2025/847

7.5.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/847

af 6. maj 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår reaktioner på sikkerhedsbrud i europæiske digitale identitetstegnebøger

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 5e, stk. 5, og

ud fra følgende betragtninger:

(1) Den europæiske ramme for digital identitet (»rammen«), der blev oprettet ved forordning (EU) nr. 910/2014, er et afgørende element i etableringen af et sikkert og interoperabelt økosystem for digital identitet i hele Unionen. Med de europæiske digitale identitetstegnebøger (»tegnebøger«) som hjørnesten har rammen til formål at lette adgangen til tjenester i alle medlemsstater og samtidig sikre beskyttelsen af personoplysninger og privatlivets fred.

(2) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([2]) og forordning (EU) 2018/1725 ([3]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([4]) finder anvendelse på behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning. De regler om vurdering og information, der fastsættes i henhold til nærværende forordning, berører ikke forpligtelsen til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, hvor det er relevant i henhold til forordning (EU) 2016/679 eller forordning (EU) 2018/1725, og forpligtelsen til at underrette registrerede om brud på persondatasikkerheden, hvor det er relevant i henhold til nævnte forordninger.

(3) Kommissionen vurderer regelmæssigt nye teknologier, praksisser, standarder og tekniske specifikationer. For at sikre den højeste grad af harmonisering mellem medlemsstaterne med hensyn til udvikling og certificering af tegnebøgerne er de tekniske specifikationer, der er fastsat i nærværende forordning, baseret på det arbejde, der er udført i henhold til Kommissionens henstilling (EU) 2021/946 ([5]), og navnlig den tekniske struktur og referencerammen, som er en del heraf. I overensstemmelse med betragtning 75 i Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([6]) bør Kommissionen revidere og om nødvendigt ajourføre nærværende forordning for at sikre, at den er i overensstemmelse med den globale udvikling, den tekniske struktur og referencerammen og følger bedste praksis på det indre marked.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Kommissionens henstilling (EU) 2021/946 af 3. juni 2021 om en fælles EU-værktøjskasse for en koordineret tilgang til en ramme for en europæisk digital identitet (EUT L 210 af 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) I tilfælde af sikkerhedsbrud i eller kompromitteringer af tegnebogsløsningerne eller de valideringsmekanismer, der er omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014, eller den elektroniske identifikationsordning, efter hvilken tegnebogsløsningerne leveres, skal reaktionerne på disse sikkerhedsbrud og kompromitteringer ske hurtigt, koordineret og på sikker vis i alle medlemsstater for at beskytte brugerne og opretholde tilliden til økosystemet for digital identitet. Dette berører ikke Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([7]) og Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([8]) og forordning (EU) 2024/2847 ([9]), især for så vidt angår håndteringen af hændelser eller sårbarheder og kategoriseringen af dem som sikkerhedsbrud. Medlemsstaterne bør derfor sikre, at leveringen og anvendelsen af tegnebøger, der er berørt af et sikkerhedsbrud eller en kompromittering, suspenderes rettidigt, eller, hvis det er relevant, at tegnebøgerne trækkes tilbage.

(5) For at sikre passende reaktioner på sikkerhedsbrud eller kompromitteringer bør medlemsstaterne vurdere, om et sikkerhedsbrud i eller en kompromittering af en tegnebogsløsning, de valideringsmekanismer, der er omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014, eller den elektroniske identifikationsordning, efter hvilken en tegnebogsløsning leveres, påvirker pålideligheden af den pågældende tegnebogsløsning eller af andre tegnebogsløsninger. Vurderingen bør baseres på ensartede kriterier såsom antallet og kategorien af tegnebogsbrugere, fysiske personer og berørte tegnebogsmodtagere, karakteren af de berørte data, varigheden af kompromitteringen eller sikkerhedsbruddet, en tjenestes begrænsede tilgængelighed og de økonomiske tab samt den potentielle kompromittering af personoplysninger. Disse kriterier bør give medlemsstaterne fleksibilitet og skønsbeføjelse til på en forholdsmæssig måde at fastslå, om pålideligheden af en tegnebogsløsning er påvirket, og om det er hensigtsmæssigt at suspendere eller, hvis det er begrundet af bruddets eller kompromitteringens alvor, tilbagetrække tegnebogsløsningen. Kriterierne bør ikke udløse en automatisk tilbagetrækning af en tegnebogsløsning eller en automatisk suspension af leveringen og anvendelsen af en tegnebogsløsning, men medlemsstaterne bør tage dem behørigt i betragtning, når de afgør, det er nødvendigt at trække en tegnebogsløsning tilbage eller suspendere leveringen og anvendelsen af den.

