Uradni list
Evropske unije

SL
Serija L

2025/847

7.5.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/847

z dne 6. Maja 2025

o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede odzivanja na kršitve varnosti evropskih denarnic za digitalno identiteto

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES ([1]) in zlasti člena 5e(5) Uredbe,

ob upoštevanju naslednjega:

(1) Evropski okvir za digitalno identiteto (v nadaljnjem besedilu: okvir) iz Uredbe (EU) št. 910/2014 je ključni element pri vzpostavitvi varnega in interoperabilnega ekosistema ldigitalne identitete po vsej Uniji. Temelji na evropskih denarnicah za digitalno identiteto (v nadaljnjem besedilu: denarnice), njegov cilj pa je olajšati dostop do storitev v državah članicah ter hkrati zagotoviti varstvo osebnih podatkov in zasebnosti.

(2) Uredbi (EU) 2016/679 ([2]) in (EU) 2018/1725 ([3]) Evropskega parlamenta in Sveta ter, kadar je ustrezno, Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([4]) se uporabljajo za dejavnosti obdelave osebnih podatkov na podlagi te uredbe. Pravila o ocenjevanju in zagotavljanju informacij, določena v skladu s to uredbo, ne posegajo v obveznost obveščanja pristojnega nadzornega organa o kršitvah varstva osebnih podatkov, kadar je to ustrezno v skladu z Uredbo (EU) 2016/679 ali Uredbo (EU) 2018/1725, in v obveznost obveščanja posameznikov, na katere se nanašajo osebni podatki, o kršitvah varstva osebnih podatkov, kadar je to ustrezno v skladu z navedenima uredbama.

(3) Komisija redno ocenjuje nove tehnologije, prakse, standarde in tehnične specifikacije. Za zagotovitev najvišje ravni harmonizacije med državami članicami za razvoj in certificiranje denarnic tehnične specifikacije iz te uredbe temeljijo na delu, opravljenem na podlagi Priporočila Komisije (EU) 2021/946 ([5]), zlasti na arhitekturnem in referenčnem okviru, ki je del navedenega priporočila. V skladu z uvodno izjavo 75 Uredbe (EU) 2024/1183 Evropskega parlamenta in Sveta ([6]) bi morala Komisija pregledovati in po potrebi posodabljati to izvedbeno uredbo, da bi bila usklajena s svetovnim razvojem ter arhitekturnim in referenčnim okvirom ter sledila najboljšim praksam na notranjem trgu.

([1]) UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data. europa.eu/eli/reg/2018/1725/oj).
([4]) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([5]) Priporočilo Komisije (EU) 2021/946 z dne 3. junija 2021 o skupnem unijskem naboru orodij za usklajen pristop k okviru za evropsko digitalno identiteto (UL L 210, 14.6.2021, str. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([6]) Uredba (EU) 2024/1183 Evropskega parlamenta in Sveta z dne 11. aprila 2024 o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo evropskega okvira za digitalno identiteto (UL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) V primeru kršitve varnosti ali ogrožanja rešitev denarnice ali mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 ali sheme elektronske identifikacije, v okviru katere se rešitve denarnic zagotavljajo, je treba odzive na take varnostne kršitve in ogrožanja spremljati hitro, usklajeno in varno v vseh državah članicah, da se zaščitijo uporabniki in ohrani zaupanje v ekosistem digitalne identitete. To ne posega v Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta ([7]), uredbi (EU) 2019/881 ([8]) ter (EU) 2024/2847 ([9]) Evropskega parlamenta in Sveta, zlasti kar zadeva obravnavanje incidentov ali ranljivosti in njihovo obravnavo kot kršitev varnosti. Zato bi morale države članice zagotoviti pravočasno razveljavitev zagotavljanja in uporabe denarnic, pri katerih je prišlo do kršitve varnosti ali ogrožanja, ali, kadar je ustrezno, njihovega umika.

