Europeiska unionens
officiella tidning

SV
L-serien

2025/847

7.5.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/847

av den 6 maj 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller åtgärder mot säkerhetsincidenter som rör europeiska digitala identitetsplånböcker

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG ([1]), särskilt artikel 5e.5, och

av följande skäl:

(1) Det europeiska ramverket för digital identitet (*ramverket*), som föreskrivs i förordning (EU) nr 910/2014, är en avgörande komponent i inrättandet av ett säkert och interoperabelt ekosystem för digital identitet i hela unionen. De europeiska digitala identitetsplånböckerna (*plånböckerna*) utgör hörnstenen i ramverket som syftar till att underlätta tillgång till tjänster i alla medlemsstater, samtidigt som skyddet av personuppgifter och integritet säkerställs.

(2) Europaparlamentets och rådets förordningar (EU) 2016/679 ([2]) och (EU) 2018/1725 ([3]) samt, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG ([4]) är tillämpliga på behandlingen av personuppgifter enligt denna förordning. Reglerna för bedömningen och tillhandahållandet av information som upprättats enligt denna förordning ska inte påverka skyldigheten att anmäla personuppgiftsincidenter till den behöriga tillsynsmyndigheten när det är tillämpligt enligt förordning (EU) 2016/679 eller förordning (EU) 2018/1725, och skyldigheten att meddela personuppgiftsincidenterna till de registrerade när det är tillämpligt enligt dessa förordningar.

(3) Kommissionen utvärderar regelbundet ny teknik, nya metoder, standarder och tekniska specifikationer. För att säkerställa största möjliga harmonisering bland medlemsstaterna för utveckling och certifiering av plånböcker bygger de tekniska specifikationerna i denna förordning på det arbete som utförts enligt kommissionens rekommendation (EU) 2021/946 ([5]), särskilt arkitekturen och referensramen som är en del av den. I enlighet med skäl 75 i Europaparlamentets och rådets förordning (EU) 2024/1183 ([6]) bör kommissionen vid behov se över och uppdatera denna genomförandeförordning för att hålla den i linje med den globala utvecklingen och arkitekturen och referensramen och för att följa praxis på den inre marknaden.

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

([2]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Kommissionens rekommendation (EU) 2021/946 av den 3 juni 2021 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet (EUT L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Vid en säkerhetsincident eller ett äventyrande rörande plånbokslösningarna eller rörande de valideringsmekanismer som avses i artikel 5a.8 i förordning (EU) nr 910/2024, eller rörande det system för elektronisk identifiering under vilket plånbokslösningarna tillhandahålls, behöver sådana säkerhetsincidenter och äventyranden följas av snabba, samordnade och säkra åtgärder i alla medlemsstater för att skydda användarna och upprätthålla förtroendet för ekosystemet för digital identitet. Detta ska inte påverka tillämpningen av Europaparlamentets och rådets direktiv (EU) 2022/2555 ([7]) och Europaparlamentets och rådets förordningar (EU) 2019/881 ([8]) och (EU) 2024/2847 ([9]), särskilt vad gäller att hantera incidenter eller sårbarheter och betrakta dem som säkerhetsincidenter. Därför bör medlemsstaterna säkerställa det tillfälliga upphävandet av tillhandahållandet, användningen och, i tillämpliga fall, återkallandet av de plånbokslösningar som berörs av en säkerhetsincident eller ett äventyrande.

(5) För att säkerställa lämpliga åtgärder mot en säkerhetsincident eller ett äventyrande bör medlemsstaterna bedöma om en säkerhetsincident eller ett äventyrande rörande en plånbokslösning, rörande den valideringsmekanism som avses i artikel 5a.8 i förordning (EU) nr 910/2014, eller rörande det system för elektronisk identifiering under vilket en plånbokslösning tillhandahålls, påverkar den plånbokslösningens eller andra plånbokslösningars tillförlitlighet. En sådan bedömning bör grundas på enhetliga kriterier, såsom antal och kategori av plånboksanvändare, av fysiska personer och av förlitande parter som berörs, arten av de påverkade uppgifterna, varaktigheten hos äventyrandet eller säkerhetsincidenten, den begränsade tillgången på en tjänst och de ekonomiska förlusterna samt det potentiella äventyrandet av personuppgifter. Dessa kriterier bör ge medlemsstaterna flexibilitet och självbestämmande när det gäller att, på ett proportionerligt sätt, fastställa om en plånbokslösnings tillförlitlighet påverkas och om det är lämpligt att tillfälligt upphäva eller, när det är motiverat mot bakgrund av allvaret i säkerhetsincidenten eller äventyrandet, återkalla plånbokslösningen. Dessa kriterier bör inte utlösa ett automatiskt återkallande av en plånbokslösning eller ett automatiskt tillfälligt upphävande av tillhandahållandet och användningen av en plånbokslösning, men de bör vederbörligen beaktas av medlemsstaterna när de beslutar om huruvida ett återkallande, eller ett tillfälligt upphävande av tillhandahållandet eller användningen, av en plånbokslösning är nödvändig.