(6) På grund af konsekvenserne og ulemperne ved at suspendere anvendelsen af tegnebogsløsninger vil medlemsstaterne skulle vurdere, om det er nødvendigt at tilbagekalde tegnebogsenhedsattesteringer eller træffe andre yderligere foranstaltninger for at reagere hensigtsmæssigt på sikkerhedsbruddet eller kompromitteringen.

(7) For at holde tegnebogsbrugerne informeret om status for deres tegnebøger, skal de have tilstrækkelig information om sikkerhedsbrud eller kompromitteringer, der påvirker deres tegnebøger. Da tegnebogsmodtagere, der er registreret i Unionen, også kan blive berørt af sikkerhedsbrud og kompromitteringer, skal den relevante information om sikkerhedsbrud og kompromitteringer også deles med dem.

(8) For at fremme gennemsigtigheden og opbygge tillid til økosystemet for digital identitet bør den information, der skal gives om sikkerhedsbrud og kompromitteringer og konsekvenserne heraf, som minimum omfatte de oplysninger, der kræves i henhold til nærværende forordning. De oplysninger om sikkerhedsbrud eller kompromitteringer, der deles med tegnebogsbrugerne og tegnebogsmodtagerne, bør imidlertid vurderes nøje for at forebygge og minimere risikoen for, at de udnyttes af angribere.

([7]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) For at give brugerne mulighed for at få adgang til deres tegnebogsenheder igen, efter at et sikkerhedsbrud eller en kompromittering er blevet afhjulpet, skal den medlemsstat, der leverede tegnebogsløsningerne, genoprette leveringen og anvendelsen af de pågældende tegnebogsløsninger uden unødigt ophold. Dette kan gøres ved at genoprette tegnebogsenhederne, ved at udstede tegnebogsenheder, der leveres under en ny version af tegnebogsløsningerne, eller ved at udstede nye gyldige tegnebogsenhedsattesteringer. De berørte tegnebogsbrugere og tegnebogsmodtagere, de centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, i forordning (EU) nr. 910/2014, og Kommissionen skal underrettes herom.

(10) For at sikre, at tegnebøgerne trækkes tilbage, når et sikkerhedsbrud eller en kompromittering ikke er blevet afhjulpet inden for tre måneder efter suspensionen, eller hvis tilbagetrækningen er begrundet af sikkerhedsbruddets eller kompromitteringens alvor, bør medlemsstaten sikre, at de relevante tegnebogsenhedsattesteringer tilbagekaldes, og at de ikke kan genoprettes til en gyldig tilstand eller udstedes eller leveres til eksisterende tegnebogsenheder. Desuden bør der ikke leveres nye tegnebogsenheder under den berørte tegnebogsløsning. Af hensyn til gennemsigtigheden skal brugerne, tegnebogsmodtagerne, de centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, i forordning (EU) nr. 910/2014, og Kommissionen underrettes om tilbagetrækningen. Dette omfatter en redegørelse for de potentielle virkninger for tegnebogsbrugerne, og navnlig for forvaltningen af udstedte attesteringer, eller for tegnebogsmodtagerne.