(5) Za zagotovitev ustreznih odzivov na kršitev varnosti ali ogrožanje bi morale države članice oceniti, ali kršitev varnosti ali ogrožanje rešitve denarnice, mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 ali sheme elektronske identifikacije, v okviru katere se rešitev denarnice zagotavlja, vpliva na zanesljivost te rešitve denarnice ali drugih rešitev denarnice. Taka ocena bi morala temeljiti na enotnih merilih, kot so število in kategorija uporabnikov denarnic, fizičnih oseb in prizadetih na denarnice zanašajočih se strank, narava zadevnih podatkov, trajanje ogrožanja ali kršitve varnosti, omejena razpoložljivost storitve in finančne izgube ter morebitno ogrožanje osebnih podatkov. Ta merila bi morala državam članicam zagotoviti prožnost in diskrecijsko pravico pri sorazmernem ugotavljanju učinka na zanesljivost rešitve denarnice in ali je ustrezno začasno razveljaviti rešitev denarnice ali jo umakniti, kadar je to upravičeno zaradi resnosti kršitve ali ogrožanja. Ta merila ne bi smela sprožiti samodejnega umika rešitve denarnice ali samodejne začasne razveljavitve zagotavljanja in uporabe rešitve denarnice, temveč bi jih morale države članice ustrezno upoštevati pri odločanju o ustreznosti umika ali začasne razveljavitve.

(6) Zaradi učinka in nevšečnosti, ki jih povzroča začasna razveljavitev uporabe rešitev denarnic, bodo morale države članice oceniti, ali je za ustrezen odziv na kršitev varnosti ali ogrožanje potreben preklic potrdila o enotah denarnice ali kateri koli drug dodaten ukrep.

(7) Da bi bili uporabniki denarnic obveščeni o statusu svojih denarnic, jim je treba zagotoviti ustrezne informacije o kršitvah varnosti ali ogrožanju, ki vplivajo na njihove denarnice. Ker lahko kršitve varnosti in ogrožanja vplivajo tudi na v Uniji registrirane na denarnice zanašajoče se stranke, je treba tudi njim posredovati ustrezne informacije o kršitvah varnosti in ogrožanjih.

(8) Za povečanje preglednosti in vzpostavitev zaupanja v ekosistem digitalne identitete bi morale informacije o kršitvah varnosti ali ogrožanjih in zadevnih posledicah vključevati vsaj informacije, ki se zahtevajo v skladu s to uredbo. Vendar bi bilo treba informacije o kršitvah varnosti ali ogrožanju, ki se posredujejo uporabnikom denarnic in na denarnice zanašajočim se strankam, skrbno oceniti, da bi se čim bolj zmanjšalo tveganje njihovega izkoriščanja s strani napadalcev.

([7]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Da bi uporabnikom omogočili ponovni dostop do njihovih denarnic po odpravi kršitve varnosti ali ogrožanja, bo morala država članica, ki je zagotovila rešitve denarnice, brez nepotrebnega odlašanja ponovno vzpostaviti zagotavljanje in uporabo teh rešitev. To je mogoče doseči s ponovno vzpostavitvijo enot denarnic, izdajo denarnic v okviru nove različice rešitev denarnice ali ponovno izdajo novih veljavnih potrdil o enoti denarnice. Prizadete uporabnike denarnic, na denarnice zanašajoče se stranke, enotne kontaktne točke, imenovane v skladu s členom 46c(1) Uredbe (EU) št. 910/2014, in Komisijo je treba ustrezno obvestiti.

(10) Za zagotovitev umika denarnic, kadar kršitev varnosti ali ogrožanje ni bilo odpravljeno v treh mesecih od začasne razveljavitve ali kadar je to upravičeno zaradi resnosti kršitve varnosti ali ogrožanja, bi morala država članica zagotoviti, da se zadevna potrdila o enoti denarnice prekličejo in ne morejo vrniti v veljavno stanje niti izdati ali zagotoviti obstoječim enotam denarnic. Poleg tega se v okviru prizadete rešitve denarnice ne bi smele zagotoviti nove enote denarnice. Zaradi preglednosti je treba uporabnike, zanašajoče se stranke, enotne kontaktne točke, imenovane v skladu s členom 46c(1) Uredbe (EU) št. 910/2014, in Komisijo obvestiti o umiku. To vključuje opis morebitnih učinkov na uporabnike denarnic in zlasti na upravljanje izdanih potrdil ali na denarnice zanašajoče se stranke.