(6) På grund av den inverkan och den olägenhet som orsakas av ett tillfälligt upphävande av användningen av plånbokslösningar, behöver medlemsstaterna utvärdera om återkallandet av plånboksenhetsintyg eller andra ytterligare åtgärder är nödvändiga för att vidta lämpliga åtgärder mot en säkerhetsincident eller ett äventyrande.

(7) För att plånboksanvändarna ska hållas informerade om plånböckernas status ska de ges lämplig information om de säkerhetsincidenter och äventyranden som påverkar deras plånböcker. Eftersom de förlitande parter som är registrerade i unionen också kan påverkas av säkerhetsincidenter och äventyranden, ska relevant information om säkerhetsincidenter och äventyranden också delas med dem.

(8) För att öka transparensen hos och skapa förtroende för ekosystemet för digital identitet, bör informationen om säkerhetsincidenterna eller äventyrandena och om deras konsekvenser åtminstone omfatta den information som krävs enligt denna förordning. Den information om säkerhetsincidenter eller äventyranden som delas med plånboksanvändare och förlitande parter bör dock noggrant bedömas för att förebygga och minimera risken att den utnyttjas av angripare.

([7]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) För att göra det möjligt för användare att få tillgång till sina plånboksenheter på nytt efter att en säkerhetsincident eller ett äventyrande har åtgärdats, behöver de medlemsstater som tillhandahöll plånbokslösningarna återupprätta tillhandahållandet och användningen av de plånbokslösningarna utan onödigt dröjsmål. Detta kan ske genom att återupprätta plånboksenheterna, genom att utfärda plånboksenheter som tillhandahålls under en ny version av plånbokslösningarna eller genom att på nytt utfärda nya giltiga plånboksenhetsintyg. De berörda plånboksanvändarna, de förlitande parterna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i förordning (EU) nr 910/2014 och kommissionen ska underrättas om detta.

(10) För att säkerställa återkallandet av plånböcker när en säkerhetsincident eller ett äventyrande inte har åtgärdats inom tre månader från det tillfälliga upphävandet eller när det är motiverat mot bakgrund av allvaret i säkerhetsincidenten eller äventyrandet, bör medlemsstaterna säkerställa att de relevanta plånboksenhetsintygen återkallas och att de varken kan återställas till giltig status eller utfärdas eller tillhandahållas till befintliga plånboksenheter. Vidare bör inga nya plånboksenheter tillhandahållas under den berörda plånbokslösningen. Av transparensskäl behöver användarna, de förlitande parterna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i förordning (EU) nr 910/2014 och kommissionen underrättas om återkallandet. Detta innefattar en beskrivning av den möjliga inverkan på plånboksanvändarna och i synnerhet förvaltningen av utfärdade intyg, eller på de förlitande parterna.

(11) När tremånadersperioden efter det tillfälliga upphävandet av tillhandahållandet och användningen av en plånbokslösning, under vilken den säkerhetsincident eller det äventyrande som ledde till det tillfälliga upphävandet ska åtgärdas, har löpt ut ska plånbokslösningen återkallas om inte en lämplig åtgärd har vidtagits. Medlemsstaterna får dock kräva att säkerhetsincidenten eller äventyrandet åtgärdas inom en tidsfrist som är kortare än tre månader, särskilt, och om det är relevant, med beaktande av den säkerhetsincidentens eller det äventyrandets omfattning, varaktighet och följder. Om säkerhetsincidenten eller äventyrandet inte har åtgärdats eller inte har kunnat åtgärdas inom den tidsfrist som fastställts av medlemsstaten, får medlemsstaten kräva att plånbokslösningen återkallas innan tremånadersperioden löper ut. Medlemsstaterna bör använda denna tidsperiod, under vilken en säkerhetsincident eller ett äventyrande som ledde till det tillfälliga upphävandet av tillhandahållandet och användningen av en plånbokslösning måste åtgärdas, till att förbereda det eventuella återkallandet av plånbokslösningen och åtföljande meddelanden.