(11) Den periode på tre måneder efter suspensionen af leveringen og anvendelsen af en tegnebogsløsning, som det sikkerhedsbrud eller den kompromittering, der førte til suspensionen, skal afhjælpes inden for, bør udgøre en frist, efter hvilken tegnebogsløsningen skal trækkes tilbage, medmindre der er truffet passende afhjælpende foranstaltninger. Medlemsstaterne kan dog frit kræve, at sikkerhedsbruddet eller kompromitteringen skal afhjælpes inden for en frist, der er kortere end tre måneder, navnlig og hvis det er relevant, under hensyntagen til omfanget, varigheden og konsekvenserne af sikkerhedsbruddet eller kompromitteringen. Hvis sikkerhedsbruddet eller kompromitteringen ikke er eller ikke kan afhjælpes inden for den frist, som medlemsstaten har fastsat, kan medlemsstaten kræve, at tegnebogsløsningen trækkes tilbage inden udløbet af perioden på tre måneder. Medlemsstaterne bør benytte denne periode, hvor et sikkerhedsbrud eller en kompromittering, der har ført til suspension af leveringen og anvendelsen af en tegnebogsløsning, skal afhjælpes, til at forberede den eventuelle tilbagetrækning af tegnebogsløsningen og meddelelserne i den forbindelse.

(12) For at mindske den administrative byrde for medlemsstaterne med hensyn til de oplysninger, der i overensstemmelse med nærværende forordning skal gives til Kommissionen og til andre medlemsstater, bør medlemsstaterne anvende eksisterende underretningsværktøjer såsom systemet til indberetning og analyse af cyberhændelser (»CIRAS«), der drives af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«). Med hensyn til alternative kanaler eller midler til at informere de tegnebogsbrugere, der er berørt af et sikkerhedsbrud eller en kompromittering, og tegnebogsmodtagerne bør medlemsstaterne sikre, at de relevante oplysninger gives på en klar, fyldestgørende og lettilgængelig måde. Kanalerne til at give disse oplysninger til de berørte tegnebogsbrugere og tegnebogsmodtagerne, bør omfatte passende løsninger til webstedsbaseret udsendelse, realtidssporing af webstedsopdateringer og nyhedsaggregering.

(13) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav udtalelse den 31. januar 2025.

(14) Foranstaltningerne i nærværende forordning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

Ved denne forordning fastsættes der regler for reaktioner på sikkerhedsbrud i tegnebøgerne, de valideringsmekanismer, der er omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014, og den elektroniske identifikationsordning, efter hvilken tegnebøgerne leveres.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) »tegnebogsløsning«: en kombination af software, hardware, tjenester, indstillinger og konfigurationer, herunder tegnebogsforekomster, en eller flere sikre kryptografiske tegnebogsapplikationer og en eller flere sikre kryptografiske tegnebogsanordninger

2) »tegnebogsbruger«: en bruger, der har kontrol over tegnebogsenheden

3) »tegnebogsmodtager«: en modtagerpart, der har til hensigt at benytte tegnebogsenheder til levering af offentlige eller private tjenester ved hjælp af digital interaktion

4) »tegnebogsforekomst«: den applikation, der er installeret og konfigureret på en tegnebogsbrugers enhed eller miljø, som er en del af en tegnebogsenhed, og som tegnebogsbrugeren bruger til at interagere med tegnebogsenheden

5) »sikker kryptografisk tegnebogsapplikation«: en applikation, der forvalter kritiske aktiver ved at være knyttet til og anvende de kryptografiske og ikkekryptografiske funktioner, der leveres af en sikker kryptografisk tegnebogsanordning

6) »sikker kryptografisk tegnebogsanordning«: en anordning, der er sikret mod manipulation, og som tilvejebringer et miljø, der er knyttet til og anvendes af den sikre kryptografiske tegnebogsapplikation til at beskytte kritiske aktiver og tilvejebringe kryptografiske funktioner til sikker udførelse af kritiske operationer

7) »tegnebogsudbyder«: en fysisk eller juridisk person, der leverer tegnebogsløsninger

8) »tegnebogsenhed«: en unik konfiguration af en tegnebogsløsning, der omfatter tegnebogsforekomster, sikre kryptografiske tegnebogsapplikationer og sikre kryptografiske tegnebogsanordninger, som en tegnebogsudbyder leverer til en individuel tegnebogsbruger

9) »kritiske aktiver«: aktiver i eller i forbindelse med en tegnebogsenhed af så ekstraordinær betydning, at det i alvorlig grad vil svække muligheden for at have tillid til tegnebogsenheden, hvis deres tilgængelighed, fortrolighed eller integritet kompromitteres

10) »attestering af tegnebogsenhed« og »tegnebogsenhedsattestering«: et dataobjekt, der beskriver tegnebogsenhedens komponenter eller gør det muligt at autentificere og validere disse komponenter.