(11) Po izteku trimesečnega obdobja, ki sledi začasni razveljavitvi zagotavljanja in uporabe rešitve denarnice, v katerem je treba odpraviti kršitev varnosti ali ogrožanje, ki je privedlo do začasne razveljavitve, je treba rešitev denarnice umakniti, razen če je bil v navedenem roku izveden ustrezen popravni ukrep. Vendar lahko države članice svobodno zahtevajo, da se kršitev varnosti ali ogrožanje odpravi v roku, krajšem od treh mesecev, pri čemer, kadar je to ustrezno, upoštevajo zlasti obseg, trajanje in posledice te kršitve varnosti ali ogrožanja. Kadar kršitev varnosti ali ogrožanje ni odpravljeno ali ga ni mogoče odpraviti v roku, ki ga določi država članica, lahko država članica zahteva, da se rešitev denarnice umakne pred iztekom trimesečnega obdobja. Države članice bi morale to obdobje, v katerem je treba odpraviti kršitev varnosti ali ogrožanje, ki je privedlo do začasne razveljavitve zagotavljanja in uporabe rešitve denarnice, uporabiti za pripravo morebitnega umika te rešitve denarnice in z njim povezane komunikacije.

(12) Za zmanjšanje upravnega bremena za države članice v zvezi z informacijami, ki jih je treba v skladu s to uredbo zagotoviti Komisiji in drugim državam članicam, bi morale države članice uporabiti obstoječa orodja za priglasitev, kot je sistem za poročanje in analizo kibernetskih incidentov (CIRAS), ki ga upravlja Agencija Evropske unije za kibernetsko varnost (ENISA). Kar zadeva alternativne kanale ali sredstva, ki jih je treba uporabiti za obveščanje uporabnikov denarnic, ki jih je prizadela kršitev varnosti ali ogrožanje, in na denarnice zanašajočih se strank, bi morale države članice zagotoviti, da se ustrezne informacije zagotovijo na jasen, celovit in lahko dostopen način. Kanali za zagotavljanje takih informacij prizadetim uporabnikom denarnic in na denarnice zanašajočim se strankam bi morali vključevati ustrezne rešitve za spletno objavljanje, sledenje posodobitvam spletnih mest v realnem času in združevanje novic.

(13) V skladu s členom 42(1) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 31. januarja 2025.

(14) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 48 Uredbe (EU) št. 910/2014 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Predmet urejanja

Ta uredba določa pravila za odzive na kršitve varnosti denarnic, mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 in sheme elektronske identifikacije, v okviru katere se zagotavljajo denarnice.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „rešitev denarnice“ pomeni kombinacijo programske opreme, strojne opreme, storitev, nastavitev in konfiguracij, vključno z instancami denarnic, eno ali več varnimi kriptografskimi aplikacijami denarnic in eno ali več varnimi kriptografskimi napravami denarnic;

(2) „uporabnik denarnice“ pomeni uporabnika, ki upravlja enoto denarnice;

(3) „na denarnice zanašajoča se stranka,“ pomeni zanašajočo se stranko, ki se namerava zanašati na enote denarnice za zagotavljanje javnih ali zasebnih storitev prek digitalne interakcije;

(4) „instanca denarnice“ pomeni aplikacijo, nameščeno in konfigurirano na napravi ali v okolju uporabnika denarnice, ki je del enote denarnice in ki jo uporabnik denarnice uporablja za interakcijo z enoto denarnice;

(5) „varna kriptografska aplikacija denarnice“ pomeni aplikacijo, ki upravlja kritična sredstva tako, da je povezana s kriptografskimi in nekriptografskimi funkcijami, ki jih zagotavlja varna kriptografska naprava denarnice, in jih uporablja;

(6) „varna kriptografska naprava denarnice“ pomeni napravo, odporno proti nedovoljenim posegom, ki zagotavlja okolje, ki je povezano z varno kriptografsko aplikacijo denarnice in ga ta uporablja za zaščito kritičnih sredstev ter zagotavljanje kriptografskih funkcij za varno izvajanje kritičnih operacij;

(7) „ponudnik denarnice“ pomeni fizično ali pravno osebo, ki zagotavlja rešitve denarnice;

(8) „enota denarnice“ pomeni edinstveno konfiguracijo rešitve denarnice, ki vključuje instance denarnice, varne kriptografske aplikacije denarnice in varne kriptografske naprave denarnice, ki jih ponudnik denarnice zagotavlja posameznemu uporabniku denarnice;

(9) „kritična sredstva“ pomenijo sredstva znotraj enote denarnice ali v zvezi z njo, ki so tako izjemno pomembna, da bi ogrožanje njihove razpoložljivosti, zaupnosti ali celovitosti resno ogrozilo zmožnost zanašanja na enoto denarnice;

(10) „potrdilo o enoti denarnice“ pomeni podatkovni objekt, ki opisuje komponente enote denarnice ali omogoča avtentikacijo in potrjevanje teh komponent.