(12) För att minska medlemsstaternas administrativa börda avseende den information som ska tillhandahållas, i enlighet med denna förordning, till kommissionen och andra medlemsstater, bör medlemsstaterna använda befintliga anmälningsverktyg, såsom systemet för rapportering och analys av cyberincidenter (*Cyber Incident Reporting and Analysis System*, CIRAS) som drivs av Europeiska unionens cybersäkerhetsbyrå (Enisa). När det gäller alternativa kanaler eller sätt för tillhandahållande av information till de plånboksanvändare som berörs av en säkerhetsincident eller ett äventyrande och till de förlitande parterna bör medlemsstaterna säkerställa att den relevanta informationen tillhandahålls på ett tydligt, heltäckande och lättillgängligt sätt. Kanalerna för tillhandahållande av sådan information till de berörda plånboksanvändarna och de förlitande parterna bör innefatta lämpliga lösningar för webbplatsbaserade sändningstjänster, spårning i realtid av webbplatsuppdateringar samt nyhetssamlare.

(13) Samråd med Europeiska datatillsynsmannen har skett i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 31 januari 2025.

(14) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 48 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Innehåll

I denna förordning fastställs regler för åtgärder mot säkerhetsincidenter rörande plånböckerna, rörande de valideringsmekanismer som avses i artikel 5a.8 i förordning (EU) nr 910/2014 och rörande det system för elektronisk identifiering under vilket plånböckerna tillhandahålls.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

(1) *plånbokslösning*: en kombination av programvara, hårdvara, tjänster, inställningar och konfigureringar, inklusive plånboksinstanser, en eller flera krypteringsapplikationer och en eller flera krypteringshårdvaror.

(2) *plånboksanvändare*: en användare som kontrollerar plånboksenheten.

(3) *förlitande part*: en förlitande part som avser att förlita sig på plånboksenheter för att genom digital interaktion tillhandahålla offentliga eller privata tjänster.

(4) *plånboksinstans*: den applikation som är installerad och konfigurerad på en plånboksanvändares hårdvara eller i en plånboksanvändares miljö, som ingår i en plånboksenhet och som plånboksanvändaren använder för att interagera med plånboksenheten.

(5) *krypteringsapplikation*: en applikation som hanterar kritiska tillgångar genom att vara kopplad till och använda de kryptografiska och icke-kryptografiska funktioner som tillhandahålls av krypteringshårdvaran.

(6) *krypteringshårdvara*: manipuleringssäker hårdvara som tillhandahåller en miljö som är kopplad till och används av krypteringsapplikationen för att skydda kritiska tillgångar och tillhandahålla kryptografiska funktioner för att säkert kunna utföra kritiska operationer.

(7) *plånbokstillhandahållare*: en fysisk eller juridisk person som tillhandahåller plånbokslösningar.

(8) *plånboksenhet*: en unik konfigurering av en plånbokslösning som omfattar plånboksinstanser, krypteringsapplikationer och krypteringshårdvaror som en plånbokstillhandahållare tillhandahåller en enskild plånboksanvändare.

(9) *kritiska tillgångar*: tillgångar inom eller i samband med en plånboksenhet som är av sådan extraordinär betydelse att det, om deras konfidentialitet, integritet och tillgänglighet äventyrades, skulle få en mycket allvarlig, funktionsnedsättande inverkan på förmågan att förlita sig på plånboksenheten.

(10) *plånboksenhetsintyg*: ett dataobjekt som beskriver plånboksenhetens komponenter eller möjliggör autentisering och validering av dessa komponenter.