Artikel 3

Konstatering af et sikkerhedsbrud eller en kompromittering

1. Uden at det berører direktiv (EU) 2022/2555 og forordning (EU) 2019/881 og (EU) 2024/2847, tager medlemsstaterne behørigt hensyn til kriterierne i bilag I til nærværende forordning for at vurdere, om et sikkerhedsbrud i eller en kompromittering af en tegnebogsløsning, de valideringsmekanismer, der er omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014, eller den elektroniske identifikationsordning, efter hvilken tegnebogsløsningen leveres, påvirker deres pålidelighed eller andre tegnebogsløsningers pålidelighed.

2. Hvis en medlemsstat på grundlag af vurderingen i stk. 1 fastslår, at et sikkerhedsbrud eller en kompromittering påvirker pålideligheden af en tegnebogsløsning, og suspenderer leveringen og anvendelsen af den pågældende tegnebogsløsning, træffer den pågældende medlemsstat de foranstaltninger, der er fastsat i artikel 4 og 5. Hvis en medlemsstat trækker tegnebogsløsningen tilbage, træffer medlemsstaten de foranstaltninger, der er fastsat i artikel 8 og 9.

3. Når en medlemsstat bliver bekendt med oplysninger om et muligt sikkerhedsbrud eller en mulig kompromittering, der muligvis påvirker pålideligheden af en eller flere tegnebogsløsninger, der leveres af en anden medlemsstat, giver den pågældende medlemsstat uden unødigt ophold meddelelse herom til Kommissionen og de berørte medlemsstaters centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, i forordning (EU) nr. 910/2014. Meddelelsen skal indeholde de oplysninger, der er omhandlet i artikel 5, stk. 2.

4. En medlemsstat, der modtager oplysninger, der er givet efter stk. 3, træffer uden unødigt ophold de foranstaltninger, der er fastsat i stk. 1 og 2.

Artikel 4

Suspension af leveringen og anvendelsen af tegnebøger og andre afhjælpende foranstaltninger

1. Medlemsstaterne sikrer, at ingen tegnebogsenheder leveres, anvendes eller aktiveres under den suspenderede tegnebogsløsning.

2. Medlemsstaterne vurderer, om det er nødvendigt at tilbagekalde tegnebogsenhedsattesteringer for de tegnebogsenheder, der er berørt af suspensionen af en tegnebogsløsning, eller træffe andre afhjælpende foranstaltninger for at reagere hensigtsmæssigt på sikkerhedsbruddet eller kompromitteringen.

3. Foranstaltningerne i stk. 1 og 2 træffes uden unødigt ophold og under alle omstændigheder senest 24 timer efter suspensionen af leveringen og anvendelsen af den tegnebogsløsning, der er berørt af sikkerhedsbruddet eller kompromitteringen.

4. Foranstaltningerne i stk. 1 og 2 må ikke hindre berørte tegnebogsbrugere i at udøve deres ret til dataportabilitet, jf. artikel 5a, stk. 4, litra g), i forordning (EU) nr. 910/2014. Dette er under forudsætning af, at tegnebogsbrugerne kan udøve denne ret, uden at det forringer de berørte tegnebogsenheders kritiske aktivers sikkerhed, navnlig under hensyntagen til årsagerne til suspensionen og behovet for at sikre en effektiv beskyttelse af sådanne aktiver mod misbrug.

Artikel 5

Information om suspensioner og afhjælpende foranstaltninger

1. Der gives information på en klar, fyldestgørende og lettilgængelig måde om suspension af leveringen og anvendelsen af en tegnebogsløsning uden unødigt ophold og senest 24 timer efter suspensionen af leveringen og anvendelsen af tegnebogsløsningen til:

a) de centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, i forordning (EU) nr. 910/2014

b) Kommissionen

c) de berørte tegnebogsbrugere

d) de tegnebogsmodtagere, der er registreret i overensstemmelse med artikel 5b i forordning (EU) nr. 910/2014.