Člen 3

Ugotavljanje kršitve varnosti ali ogrožanja

1. Države članice brez poseganja v Direktivo (EU) 2022/2555 in uredbi (EU) 2019/881 ter (EU) 2024/2847 ustrezno upoštevajo merila iz Priloge I k tej uredbi pri ocenjevanju, ali kršitev varnosti ali ogrožanje rešitve denarnice, mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 ali sheme elektronske identifikacije, v okviru katere se zagotavlja rešitev denarnice, vpliva na njihovo zanesljivost ali zanesljivost drugih rešitev denarnic.

2. Kadar država članica na podlagi ocene iz odstavka 1 ugotovi, da kršitev varnosti ali ogrožanje vpliva na zanesljivost rešitve denarnice, ter začasno razveljavi zagotavljanje in uporabo te rešitve, sprejme ukrepe iz členov 4 in 5. Kadar država članica umakne rešitev denarnice, sprejme ukrepe iz členov 8 in 9.

3. Kadar se država članica seznani z informacijami v zvezi z morebitno kršitvijo varnosti ali ogrožanjem, ki bi lahko vplivalo na zanesljivost ene ali več rešitev denarnic, ki jih zagotovi druga država članica, o tem brez nepotrebnega odlašanja obvestijo Komisijo in enotne kontaktne točke prizadetih držav članic, imenovane v skladu s členom 46c(1) Uredbe (EU) št. 910/2014. To obvestilo vključuje informacije iz člena 5(2).

4. Država članica, ki prejme informacije v skladu z odstavkom 3, brez nepotrebnega odlašanja sprejme ukrepe iz odstavkov 1 in 2.

Člen 4

Začasna razveljavitev zagotavljanja in uporabe denarnic ter druga pravna sredstva

1. Države članice zagotovijo, da se v okviru začasne razveljavitve rešitve denarnice ne zagotovijo, uporabljajo ali aktivirajo nobene enote denarnice.

2. Države članice ocenijo, ali je za ustrezen odziv na kršitev varnosti ali ogrožanje treba preklicati potrdila o enoti denarnice za enote denarnice, na katere vpliva začasna razveljavitev rešitve denarnice, ali uporabiti katero koli drugo dodatno pravno sredstvo.

3. Ukrepi iz odstavkov 1 in 2 se sprejmejo brez nepotrebnega odlašanja, v vsakem primeru pa najpozneje 24 ur po začasni razveljavitvi zagotavljanja in uporabe rešitve denarnice, ki je predmet kršitve varnosti ali ogrožanja.

4. Ukrepi iz odstavkov 1 in 2 ne ovirajo prizadetih uporabnikov denarnic pri uveljavljanju pravice do prenosljivosti podatkov iz člena 5a(4), točka (g), Uredbe (EU) št. 910/2014. To velja pod pogojem, da lahko uporabniki denarnic to pravico uveljavljajo brez ogrožanja varnosti kritičnih sredstev prizadetih enot denarnice, zlasti ob upoštevanju razlogov za začasno razveljavitev in potrebe po zagotovitvi učinkovite zaščite teh sredstev pred zlorabo.

Člen 5

Informacije o začasnih razveljavitvah in pravnih sredstvih

1. Informacije o začasni razveljavitvi zagotavljanja in uporabe rešitve denarnice se brez nepotrebnega odlašanja in najpozneje 24 ur po začasni razveljavitvi zagotavljanja in uporabe rešitve denarnice na jasen, celovit in lahko dostopen način posredujejo:

(a) enotni kontaktni točki, določeni v skladu s členom 46c(1) Uredbe (EU) št. 910/2014;

(b) Komisiji;

(c) prizadetim uporabnikom denarnice;

(d) na denarnice zanašajočim se strankam, registriranim v skladu s členom 5b Uredbe (EU) št. 910/2014.