Artikel 3

Fastställande av en säkerhetsincident eller ett äventyrande

1. Utan att det påverkar tillämpningen av direktiv (EU) 2022/2555, och av förordningarna (EU) 2019/881 och (EU) 2024/2847, ska kommissionen vederbörligen beakta de kriterier som anges i bilaga I till den här förordningen för att bedöma om en säkerhetsincident eller ett äventyrande rörande en plånbokslösning, rörande en valideringsmekanism enligt artikel 5a.8 i förordning (EU) nr 910/2014 eller rörande det system för elektronisk identifiering under vilket plånböckerna tillhandahålls påverkar deras eller andra plånbokslösningars tillförlitlighet.

2. Om en medlemsstat, på grundval av bedömningen i punkt 1, fastställer att en säkerhetsincident eller ett äventyrande påverkar plånbokslösningens tillförlitlighet och tillfälligt upphäver tillhandahållandet och användningen av plånbokslösningen, ska den medlemsstaten vidta de åtgärder som anges i artiklarna 4 och 5. Om en medlemsstat återkallar plånbokslösningen, ska medlemsstaten vidta de åtgärder som anges i artiklarna 8 och 9.

3. Om en medlemsstat får kännedom om information rörande en möjlig säkerhetsincident eller ett möjligt äventyrande som kan påverka tillförlitligheten hos en eller flera plånbokslösningar som tillhandahålls av en annan medlemsstat, ska den medlemsstaten utan onödigt dröjsmål underrätta kommissionen och de berörda medlemsstaternas gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i förordning (EU) nr 910/2014 om detta. Denna underrättelse ska innehålla den information som anges i artikel 5.2.

4. Den medlemsstat som mottar den information som tillhandahålls i enlighet med punkt 3 ska utan onödigt dröjsmål vidta de åtgärder som föreskrivs i punkterna 1 och 2.

Artikel 4

Tillfälligt upphävande av tillhandahållandet och användningen av plånböcker samt andra åtgärder

1. Medlemsstaterna ska säkerställa att inga plånboksenheter tillhandahålls, används eller aktiveras inom den tillfälligt upphävda plånbokslösningen.

2. Medlemsstaterna ska utvärdera om det är nödvändigt att återkalla plånboksenhetsintyg för de plånboksenheter som berörs av det tillfälliga upphävandet av plånbokslösningen, eller av någon annan ytterligare åtgärd, för att på ett lämpligt sätt vidta åtgärder mot säkerhetsincidenten eller äventyrandet.

3. De åtgärder som anges i punkterna 1 och 2 ska vidtas utan onödigt dröjsmål, och i alla omständigheter senast 24 timmar efter det tillfälliga upphävandet av tillhandahållandet och användningen av den plånbokslösning som berörs av säkerhetsincidenten eller äventyrandet.

4. De åtgärder som anges i punkterna 1 och 2 ska inte hindra de berörda plånboksanvändarna från att utöva sin rätt till dataportabilitet i enlighet med artikel 5a.4 g i förordning (EU) nr 910/2014. Detta förutsätter att plånboksanvändarna kan utöva denna rätt utan att det påverkar säkerheten hos de berörda plånboksenheternas kritiska tillgångar, i synnerhet med beaktande av skälen till det tillfälliga upphävandet och behovet av att säkerställa ett effektivt skydd av de tillgångarna mot missbruk.

Artikel 5

Information om tillfälliga upphävanden och åtgärder

1. Information om det tillfälliga upphävandet av tillhandahållandet och användningen av plånbokslösningar ska tillhandahållas på ett tydligt, uttömmande och lättillgängligt sätt, utan onödigt dröjsmål och senast 24 timmar efter det tillfälliga upphävandet av tillhandahållandet och användningen av plånbokslösningen, till

a) de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i förordning (EU) nr 910/2014,

b) kommissionen,

c) de berörda plånboksanvändarna,

d) de förlitande parter som registrerats i enlighet med artikel 5b i förordning (EU) nr 910/2014.

