestiti pogođene korisnike lisnice, pouzdajuće strane lisnice, jedinstvene kontaktne točke imenovane u skladu s člankom 46.c stavkom 1. Uredbe (EU) br. 910/2014 i Komisiju.

(10) Kako bi se zajamčilo da će lisnice biti povučene ako se povreda ili ugroženost sigurnosti ne otkloni u roku od tri mjeseca od suspenzije ili ako je to opravdano zbog ozbiljnosti povrede ili ugroženosti sigurnosti, država članica trebala bi se pobrinuti za to da se relevantne potvrde jedinice lisnice opozovu te da ih nije moguće vratiti u valjano stanje niti izdati ili dati postojećim jedinicama lisnice. Nadalje, u okviru zahvaćene izvedbe lisnice ne bi se smjele stavljati na raspolaganje nove jedinice lisnice. Radi transparentnosti, o povlačenju treba obavijestiti korisnike, pouzdajuće strane lisnice, jedinstvene kontaktne točke imenovane u skladu s člankom 46.c stavkom 1. Uredbe (EU) br. 910/2014 i Komisiju. Obavijest uključuje opis mogućih posljedica za korisnike lisnice, prvenstveno kad je riječ o upravljanju izdanim potvrdama, ili za pouzdajuće strane lisnice.

(11) Rok od tri mjeseca nakon suspenzije stavljanja na raspolaganje i korištenja izvedbe lisnice u kojem treba otkloniti povredu ili ugroženosti sigurnosti zbog koje je suspenzija uvedena trebao bi ujedno biti rok nakon kojeg tu izvedbu lisnice treba povući ako nije primijenjena odgovarajuća korektivna mjera. Države članice su, međutim, slobodne zahtijevati da se povreda ili ugroženost sigurnosti otkloni u roku kraćem od tri mjeseca, osobito ako je to potrebno zbog opsega, trajanja i posljedica te povrede ili ugroženosti sigurnosti. Ako se povreda ili ugroženost sigurnosti ne otkloni ili se ne može otkloniti u roku koji odredi država članica, ona može zahtijevati da se ta izvedba lisnice povuče prije isteka razdoblja od tri mjeseca. Razdoblje u kojem se mora otkloniti povreda ili ugroženost sigurnosti zbog koje su suspendirani stavljanje na raspolaganje i korištenje izvedbe lisnice države članice trebale bi iskoristiti za pripremu potencijalnog povlačenja te izvedbe lisnice i s njime povezanih obavijesti.

(12) Kako bi ih dostavljanje informacija Komisiji i drugim državama članicama u skladu s ovom Uredbom što manje administrativno opteretilo, države članice trebale bi koristiti postojeće alate za obavješćivanje kao što je sustav za izvješćivanje i analizu kibernetičkih incidenta („CIRAS”), kojim upravlja Agencija Europske unije za kibersigurnost („ENISA”). Ako korisnike lisnice pogođene povredom ili ugroženošću sigurnosti i pouzdajuće strane lisnice informiraju alternativnim kanalima ili sredstvima, države članice trebale bi voditi računa o tome da relevantne informacije budu jasne, cjelovite i lako dostupne. Kanali za davanje takvih informacija pogođenim korisnicima lisnice i pouzdajućim stranama lisnice trebali bi raspolagati odgovarajućim rješenjima za emitiranje na internetskim stranicama, praćenje ažuriranja internetskih stranica u stvarnom vremenu i objedinjavanje vijesti.

(13) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 te je on dao mišljenje 31. siječnja 2025.

(14) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 48. Uredbe (EU) br. 910/2014,

DONIJELA JE OVU UREDBU:

Članak 1.

Predmet

Ovom se Uredbom utvrđuju pravila za reakcije na povrede sigurnosti lisnica, mehanizama validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 i sustava elektroničke identifikacije u okviru kojeg su lisnice stavljene na raspolaganje.