2. Informacije, zagotovljene v skladu z odstavkom 1, vključujejo vsaj:

(a) ime ponudnika rešitve denarnice, katere zagotavljanje in uporaba sta bila začasno razveljavljena;

(b) ime in referenčni identifikator te rešitve denarnice, kot je naveden na seznamu certificiranih denarnic, pripravljenem v skladu s členom 5d Uredbe (EU) št. 910/2014, ter po potrebi zadevne različice;

(c) datum in čas odkritja kršitve varnosti ali ogrožanja;

(d) če sta znana, datum in čas začetka kršitve varnosti ali ogrožanja na podlagi omrežnih ali sistemskih dnevnikov ali drugih virov podatkov;

(e) datum in čas začasne razveljavitve rešitve denarnice;

(f) kontaktne podatke, ki vključujejo vsaj elektronski naslov in telefonsko številko za državo članico priglasiteljico in, kadar se razlikujeta, ponudnika denarnice iz točke (a);

(g) opis kršitve varnosti ali ogrožanja;

(h) opis ogroženih podatkov, po potrebi vključno s kategorijami osebnih podatkov, kot je opredeljeno v členu 9(1) in členu 10 Uredbe (EU) 2016/679;

(i) kadar je mogoče, oceno približnega števila prizadetih uporabnikov denarnic in drugih prizadetih fizičnih oseb;

(j) opis morebitnih učinkov na na denarnice zanašajoče se stranke ali uporabnike denarnice in v slednjem primeru, kadar je ustrezno, kakršne koli predloge ukrepov, ki jih lahko sprejmejo uporabniki denarnice za ublažitev teh morebitnih učinkov;

(k) opis sprejetih ali načrtovanih ukrepov za odpravo kršitve varnosti ali ogrožanja, skupaj z načrtom in rokom take odprave;

(l) kadar je mogoče in primerno, opis sprejetih ali načrtovanih ukrepov za prehod prizadetih uporabnikov denarnic na alternativne rešitve denarnic ali storitve.

Člen 6

Ponovna vzpostavitev zagotavljanja in uporabe denarnic

Kadar je to potrebno za zagotovitev ponovne vzpostavitve zagotavljanja, aktivacije in uporabe rešitve denarnice, države članice brez nepotrebnega odlašanja:

(1) ponovno vzpostavijo zagotavljanje in uporabo denarnic, zagotavljanih v okviru te rešitve denarnice, z izdajo enote denarnice v okviru nove različice rešitve denarnice vsem prizadetim uporabnikom;

(2) izdajo nova potrdila o enoti denarnice novim enotam denarnic ali, kadar je ustrezno, predhodno izdanim enotam denarnic, če te izpolnjujejo varnostne zahteve, vzpostavljene po odpravi kršitve varnosti ali ogrožanja;

(3) razveljavijo vse ukrepe, ki se izvajajo v skladu s členom 4 in ovirajo zagotavljanje novih enot denarnic v okviru prizadete rešitve denarnice, kadar so bili ti ukrepi povezani izključno z zdaj odpravljeno kršitvijo varnosti ali ogrožanjem.

Člen 7

Informacije o ponovni vzpostavitvi

Kadar država članica ponovno vzpostavi rešitev denarnice, zagotovi, da:

(1) se informacije o tem brez nepotrebnega odlašanja zagotovijo vsem strankam, ki so prejele informacije o začasni razveljavitvi zagotavljanja in uporabe te rešitve denarnice v skladu s členom 5(1).

(2) Informacije, zagotovljene v skladu s točko (1), vključujejo vsaj elemente iz člena 5(2), točke (a), (b) in (f) do (h), ter naslednje:

(a) datum in čas odprave kršitve varnosti ali ogrožanja;

(b) datum in čas ponovne vzpostavitve prizadete rešitve denarnice in, kadar je ustrezno, prizadetih enot denarnice, zagotovljenih v okviru te rešitve denarnice;

(c) opis ukrepov, sprejetih za odpravo kršitve varnosti ali ogrožanja;

(d) opis morebitnih preostalih učinkov na na denarnice zanašajoče se stranke ali uporabnike denarnice in v slednjem primeru, kadar je ustrezno, kakršne koli predloge ukrepov, ki jih lahko sprejmejo uporabniki denarnice za ublažitev teh morebitnih preostalih učinkov.