2. Den information som tillhandahålls i enlighet med punkt 1 ska omfatta åtminstone följande:

a) Namnet på tillhandahållaren av den plånbokslösning vars tillhandahållande och användning tillfälligt har upphävts.

b) Namnet och referensidentifieraren för den plånbokslösningen, i enlighet med uppgifterna i förteckningen över certifierade plånböcker som upprättats i enlighet med artikel 5d i förordning (EU) nr 910/2014 och, i förekommande fall, de berörda versionerna.

c) Det datum och den tidpunkt då säkerhetsincidenten eller äventyrandet upptäcktes.

d) Om kända, det datum och den tidpunkt då säkerhetsincidenten eller äventyrandet inträffade, på grundval av nätverks- eller systemloggar eller andra datakällor.

e) Datumet och tidpunkten för det tillfälliga upphävandet av plånbokslösningen.

f) Kontaktuppgifter, inklusive åtminstone e-postadress och ett telefonnummer till den anmälande medlemsstaten och, om dessa skiljer sig åt, till den plånbokstillhandahållare som avses i punkt (a).

g) Beskrivning av säkerhetsincidenten eller äventyrandet.

h) Beskrivning av de uppgifter som äventyrats, inklusive, i förekommande fall, de kategorier av personuppgifter som anges i artikel 9.1 och artikel 10 i förordning (EU) 2016/679.

i) Om detta är möjligt, en uppskattning av antalet berörda plånboksanvändare och av andra berörda fysiska personer.

j) Beskrivning av den möjliga inverkan på de förlitande parterna eller plånboksanvändarna, och i det senare fallet, om detta är relevant, angivande av åtgärder som plånboksanvändarna kan vidta för att förmildra denna inverkan.

k) Beskrivning av de åtgärder som vidtagits eller planeras för att åtgärda säkerhetsincidenten eller äventyrandet, tillsammans med planering och tidsfrist för åtgärderna.

l) När så är tillämpligt och lämpligt, en beskrivning av de åtgärder som vidtagits eller planeras för en omställning av berörda plånboksanvändare till alternativa plånbokslösningar eller tjänster

Artikel 6

Återupprättande av tillhandahållandet och användningen av plånböcker

Om det är nödvändigt för att säkerställa att tillhandahållandet, aktiveringen och användningen av en plånbokslösning återupprättas, ska medlemsstaterna utan onödigt dröjsmål

(1) återupprätta tillhandahållandet och användningen av de plånboksenheter som tillhandahålls enligt den plånbokslösningen genom att utfärda en plånboksenhet som tillhandahålls enligt en ny version av plånbokslösningen till alla berörda användare,

(2) utfärda ett nytt plånboksenhetsintyg till nya plånboksenheter eller, i förekommande fall, till tidigare utfärdade plånboksenheter, under förutsättning att de plånboksenheterna uppfyller de gällande säkerhetskraven efter det att säkerhetsincidenten eller äventyrandet har åtgärdats,

(3) upphäva varje åtgärd som genomförts i enlighet med artikel 4 och som hindrar tillhandahållandet av nya plånboksenheter enligt den berörda plånbokslösningen, om en sådan åtgärd var kopplad endast till den säkerhetsincident eller det äventyrande som nu har åtgärdats.

Artikel 7

Information om återupprättandet

Om en medlemsstat återupprättar en plånbokslösning, ska den medlemsstaten säkerställa att

(1) information om detta utan onödigt dröjsmål tillhandahålls till alla parter som har mottagit information om det tillfälliga upphävandet av tillhandahållandet och användningen av den plånbokslösningen i enlighet med artikel 5.1,

(2) den information som tillhandahålls i enlighet med punkt (1) omfattar åtminstone de delar som avses i artikel 5.2 punkterna (a), (b) och (f)–(h) och följande:

a) Det datum och den tidpunkt då säkerhetsincidenten eller äventyrandet åtgärdades.

b) Datum och tidpunkten för återupprättandet av den berörda plånbokslösningen och, i förekommande fall, av de berörda plånbokslösningar som tillhandahållits enligt den plånbokslösningen,

c) Beskrivning av de åtgärder som har vidtagits för att åtgärda säkerhetsincidenten eller äventyrandet.

d) Beskrivning av den möjliga kvarstående inverkan på förlitande parter eller plånboksanvändare, och i det senare fallet, om detta är relevant, angivande av åtgärder som plånboksanvändarna kan vidta för att förmildra denna möjliga kvarstående inverkan.