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „izvedba lisnice” znači kombinacija softvera, hardvera, usluga, postavki i konfiguracija, uključujući instance lisnice, najmanje jednu sigurnu kriptografsku aplikaciju lisnice i najmanje jedan sigurni kriptografski uređaj lisnice;

2. „korisnik lisnice” znači korisnik koji ima kontrolu nad jedinicom lisnice;

3. „pouzdajuća strana lisnice” znači pouzdajuća strana koja se namjerava pouzdati u jedinice lisnice radi pružanja javnih ili privatnih usluga putem digitalne interakcije;

4. „instanca lisnice” znači aplikacija koja je instalirana i konfigurirana na uređaju ili u okruženju korisnika lisnice, dio je jedinice lisnice i korisniku lisnice služi za interakciju s jedinicom lisnice;

5. „sigurna kriptografska aplikacija lisnice” znači aplikacija za upravljanje ključnim resursima povezana sa sigurnim kriptografskim uređajem lisnice čije kriptografske i nekriptografske funkcije koristi;

6. „sigurni kriptografski uređaj lisnice” znači uređaj zaštićen od neovlaštenih radnji koji osigurava okruženje povezano sa sigurnom kriptografskom aplikacijom lisnice koje ona koristi za zaštitu ključnih resursa i u kojem se za nju izvršavaju kriptografske funkcije za sigurno izvođenje ključnih operacija;

7. „pružatelj lisnice” znači fizička ili pravna osoba koja stavlja na raspolaganje izvedbe lisnice;

8. „jedinica lisnice” znači jedinstvena konfiguracija izvedbe lisnice, koja obuhvaća instance lisnice, sigurne kriptografske aplikacije lisnice i sigurne kriptografske uređaje lisnice i koju pružatelj lisnice daje pojedinačnom korisniku lisnice;

9. „ključni resursi” znači resursi unutar lisnice ili povezani s njom koji su toliko izvanredno važni da bi zbog ugrožavanja njihove dostupnosti, povjerljivosti ili cjelovitosti mogućnost pouzdavanja u jedinicu lisnice bila ozbiljno narušena;

10. „potvrda jedinice lisnice” znači podatkovni objekt koji opisuje komponente jedinice lisnice ili omogućuje njihovu autentifikaciju i validaciju.

Članak 3.

Utvrđivanje povrede ili ugroženosti sigurnosti

1. Ne dovodeći u pitanje Direktivu (EU) 2022/2555, i uredbe (EU) 2019/881 i (EU) 2024/2847, kako bi se procijenilo utječe li povreda ili ugroženost sigurnosti izvedbe lisnice, mehanizama validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 ili sustava elektroničke identifikacije u okviru kojeg je izvedba lisnice stavljena na raspolaganje na njihovu pouzdanost ili pouzdanost drugih izvedbi lisnice, države članice na odgovarajući način razmatraju kriterije iz Priloga I.

2. Ako država članica na temelju procjene iz stavka 1. utvrdi da povreda ili ugroženost sigurnosti utječe na pouzdanost izvedbe lisnice i suspendira stavljanje na raspolaganje i korištenje te izvedbe, ona poduzima mjere iz članaka 4. i 5. Ako država članica povuče izvedbu lisnice, poduzima mjere iz članaka 8. i 9.

3. Ako država članica sazna informacije o mogućoj povredi ili ugroženost sigurnosti koja bi mogla utjecati na pouzdanost jedne ili više izvedbi lisnice koje na raspolaganje stavlja druga država članica, ta država članica o toj činjenici bez nepotrebne odgode obavješćuje Komisiju i jedinstvene kontaktne točke zahvaćenih država članica imenovane u skladu s člankom 46.c stavkom 1. Uredbe (EU) br. 910/2014. Ta obavijest mora sadržavati sve informacije navedene u članku 5. stavku 2.

4. Država članica koja primi informacije poslane na temelju stavka 3. bez nepotrebne odgode poduzima mjere iz stavaka 1. i 2.

Članak 4.

Suspenzija izdavanja i korištenja lisnica i druge korektivne mjere

1. Države članice dužne su pobrinuti se da se u okviru suspendirane izvedbe lisnice ne izdaju, koriste niti aktiviraju jedinice lisnice.

2. Države članice ocjenjuju je li za odgovarajuću reakciju na povredu ili ugroženost sigurnosti potrebno opozvati potvrde jedinice lisnice za jedinice lisnice zahvaćene suspenzijom izvedbe lisnice ili poduzeti neku drugu korektivnu mjeru.

3. Mjere iz stavaka 1. i 2. poduzimaju se bez nepotrebne odgode, a u svakom slučaju najkasnije 24 sata nakon suspenzije stavljanja na raspolaganje i korištenja izvedbe lisnice čija je sigurnost povrijeđena ili ugrožena.

4. Mjere iz stavaka 1. i 2. ne smiju spriječiti pogođene korisnike lisnice da ostvare pravo na prenosivost podataka iz članka 5.a stavka 4. točke (g) Uredbe (EU) br. 910/2014. Pritom se mora zajamčiti da korisnici lisnice to pravo mogu ostvariti tako da to ne naruši sigurnost ključnih resursa zahvaćenih jedinica lisnice, osobito vodeći računa o razlozima za suspenziju i potrebi da se osigura djelotvorna zaštita tih resursa od zlouporabe.