Člen 8

Umik denarnic

1. Če kršitev varnosti ali ogrožanje, ki je privedlo do začasne razveljavitve zagotavljanja in uporabe rešitve denarnice, ni odpravljeno v treh mesecih po datumu začasne razveljavitve zagotavljanja in uporabe te rešitve denarnice, država članica, ki zagotavlja to rešitev denarnice, zagotovi, da se prizadeta rešitev denarnice umakne in njena veljavnost prekliče brez nepotrebnega odlašanja, v vsakem primeru pa v 72 urah po izteku trimesečnega obdobja.

2. Kadar država članica umakne rešitev denarnice, zagotovi, da:

(a) se prekličejo potrdila o enoti denarnice za enoto denarnice, izdano v okviru prizadete rešitve denarnice;

(b) se potrdila o enoti denarnice ne morejo povrniti v veljavno stanje;

(c) za obstoječe enote denarnice, zagotovljene v okviru prizadete rešitve denarnice, ni mogoče izdati novega potrdila o enoti denarnice;

(d) v okviru prizadete rešitve denarnice ni mogoče zagotoviti nove enote denarnice.

3. Ukrepi iz odstavkov 1 in 2 ne ovirajo prizadetih uporabnikov denarnic pri uveljavljanju pravice do prenosljivosti podatkov iz člena 5a(4), točka (g), Uredbe (EU) št. 910/2014. To velja pod pogojem, da lahko uporabniki denarnic to pravico uveljavljajo brez ogrožanja varnosti kritičnih sredstev prizadetih enot denarnice, zlasti ob upoštevanju razlogov za umik in potrebe po zagotovitvi učinkovite zaščite teh sredstev pred zlorabo.

Člen 9

Informacije o umiku

1. Informacije o umiku rešitve denarnice se brez nepotrebnega odlašanja in najpozneje 24 ur po umiku na jasen, celovit in lahko dostopen način zagotovijo:

(a) enotni kontaktni točki, določeni v skladu s členom 46c(1) Uredbe (EU) št. 910/2014;

(b) Komisiji;

(c) prizadetim uporabnikom denarnice;

(d) na denarnice zanašajočim se strankam, registriranim v skladu s členom 5b Uredbe (EU) št. 910/2014.

2. Informacije, zagotovljene v skladu z odstavkom 1, vključujejo vsaj:

(a) ime ponudnika umaknjene rešitve denarnice;

(b) ime in referenčni identifikator te rešitve denarnice, kot je naveden na seznamu certificiranih denarnic, pripravljenem v skladu s členom 5d Uredbe (EU) št. 910/2014, ter po potrebi zadevne različice;

(c) datum in čas odkritja kršitve varnosti ali ogrožanja, ki je privedlo do umika prizadete rešitve denarnice zaradi njegove resnosti ali ker ni bilo odpravljeno v treh mesecih;

(d) če sta znana, datum in čas začetka kršitve varnosti ali ogrožanja na podlagi omrežnih ali sistemskih dnevnikov ali drugih virov podatkov;

(e) datum in čas umika rešitve denarnice ter dejanskega preklica potrdil o enoti denarnice za enote denarnic, zagotovljene v okviru zadevne rešitve denarnice;

(f) ali je umik posledica resnosti ali neodprave kršitve varnosti ali ogrožanja;

(g) kontaktne podatke, ki vključujejo vsaj elektronski naslov in telefonsko številko za državo članico priglasiteljico in, kadar se razlikujeta, ponudnika denarnice iz točke (a);

(h) opis kršitve varnosti ali ogrožanja;

(i) opis ogroženih podatkov, po potrebi vključno s kategorijami osebnih podatkov, kot je opredeljeno v členu 9(1) in členu 10 Uredbe (EU) 2016/679;

(j) kadar je mogoče, oceno približnega števila prizadetih uporabnikov denarnic in drugih prizadetih fizičnih oseb;

(k) opis morebitnih učinkov na na denarnice zanašajoče se stranke ali uporabnike denarnice in v slednjem primeru, kadar je ustrezno, kakršne koli predloge ukrepov, ki jih lahko sprejmejo uporabniki denarnice za ublažitev teh morebitnih učinkov;

(l) opis sprejetih ali načrtovanih ukrepov za prehod prizadetih uporabnikov denarnic na alternativne rešitve denarnic ali, kadar je to mogoče in primerno, alternativne storitve.