2. Den information, der gives i overensstemmelse med stk. 1, skal som minimum omfatte følgende:

a) navnet på udbyderen af den tegnebogsløsning, hvis levering og anvendelse er blevet suspenderet

b) navnet på og referenceidentifikatoren for den pågældende tegnebogsløsning som angivet på den liste over certificerede tegnebøger, der er udarbejdet i henhold til artikel 5d i forordning (EU) nr. 910/2014, og, hvis det er relevant, de berørte versioner

c) dato og klokkeslæt, hvor sikkerhedsbruddet eller kompromitteringen blev opdaget

d) dato og klokkeslæt, hvis disse er kendt, for, hvornår sikkerhedsbruddet eller kompromitteringen indtraf, baseret på net- eller systemlogfiler eller andre datakilder

e) dato og klokkeslæt for suspensionen af tegnebogsløsningen

f) kontaktoplysninger, herunder som minimum en e-mailadresse og et telefonnummer for den anmeldende medlemsstat og for den tegnebogsudbyder, der er omhandlet i litra (a), hvis disse ikke er den samme

g) en beskrivelse af sikkerhedsbruddet eller kompromitteringen

h) en beskrivelse af de kompromitterede data, herunder, hvis det er relevant, kategorierne af personoplysninger som fastsat i artikel 9, stk. 1, og artikel 10 i forordning (EU) 2016/679

i) hvis det er muligt, et skøn over det omtrentlige antal berørte tegnebogsbrugere og over andre berørte fysiske personer

j) en redegørelse for de potentielle virkninger for tegnebogsmodtagerne eller tegnebogsbrugerne og for sidstnævntes vedkommende, hvis det er relevant, en angivelse af, hvilke foranstaltninger tegnebogsbrugerne kan træffe for at afbøde disse potentielle virkninger

k) en redegørelse for de foranstaltninger, der er truffet eller planlagt for at afhjælpe sikkerhedsbruddet eller kompromitteringen, sammen med en plan og frist for afhjælpningen

l) hvis det er relevant og hensigtsmæssigt, en redegørelse for de foranstaltninger, der er truffet eller planlagt for at overflytte de berørte tegnebogsbrugere til alternative tegnebogsløsninger eller tjenester.

Artikel 6

Genoprettelse af leveringen og anvendelsen af tegnebøger

Hvis det er nødvendigt for at genoprette leveringen, aktiveringen og anvendelsen af en tegnebogsløsning, skal medlemsstaterne uden unødigt ophold:

1) genoprette leveringen og anvendelsen af de tegnebogsenheder, der leveres under den pågældende tegnebogsløsning, ved at udstede en tegnebogsenhed, der leveres under en ny version af tegnebogsløsningen, til alle berørte brugere

2) udstede nye tegnebogsenhedsattesteringer til nye tegnebogsenheder eller, hvis det er relevant, til tidligere udstedte tegnebogsenheder, forudsat at disse tegnebogsenheder opfylder de sikkerhedskrav, der gælder efter afhjælpningen af sikkerhedsbruddet eller kompromitteringen

3) ophæve enhver foranstaltning, der er gennemført i henhold til artikel 4, og som hindrer leveringen af nye tegnebogsenheder under den berørte tegnebogsløsning, hvis denne foranstaltning udelukkende var knyttet til det sikkerhedsbrud eller den kompromittering, der nu er afhjulpet.

Artikel 7

Information om genoprettelse

Når en medlemsstat genopretter en tegnebogsløsning, sikrer medlemsstaten, at:

1) information om dette forhold gives uden unødigt ophold til alle parter, der er blevet informeret om suspensionen af leveringen og anvendelsen af den pågældende tegnebogsløsning i overensstemmelse med artikel 5, stk. 1