Članak 5.

Informacije o suspenzijama i korektivnim mjerama

1. Jasne, sveobuhvatne i lako dostupne informacije o suspenziji stavljanja na raspolaganje i korištenja izvedbe lisnice bez nepotrebne se odgode, a najkasnije 24 sata nakon suspenzije stavljanja na raspolaganje i korištenja izvedbe lisnice, dostavljaju:

(a) jedinstvenim kontaktnim točkama imenovanima na temelju članka 46.c stavkom 1. Uredbe (EU) br. 910/2014;

(b) Komisiji;

(c) pogođenim korisnicima lisnice;

(d) pouzdajućim stranama lisnice registriranima u skladu s člankom 5.b Uredbe (EU) br. 910/2014.

2. Informacije dostavljene na temelju stavka 1. sadržavaju barem sljedeće:

(a) ime pružatelja izvedbe lisnice čije su stavljanje na raspolaganje i korištenje suspendirani;

(b) ime i referentnu oznaku te izvedbe lisnice, kako su navedeni na popisu certificiranih lisnica sastavljenom u skladu s člankom 5.d Uredbe (EU) br. 910/2014 i, prema potrebi, relevantnih verzija;

(c) datum i vrijeme otkrivanja povrede ili ugroženosti sigurnosti;

(d) ako su poznati, datum i vrijeme početka povrede ili ugroženosti sigurnosti na temelju evidencije mrežnih ili sistemskih događaja ili drugih izvora podataka;

(e) datum i vrijeme suspenzije izvedbe lisnice;

(f) podatke za kontakt, uključujući barem e-adresu i telefonski broj za državu članicu koja dostavlja informacije i, ako se razlikuju, pružatelja lisnice iz točke (a);

(g) opis povrede ili ugroženosti sigurnosti;

(h) opis ugroženih podataka, uključujući, prema potrebi, kategorije osobnih podataka kako su definirane u članku 9. stavku 1. i članku 10. Uredbe (EU) 2016/679;

(i) ako je moguće, procjenu približnog broja pogođenih korisnika lisnice i drugih pogođenih fizičkih osoba;

(j) opis mogućih posljedica za pouzdajuće strane lisnice ili korisnike lisnice i, u potonjem slučaju, prema potrebi, eventualne prijedloge mjera koje korisnici lisnice mogu poduzeti da te potencijalne posljedice ublaže;

(k) opis poduzetih ili planiranih mjera za otklanjanje povrede ili ugroženosti sigurnosti te plan i rok za te mjere;

(l) ako je to primjenjivo i primjereno, opis poduzetih ili planiranih mjera za prelazak korisnika lisnice na alternativne izvedbe lisnice ili usluge.

Članak 6.

Ponovna uspostava stavljanja na raspolaganje i korištenja lisnica

Ako je to potrebno kako bi se ponovno uspostavili stavljanje na raspolaganje, aktivacija i korištenje izvedbe lisnice, države članice bez nepotrebne odgode:

1. ponovno uspostavljaju stavljanje na raspolaganje i korištenje jedinica lisnice koje se stavljaju na raspolaganje u okviru te izvedbe lisnice, i to tako što svim pogođenim korisnicima izdaju jedinicu lisnice u okviru nove verzije izvedbe lisnice;

2. novim jedinicama lisnice ili, prema potrebi, prethodno izdanim jedinicama lisnice izdaju nove potvrde jedinice lisnice pod uvjetom da te jedinice lisnice ispunjavaju sigurnosne zahtjeve koji vrijede nakon otklanjanja povrede ili ugroženosti sigurnosti;

3. stavljaju izvan snage sve mjere poduzete u skladu s člankom 4. koje sprečavaju stavljanje na raspolaganje novih jedinica lisnice u okviru zahvaćene izvedbe lisnice, ako su se te mjere odnosile isključivo na sad već otklonjenu povredu ili ugroženost sigurnosti.

Članak 7.