Artikel 8

Återkallande av plånböcker

1. Om en säkerhetsincident eller ett äventyrande som har lett till det tillfälliga upphävandet av tillhandahållandet och användningen av en plånbokslösning inte åtgärdas inom tre månader efter datumet för det tillfälliga upphävandet av tillhandahållandet och användningen av den plånbokslösningen, ska den medlemsstat som tillhandahåller den plånbokslösningen säkerställa att den berörda plånbokslösningen återkallas och dess giltighet upphävs, utan onödigt dröjsmål och i alla händelser inom 72 timmar efter det att tremånadersperioden har löpt ut.

2. När en medlemsstat återkallar en plånbokslösning ska den säkerställa att

a) plånboksenhetsintygen tillhörande den berörda plånbokslösningens plånboksenheter upphävs,

b) plånboksenhetsintygen inte kan återställas till giltig status,

c) inget nytt plånboksenhetsintyg kan utfärdas till befintliga plånboksenheter som tillhandahålls under den berörda plånbokslösningen,

d) ingen ny plånboksenhet kan tillhandahållas under den berörda plånbokslösningen.

3. De åtgärder som anges i punkterna 1 och 2 ska inte hindra de berörda plånboksanvändarna från att utöva sin rätt till dataportabilitet i enlighet med artikel 5a.4 g i förordning (EU) nr 910/2014. Detta förutsätter att plånboksanvändarna kan utöva denna rätt utan att det påverkar säkerheten hos de berörda plånboksenheternas kritiska tillgångar, i synnerhet med beaktande av skälen till återkallandet och behovet av att säkerställa ett effektivt skydd av de tillgångarna mot missbruk.

Artikel 9

Information om tillbakadragandet

1. Information om återkallandet av en plånbokslösning ska tillhandahållas på ett tydligt, uttömmande och lättillgängligt sätt, utan onödigt dröjsmål och senast 24 timmar efter återkallandet av plånbokslösningen, till

a) de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i förordning (EU) nr 910/2014,

b) kommissionen,

c) de berörda plånboksanvändarna,

d) de förlitande parter som registrerats i enlighet med artikel 5b i förordning (EU) nr 910/2014.

2. Den information som tillhandahålls i enlighet med punkt 1 ska omfatta åtminstone följande:

a) Namnet på tillhandahållaren av den plånbokslösning som har återkallats.

b) Namnet och referensidentifieraren för den plånbokslösningen, i enlighet med uppgifterna i förteckningen över certifierade plånböcker som upprättats i enlighet med artikel 5d i förordning (EU) nr 910/2014 och, i förekommande fall, de berörda versionerna.

c) Dagen och tidpunkten för upptäckten av den säkerhetsincident eller det äventyrande som ledde till återkallandet av den berörda plånbokslösningen på grund av säkerhetsincidentens eller äventyrandets allvar eller på grund av att säkerhetsincidenten eller äventyrandet inte åtgärdades inom tre månader.

d) Om kända, det datum och den tidpunkt då säkerhetsincidenten eller äventyrandet ägde rum, på grundval av nätverks- eller systemloggar eller andra datakällor.

e) Dagen och tidpunkten för återkallandet av plånbokslösningen och det faktiska återkallandet av plånboksenhetsintygen tillhörande de plånboksenheter som tillhandahålls under plånbokslösningen.

f) Angivande av om återkallandet är ett resultat av säkerhetsincidentens eller äventyrandets allvar eller är en följd av att säkerhetsincidenten eller äventyrandet inte åtgärdats.

g) Kontaktuppgifter, inklusive åtminstone e-postadress och ett telefonnummer till den anmälande medlemsstaten och, om dessa skiljer sig åt, till den plånbokstillhandahållare som avses i punkt (a).

h) Beskrivning av säkerhetsincidenten eller äventyrandet.

i) Beskrivning av de uppgifter som äventyrats, inklusive, i förekommande fall, de kategorier av personuppgifter som anges i artikel 9.1 och artikel 10 i förordning (EU) 2016/679.

j) Om detta är möjligt, en uppskattning av antalet berörda plånboksanvändare och av andra berörda fysiska personer.

k) Beskrivning av den möjliga inverkan på förlitande parter eller plånboksanvändare, och i det senare fallet, om detta är relevant, angivande av åtgärder som plånboksanvändarna kan vidta för att förmildra denna möjliga inverkan.

l) Beskrivning av de åtgärder som vidtagits eller planeras för en omställning av berörda plånboksanvändare till alternativa plånbokslösningar eller, när så är tillämpligt och lämpligt, alternativa tjänster.