Člen 10

Informacijski sistem

Države članice pošljejo informacije iz členov 3, 5, 7 in 9 Komisiji in enotnim kontaktnim točkam držav članic, imenovanim v skladu s členom 46c(1) Uredbe (EU) št. 910/2014, prek sistema za poročanje in analizo kibernetskih incidentov (CIRAS), ki ga upravlja Agencija Evropske unije za kibernetsko varnost (ENISA), ali enakovrednega sistema, o katerem se dogovorijo države članice in Komisija.

Člen 11

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah, razen člena 10, ki se uporablja od 7. maja 2026.

V Bruslju, 6. maja 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA

Merila za oceno kršitve varnosti ali ogrožanja

1. Države članice svojo oceno kršitve ali ogrožanja varnosti utemeljijo na naslednjih merilih:

(a) kršitev ali ogrožanje je ali bi lahko povzročilo smrt fizične osebe ali znatno škodovalo njenemu zdravju;

(b) do uspešnega domnevnega zlonamernega ali nepooblaščenega dostopa do omrežnih in informacijskih sistemov ponudnika denarnice, ponudnika mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 ali ponudnika sheme elektronske identifikacije, v okviru katere se zagotavlja rešitev denarnice (v nadaljnjem besedilu: zadevni subjekti), je ali bi lahko prišlo na način, ki lahko povzroči resne operativne motnje, in ti sistemi so ključne komponente prizadete rešitve denarnice, prizadetih mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 ali prizadete sheme elektronske identifikacije, v okviru katere se zagotavlja rešitev denarnice;

(c) rešitev denarnice, mehanizem potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014 ali shema elektronske identifikacije, v okviru katere se zagotavlja rešitev denarnice, ali njen del:

— je ali bo predvidoma popolnoma nerazpoložljiv uporabnikom denarnic ali na denarnice zanašajočim se strankam več kot 12 zaporednih ur;

— je ali bo predvidoma popolnoma nerazpoložljiv uporabnikom denarnic ali na denarnice zanašajočim se strankam dlje kot 16 ur, izračunano na podlagi koledarskega tedna;

(d) obstaja sum, da omejena razpoložljivost rešitve denarnice ali storitev, ki jih zagotavljajo zadevni subjekti v zvezi z rešitvijo denarnice, vpliva ali bo predvidoma vplivala na več kot 1 % uporabnikov denarnice ali na denarnice zanašajočih se strank;

(e) fizični dostop, omejen na zaupanja vredno osebje zadevnih subjektov, ali zaščita takega fizičnega dostopa do ene ali več lokacij omrežnih in informacijskih sistemov, ki podpirajo rešitev denarnice, zagotavljanje mehanizmov potrjevanja iz člena 5a(8) Uredbe (EU) št. 910/2014, povezanih z rešitvijo denarnice, ali shema elektronske identifikacije, v okviru katere se zagotavlja rešitev denarnice, so ogroženi ali bi lahko bili ogroženi;

(f) zasebnost, celovitost, zaupnost ali avtentičnost podatkov, ki so shranjeni, preneseni ali obdelani v rešitvi denarnice, so ogroženi ali bi lahko bili ogroženi na enega ali več naslednjih načinov:

— incident vpliva na več kot 1 % ali 100 000 uporabnikov denarnice prizadete rešitve denarnice, kar je manj;

— incident je rezultat uspešne domnevno zlonamerne dejavnosti;

— incident je rezultat ali je verjetno rezultat ene ali več znanih ranljivosti, vključno s tistimi, ki se obravnavajo v skladu z Izvedbeno uredbo Komisije (EU) 2024/2981 ([1]);

— incident bo verjetno vplival na osebne podatke na način, ki bo verjetno ogrozil pravice in svoboščine zadevnih fizičnih oseb, zlasti v primeru kršitve osebnih podatkov, kot so opredeljeni v členu 9(1) in členu 10 Uredbe (EU) 2016/679;