Informacije o ponovnoj uspostavi

Ako država članica ponovno uspostavi izvedbu lisnice, dužna je pobrinuti se:

1. da se informacije o toj činjenici bez nepotrebne odgode pošalju svim stranama koje su u skladu s člankom 5. stavkom 1. primile informacije o suspenziji stavljanja na raspolaganje i korištenja te izvedbe lisnice;

2. da informacije koje se dostavljaju na temelju točke 1. sadržavaju barem elemente iz članka 5. stavka 2. točaka (a) i (b) te od (f) do (h), kao i sljedeće:

   (a) datum i vrijeme otklanjanja povrede ili ugroženosti sigurnosti;

   (b) datum i vrijeme ponovne uspostave zahvaćene izvedbe lisnice i, prema potrebi, zahvaćenih jedinica lisnice koje su stavljene na raspolaganje u okviru te izvedbe lisnice;

   (c) opis mjera poduzetih za otklanjanje povrede ili ugroženosti sigurnosti;

   (d) opis mogućih preostalih posljedica za pouzdajuće strane lisnice ili korisnike lisnice i, u potonjem slučaju, prema potrebi, eventualne prijedloge mjera koje korisnici lisnice mogu poduzeti da te potencijalne preostale posljedice ublaže;

Članak 8.

Povlačenje lisnica

1. Ako se povreda ili ugroženost sigurnosti zbog koje su suspendirani stavljanje na raspolaganje i korištenje izvedbe lisnice ne otkloni u roku od tri mjeseca od datuma suspenzije stavljanja na raspolaganje i korištenja te izvedbe lisnice, država članica koja tu izvedbu stavlja na raspolaganje dužna je pobrinuti se da se zahvaćena izvedba lisnice povuče i da se njezina valjanost opozove bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata nakon isteka tromjesečnog razdoblja.

2. Ako država članica povuče izvedbu lisnice, dužna je pobrinuti se:

(a) da se opozovu potvrde jedinice lisnice za lisnice izdane u okviru zahvaćene izvedbe lisnice;

(b) da se potvrde jedinice lisnice ne mogu vratiti u valjano stanje;

(c) da se postojećim jedinicama lisnice koje su stavljene na raspolaganje u okviru zahvaćene izvedbe lisnice ne može izdati nova potvrda jedinice lisnice;

(d) da se u okviru zahvaćene izvedbe lisnice ne mogu staviti na raspolaganje nove jedinice lisnice.

3. Mjere iz stavaka 1. i 2. ne smiju spriječiti pogođene korisnike lisnice da ostvare pravo na prenosivost podataka iz članka 5.a stavka 4. točke (g) Uredbe (EU) br. 910/2014. Pritom se mora zajamčiti da korisnici lisnice to pravo mogu ostvariti tako da to ne naruši sigurnost ključnih resursa zahvaćenih jedinica lisnice, osobito vodeći računa o razlozima za povlačenje i potrebi da se osigura djelotvorna zaštita tih resursa od zlouporabe.

Članak 9.

Informacije o povlačenju

1. Jasne, sveobuhvatne i lako dostupne informacije o povlačenju izvedbe lisnice bez nepotrebne se odgode, a najkasnije 24 sata nakon povlačenja izvedbe lisnice, dostavljaju:

(a) jedinstvenim kontaktnim točkama imenovanima na temelju članka 46.c stavkom 1. Uredbe (EU) br. 910/2014;

(b) Komisiji;

(c) pogođenim korisnicima lisnice;

(d) pouzdajućim stranama lisnice registriranima u skladu s člankom 5.b Uredbe (EU) br. 910/2014.

2. Informacije dostavljene na temelju stavka 1. sadržavaju barem sljedeće:

(a) ime pružatelja izvedbe lisnice koja je povučena;

(b) ime i referentnu oznaku te izvedbe lisnice, kako su navedeni na popisu certificiranih lisnica sastavljenom u skladu s člankom 5.d Uredbe (EU) br. 910/2014 i, prema potrebi, relevantnih verzija;

(c) datum i vrijeme otkrivanja povrede ili ugroženosti sigurnosti zbog čije je ozbiljnosti ili neotklanjanja u roku od tri mjeseca povučena pogođena izvedba lisnice;

(d) ako su poznati, datum i vrijeme početka povrede ili ugroženosti sigurnosti na temelju evidencije mrežnih ili sistemskih događaja ili drugih izvora podataka;

(e) datum i vrijeme povlačenja izvedbe lisnice i stvarnog opoziva potvrda jedinice lisnice za jedinice stavljene na raspolaganje u okviru dotične izvedbe lisnice;

(f) informaciju je li povlačenje uslijedilo zbog ozbiljnosti povrede ili ugroženosti sigurnosti ili zbog neotklanjanja povrede ili ugroženosti sigurnosti;