Artikel 10

Informationssystem

Medlemsstaterna ska sända den information som avses i artiklarna 3, 5, 7 och 9 till kommissionen och de gemensamma kontaktpunkter i medlemsstaterna som utsetts i enlighet med artikel 46c.1 i förordning (EU) nr 910/2014 via systemet för analys och rapportering av cyberincidenter, (*Cyber Incicent Reporting and Analysis System*, CIRAS) som drivs av Enisa, eller ett likvärdigt system som överenskommits av medlemstaterna och kommissionen.

Artikel 11

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning ska vara bindande i sin helhet och direkt tillämplig i alla medlemsstater, utom artikel 10, som ska tillämpas från och med 7 maj 2026.

Utfärdad i Bryssel den 6 maj 2025.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

Kriterier för bedömningen av en säkerhetsincident eller ett äventyrande

1. Medlemsstaterna ska grunda sin bedömning av en säkerhetsincident eller ett äventyrande på följande kriterier:

a) Incidenten eller äventyrandet har orsakat eller kan orsaka en fysisk persons dödsfall eller betydande skada för en fysisk persons hälsa.

b) En framgångsrik, misstänkt skadlig eller obehörig åtkomst till nätverks- och informationssystemen tillhörande en plånbokstillhandahållare, tillhörande en tillhandahållare av de valideringsmekanismer som avses i artikel 5a.8 i förordning (EU) nr 910/2014, eller tillhörande en tillhandahållare av det system för elektronisk identifiering under vilket en plånbokslösning tillhandahålls (*de berörda entiteterna*) har skett, eller kan ske, på ett sätt som kan orsaka allvarliga driftstörningar, och de systemen är kritiska komponenter i den berörda plånbokslösningen, i de berörda valideringsmekanismer som avses i artikel 5a.8 i förordning (EU) nr 910/2014 eller i det berörda system för elektronisk identifiering under vilket en plånbokslösning tillhandahålls.

c) En plånbokslösning, en valideringsmekanism som avses i artikel 5a.8 i förordning (EU) nr 910/2014, eller ett berört system för elektronisk identifiering under vilket en plånbokslösning tillhandahålls, eller en del av dem,

— är fullständigt eller prognostiseras bli fullständigt otillgängligt för plånboksanvändare eller förlitande parter i mer än 12 timmar i sträck,

— är otillgängligt eller prognostiseras bli otillgängligt för användare eller förlitande parter i mer än 16 timmar beräknat per kalendervecka.

d) Det misstänks att mer än 1 % av plånboksanvändarna eller av de förlitande parterna berörs eller prognostiseras bli berörda av en begränsad tillgänglighet hos en plånbokslösning, eller hos de tjänster som tillhandahålls av de berörda enheterna med avseende på plånbokslösningen.

e) Det kan ske ett äventyrande eller det har skett ett äventyrande av en fysisk åtkomst begränsad till betrodd personal i de berörda entiteterna, eller av skyddet av sådan fysisk åtkomst, till en eller flera platser i de nätverks- och informationssystem som stöder plånbokslösningen, tillhandahållandet av de valideringsmekanismer som avses i artikel 5a.8 i förordning (EU) nr 910/2014 associerade med plånbokslösningen, eller det system för elektronisk identifiering under vilket en plånbokslösning tillhandahålls.

f) Skyddet, integriteten, konfidentialiteten eller autenticiteten för de uppgifter som lagras, överförs eller behandlas i plånbokslösningarna äventyras, eller kan äventyras, på ett eller flera av följande sätt:

— Det berör mer än 1 % av plånboksanvändarna av den berörda plånbokslösningen eller mer än 100 000 av de plånboksanvändarna, beroende på vilket antal som är lägst.

— Det är ett resultat av en framgångsrik, misstänkt skadlig verksamhet.

— Det är resultatet av eller kommer sannolikt bli resultatet av mer kända sårbarheter, inbegripet de som behandlas i enlighet med kommissionens genomförandeförordning (EU) 2024/2981 ([1]).