([1]) Izvedbena uredba Komisije (EU) 2024/2981 z dne 28. novembra 2024 o določitvi pravil za uporabo Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta glede celovitosti in temeljnih funkcionalnosti evropskih denarnic za digitalno identiteto (UL L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— incident bo verjetno vplival na osebne elektronske komunikacije;

— incident bo verjetno povzročil veliko tveganje za pravice in svoboščine fizičnih oseb;

— incident bo verjetno vplival na ranljive fizične osebe;

(g) certificiranje rešitve denarnice je bilo ali bo predvidoma preklicano;

(h) kršitev ali ogrožanje je ali bi lahko zadevnemu subjektu povzročilo neposredno finančno izgubo, ki presega 500 000 EUR oziroma, kadar je ustrezno, 5 % skupnega letnega prometa zadevnega subjekta v predhodnem poslovnem letu, pri čemer se upošteva nižji znesek.

2. Države članice ne upoštevajo načrtovanih posledic vzdrževanja, ki ga izvedejo zadevni subjekti ali se izvede v njihovem imenu, pod pogojem, da:

(a) je bilo tako vzdrževanje predhodno priglašeno potencialno prizadetim uporabnikom denarnic, na denarnice zanašajočim se strankam in ustreznim pristojnim nadzornim organom;

(b) tako vzdrževanje ne izpolnjuje nobenega od meril iz odstavka 1 te priloge.

3. V zvezi s točko (c) odstavka 1 se trajanje incidenta, ki vpliva na razpoložljivost, meri od trenutka začetka motnje ustreznega zagotavljanja prizadete storitve do trenutka ponovne vzpostavitve in delovanja te storitve. Kadar zadevni subjekt ne more določiti trenutka začetka motnje, se trajanje incidenta meri od trenutka odkritja incidenta ali od trenutka, ko je bil incident zabeležen v omrežnih ali sistemskih dnevnikih ali drugih virih podatkov, kar nastopi prej. Popolna nerazpoložljivost storitve se meri od trenutka, ko je storitev uporabnikom popolnoma nerazpoložljiva, do trenutka, ko so se redne dejavnosti ali operacije ponovno vzpostavile na raven storitve, ki je bila zagotovljena pred incidentom. Kadar zadevni subjekt ne more določiti trenutka začetka popolne nerazpoložljivosti storitve, se nerazpoložljivost meri od trenutka, ko jo je ta subjekt odkril.

4. V zvezi s točko (d) odstavka 1 se šteje, da je razpoložljivost storitve omejena zlasti, kadar je odzivni čas storitve precej počasnejši od povprečnega ali kadar niso na voljo vse funkcije storitve. Kadar je mogoče, se za oceno zamud v odzivnem času uporabijo objektivna merila, ki temeljijo na povprečnem odzivnem času storitev.

5. Za določanje neposrednih finančnih izgub zaradi kršitve ali ogrožanja iz točke (h) odstavka 1 zadevni subjekti upoštevajo vse finančne izgube, ki so jih imeli zaradi incidenta, kot so stroški zamenjave ali premestitve programske opreme, strojne opreme ali infrastrukture, stroški zaposlenih, vključno s stroški, povezanimi z zamenjavo ali premestitvijo zaposlenih, zaposlovanjem dodatnih zaposlenih, plačilom nadur in ponovno pridobitvijo izgubljenih ali oslabljenih spretnosti, pristojbine zaradi neizpolnjevanja pogodbenih obveznosti, stroški za odpravo škode in nadomestila za stranke, izgube zaradi izpada prihodkov, stroški, povezani z notranjo in zunanjo komunikacijo, ter stroški svetovanja, vključno s stroški, povezanimi s pravnim svetovanjem, forenzičnimi storitvami in storitvami vnovične vzpostavitve delovanja. Stroški, potrebni za tekoče poslovanje podjetja, kot so stroški splošnega vzdrževanja infrastrukture, opreme, strojne in programske opreme, izboljšav in pobude za oceno tveganja ter zavarovalne premije, se ne štejejo za finančne izgube zaradi incidenta. Zadevni subjekti zneske finančnih izgub izračunajo na podlagi razpoložljivih podatkov ali jih ocenijo, kadar dejanskih zneskov finančnih izgub ni mogoče določiti.