(g) podatke za kontakt, uključujući barem e-adresu i telefonski broj za državu članicu koja dostavlja informacije i, ako se razlikuju, pružatelja lisnice iz točke (a);

(h) opis povrede ili ugroženosti sigurnosti;

(i) opis ugroženih podataka, uključujući, prema potrebi, kategorije osobnih podataka kako su navedene u članku 9. stavku 1. i članku 10. Uredbe (EU) 2016/679;

(j) ako je moguće, procjenu približnog broja pogođenih korisnika lisnice i drugih pogođenih fizičkih osoba;

(k) opis mogućih posljedica za pouzdajuće strane lisnice ili korisnike lisnice i, u potonjem slučaju, prema potrebi, eventualne prijedloge mjera koje korisnici lisnice mogu poduzeti da te potencijalne posljedice ublaže;

(l) opis poduzetih ili planiranih mjera za prelazak korisnika lisnice na alternativne izvedbe lisnice ili, ako je to primjenjivo i primjereno, na alternativne usluge.

Članak 10.

Informacijski sustav

Države članice informacije iz članaka 3., 5., 7. i 9. Komisiji i jedinstvenim kontaktnim točkama država članica imenovanima na temelju članka 46.c stavkom 1. Uredbe (EU) br. 910/2014 dostavljaju putem sustava CIRAS, kojim upravlja ENISA, ili ekvivalentnog sustava koji su dogovorile države članice i Komisija.

Članak 11.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama, osim članka 10., koji se primjenjuje od 7. svibnja 2026.

Sastavljeno u Bruxellesu 6. svibnja 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG

Kriteriji za procjenu povrede ili ugroženosti sigurnosti

1. Države članice procjenu povrede ili ugroženosti sigurnosti temelje na sljedećim kriterijima:

(a) povreda ili ugroženost uzrokovala je ili može uzrokovati smrt osobe ili znatno narušeno zdravlje osobe;

(b) izvršen je ili može biti izvršen uspješan, pretpostavljeno zlonamjeran i neovlašten pristup mrežnim i informacijskim sustavima pružatelja lisnice, pružatelja mehanizama validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 ili pružatelja sustava elektroničke identifikacije u okviru kojeg se izvedba lisnice stavlja na raspolaganje („dotični subjekti”), i to na način koji može uzrokovati ozbiljne poremećaje u radu, a ti su sustavi ključne komponente zahvaćene izvedbe lisnice, zahvaćenih mehanizama validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 ili zahvaćenog sustava elektroničke identifikacije u okviru kojeg se izvedba lisnice stavlja na raspolaganje;

(c) izvedba lisnice, mehanizam validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 ili sustav elektroničke identifikacije u okviru kojeg se izvedba lisnice stavlja na raspolaganje ili neki njihov dio:

— potpuno su ili se predviđa da će biti potpuno nedostupni korisnicima lisnice ili pouzdajućim stranama lisnice dulje od 12 uzastopnih sati,

— nedostupni su ili se predviđa da će biti nedostupni korisnicima lisnice ili pouzdajućim stranama lisnice dulje od 16 sati u kalendarskom tjednu;

(d) sumnja se da ograničena dostupnost izvedbe lisnice ili usluga koje dotični subjekti pružaju u vezi s tom izvedbom lisnice utječe ili se predviđa da će utjecati na više od 1 % korisnika lisnice ili pouzdajućih strana lisnice;

(e) ugroženi su ili se mogu ugroziti fizički pristup ograničen na pouzdano osoblje dotičnih subjekata ili zaštita takvog fizičkog pristupa jednoj ili više lokacija mrežnih i informacijskih sustava koji podupiru izvedbu lisnice, stavljanje na raspolaganje mehanizama validacije iz članka 5.a stavka 8. Uredbe (EU) br. 910/2014 povezanih s izvedbom lisnice ili sustav elektroničke identifikacije u okviru kojeg se izvedba lisnice stavlja na raspolaganje;

(f) privatnost, cjelovitost, povjerljivost ili autentičnost podataka pohranjenih, prenesenih ili obrađenih u izvedbi lisnice ugroženi su ili se mogu ugroziti na jedan ili više sljedećih načina:

— tako da to utječe na više od 1 % korisnika lisnice zahvaćene izvedbe lisnice ili na više od 100 000 korisnika te lisnice, ovisno o tome koji je broj manji,

— kao rezultat uspješne pretpostavljeno zlonamjerne aktivnosti,

— kao posljedica ili vjerojatna posljedica jedne ili više poznatih ranjivosti, uključujući one s kojima se postupa u skladu s Provedbenom uredbom Komisije (EU) 2024/2981 ([1]),