— Det kommer sannolikt påverka personuppgifter på ett sätt som sannolikt kommer att resultera i en risk för berörda fysiska personers rättigheter och friheter, i synnerhet, i händelse av personuppgiftsincidenter i enlighet med artiklarna 9.1 och 10 i förordning (EU) 2016/679.

([1]) Kommissionens genomförandeförordning (EU) 2024/2981 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller certifiering av EU:s digitala identitetsplånböcker (EUT L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— Det kommer sannolikt påverka personlig elektronisk kommunikation.

— Det kommer sannolikt resultera i en hög risk för fysiska personers rättigheter och friheter.

— Det kommer sannolikt påverka sårbara fysiska personer.

g) Certifieringen av plånbokslösningen har annullerats eller prognostiseras bli annullerad.

h) Incidenten har orsakat eller kan orsaka en direkt ekonomisk förlust för den berörda entiteten som överstiger 500 000 euro eller, i tillämpliga fall, 5 % av den berörda entitetens totala årsomsättning under föregående räkenskapsår, beroende på vilket som är lägst.

2. Medlemsstaterna ska inte beakta planerade konsekvenser av underhåll som utförts av eller på uppdrag av de berörda entiteterna, förutsatt att

a) potentiellt påverkade användare har underrättats om det underhållet i förväg,

b) det underhållet inte uppfyller kriterierna i punkt 1 i denna bilaga.

3. När det gäller led (c) i punkt 1 ska varaktigheten hos en incident som påverkar tillgängligheten mätas från den tidpunkt då det faktiska tillhandahållandet av den påverkade tjänsten avbröts till den tidpunkt då tjänsten återupprättades och är i drift igen. Om en berörd entitet inte kan fastställa det ögonblick då störningen inleddes, ska incidentens varaktighet mätas från det ögonblick då incidenten upptäcktes eller från det ögonblick då incidenten registrerades i nätverks- eller systemloggar eller andra datakällor, beroende på vilket som inträffar först. Total otillgänglighet till en tjänst ska mätas från det ögonblick då tjänsten blir helt otillgänglig för användare till det ögonblick då reguljär verksamhet eller drift har återställts till den tjänstenivå som tillhandahölls före incidenten. Om en berörd entitet inte kan fastställa när en tjänsts totala otillgänglighet inleddes, ska otillgängligheten mätas från det ögonblick då den upptäcktes av den entiteten.

4. När det gäller led (d) i punkt 1 anses begränsad tillgänglighet förekomma i synnerhet om en tjänst är betydligt långsammare än den genomsnittliga svarstiden eller om inte alla funktioner hos en tjänst är tillgängliga. När så är möjligt ska objektiva kriterier baserade på den genomsnittliga svarstiden för tjänster användas vid bedömningen av fördröjd svarstid.

5. För att fastställa de direkta ekonomiska förlusterna till följd av en incident eller ett äventyrande enligt punkt 1 (h) ska de berörda entiteterna ta hänsyn till alla ekonomiska förluster som orsakats till följd av incidenten, såsom kostnaderna för utbyte eller omlokalisering av programvara, maskinvara eller infrastruktur, personalkostnader – inklusive kostnader i samband med ersättning eller omplacering av personal, rekrytering av extra personal, övertidsersättning och återställande av förlorad eller försämrad kompetens, avgifter på grund av att avtalsförpliktelserna inte har fullgjorts, kostnader för gottgörelse och ersättning till kunder, förluster på grund av uteblivna intäkter, kostnader för intern och extern kommunikation och rådgivningskostnader, inklusive kostnader i samband med juridisk rådgivning, kriminaltekniska tjänster och saneringstjänster. Kostnader som är nödvändiga för den dagliga driften av verksamheten, såsom kostnader för allmänt underhåll av infrastruktur, utrustning, maskin- och programvara, förbättringar och riskbedömningsåtgärder, och försäkringspremier ska inte anses som ekonomiska förluster till följd av en incident. De berörda entiteterna ska beräkna de ekonomiska förlustbeloppen på grundval av tillgängliga uppgifter, och om de faktiska ekonomiska förlustbeloppen inte kan fastställas ska de entiteterna göra en uppskattning.