— tako da će to vjerojatno utjecati na osobne podatke na način koji će vjerojatno prouzročiti rizik za prava i slobode dotičnih fizičkih osoba, a posebno u slučaju povrede osobnih podataka kako su definirani u članku 9. stavku 1. i članku 10. Uredbe (EU) 2016/679,

([1]) Provedbena uredba Komisije (EU) 2024/2981 od 28. studenog 2024. o utvrđivanju pravila za primjenu Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća u pogledu certifikacije europskih lisnica za digitalni identitet (SL L, 2024/2981, 4.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— tako da će to vjerojatno utjecati na osobne elektroničke komunikacije,

— tako da će to vjerojatno uzrokovati visok rizik za prava i slobode fizičkih osoba,

— tako da će to vjerojatno utjecati na ranjive fizičke osobe;

(g) certifikacija izvedbe lisnice poništena je ili se predviđa da će biti poništena;

(h) incident je dotičnom subjektu uzrokovao ili može uzrokovati izravni financijski gubitak veći od 500 000 EUR ili, ako je to primjenjivo, 5 % ukupnog godišnjeg prometa dotičnog subjekta u prethodnoj financijskoj godini, ovisno koji je iznos niži.

2. Države članice ne uzimaju u obzir planirane posljedice održavanja koje obavljaju dotični subjekti ili koje se obavlja u njihovo ime, ako su ispunjeni sljedeći uvjeti:

(a) o radovima na održavanju unaprijed su obaviješteni potencijalno pogođeni korisnici lisnice, pouzdajuće strane lisnice i relevantna nadležna nadzorna tijela;

(b) radovi na održavanju ne ispunjavaju nijedan kriterij iz stavka 1. ovog Priloga.

3. Kad je riječ o stavku 1. točki (c), trajanje incidenta koji utječe na dostupnost mjeri se od trenutka poremećaja pravilnog pružanja zahvaćene usluge do trenutka ponovne uspostave i funkcioniranja usluge. Ako dotični subjekt ne može ustanoviti trenutak početka poremećaja, trajanje incidenta mjeri se od trenutka otkrivanja incidenta ili od trenutka kad je incident zabilježen u evidenciji mrežnih ili sistemskih događaja ili u drugim izvorima podataka, ovisno o tome što nastupi prije. Potpuna nedostupnost usluge mjeri se od trenutka kad usluga postane potpuno nedostupna korisnicima do trenutka ponovne uspostave redovitih aktivnosti ili operacija na razini usluge prije incidenta. Ako dotični subjekt ne može ustanoviti kad je nastupila potpuna nedostupnost usluge, nedostupnost se mjeri od trenutka kad ju je taj subjekt otkrio.

4. Kad je riječ o stavku 1. točki (d), smatra se da je dostupnost usluge ograničena osobito ako je usluga znatno sporija od prosječnog vremena odgovora ili ako nisu dostupne sve njezine funkcionalnosti. Kad god je moguće, pri procjeni kašnjenja u vremenu odgovora primjenjuju se objektivni kriteriji koji se temelje na prosječnom vremenu odgovora.

5. Kad utvrđuju izravne financijske gubitke zbog povrede ili ugroženosti iz točke (h), dotični subjekti uzimaju u obzir sve financijske gubitke koje su pretrpjeli zbog incidenta, npr. troškove zamjene ili premještanja softvera, hardvera ili infrastrukture, troškove osoblja, uključujući troškove zamjene ili premještanja osoblja, zapošljavanja dodatnog osoblja, naknade za prekovremeni rad i povrat izgubljenih ili umanjenih vještina, naknade zbog neispunjavanja ugovornih obveza, troškove pravne zaštite i naknada klijentima, gubitke zbog izgubljenih prihoda, troškove unutarnje i vanjske komunikacije te troškove savjetovanja, uključujući troškove povezane s pravnim savjetovanjem, forenzičkim uslugama i uslugama sanacije. Troškovi svakodnevnog poslovanja, kao što su troškovi općeg održavanja infrastrukture, opreme, hardvera i softvera, inicijativa za poboljšanja i procjenu rizika te premije osiguranja ne smatraju se financijskim gubicima pretrpljenima zbog incidenta. Dotični subjekti iznose financijskih gubitaka računaju iz dostupnih podataka, a ako se stvarni iznosi financijskih gubitaka ne mogu utvrditi, subjekti ih procjenjuju.