2) den information, der gives i henhold til punkt 1, som minimum omfatter de elementer, der er omhandlet i artikel 5, stk. 2, litra a), b) og f)-h), samt følgende oplysninger:

   a) dato og klokkeslæt, hvor sikkerhedsbruddet eller kompromitteringen blev afhjulpet

   b) dato og klokkeslæt for genoprettelsen af den berørte tegnebogsløsning og, hvis det er relevant, af de berørte tegnebogsenheder, der leveres under den pågældende tegnebogsløsning

   c) en redegørelse for de foranstaltninger, der er truffet for at afhjælpe sikkerhedsbruddet eller kompromitteringen

   d) en redegørelse for eventuelle resterende virkninger for tegnebogsmodtagerne eller tegnebogsbrugerne og for sidstnævntes vedkommende, hvis det er relevant, en angivelse af, hvilke foranstaltninger tegnebogsbrugerne kan træffe for at afbøde disse potentielle resterende virkninger

Artikel 8

Tilbagetrækning af tegnebøger

1. Hvis et sikkerhedsbrud eller en kompromittering, der har ført til suspension af leveringen og anvendelsen af en tegnebogsløsning, ikke er afhjulpet senest tre måneder efter datoen for suspensionen af leveringen og anvendelsen af tegnebogsløsningen, sikrer den medlemsstat, der leverer tegnebogsløsningen, at den berørte tegnebogsløsning trækkes tilbage, og at dens gyldighed tilbagekaldes, uden unødigt ophold og under alle omstændigheder senest 72 timer efter udløbet af perioden på tre måneder.

2. Når en medlemsstat trækker en tegnebogsløsning tilbage, sikrer den, at:

a) tegnebogsenhedsattesteringerne for tegnebogsenheden i den berørte tegnebogsløsning tilbagekaldes

b) tegnebogsenhedsattesteringerne ikke kan gendannes til en gyldig tilstand

c) der ikke kan udstedes nye tegnebogsenhedsattesteringer til eksisterende tegnebogsenheder, der leveres under den berørte tegnebogsløsning

d) der ikke kan leveres en ny tegnebogsenhed under den berørte tegnebogsløsning.

3. Foranstaltningerne i stk. 1 og 2 må ikke hindre de berørte tegnebogsbrugere i at udøve deres ret til dataportabilitet, jf. artikel 5a, stk. 4, litra g), i forordning (EU) nr. 910/2014. Dette er under forudsætning af, at tegnebogsbrugerne kan udøve denne ret, uden at det forringer de berørte tegnebogsenheders kritiske aktivers sikkerhed, navnlig under hensyntagen til årsagerne til tilbagetrækningen og behovet for at sikre en effektiv beskyttelse af sådanne aktiver mod misbrug.

Artikel 9

Information om tilbagetrækning

1. Information om tilbagetrækningen af en tegnebogsløsning gives på en klar, fyldestgørende og lettilgængelig måde uden unødigt ophold og senest 24 timer efter tilbagetrækningen af tegnebogsløsningen til:

a) de centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, i forordning (EU) nr. 910/2014

b) Kommissionen

c) de berørte tegnebogsbrugere

d) de tegnebogsmodtagere, der er registreret i overensstemmelse med artikel 5b i forordning (EU) nr. 910/2014.

2. Den information, der gives i henhold til stk. 1, skal som minimum omfatte følgende oplysninger:

a) navnet på udbyderen af den tegnebogsløsning, der er blevet trukket tilbage

b) navnet på og referenceidentifikatoren for den pågældende tegnebogsløsning, som angivet på den liste over certificerede tegnebøger, der er udarbejdet i henhold til artikel 5d i forordning (EU) nr. 910/2014, og, hvis det er relevant, de berørte versioner

c) dato og klokkeslæt for opdagelsen af det sikkerhedsbrud eller den kompromittering, der på grund af sin alvor eller manglende afhjælpning inden for tre måneder har ført til tilbagetrækningen af den berørte tegnebogsløsning

d) dato og klokkeslæt, hvis disse er kendt, for, hvornår sikkerhedsbruddet eller kompromitteringen indtraf, baseret på net- eller systemlogfiler eller andre datakilder

e) dato og klokkeslæt for tilbagetrækningen af tegnebogsløsningen og for den faktiske tilbagekaldelse af tegnebogsenhedsattesteringerne for de tegnebogsenheder, der leveres under tegnebogsløsningen

f) om tilbagetrækningen skyldes alvoren af sikkerhedsbruddet eller kompromitteringen eller er en konsekvens af, at sikkerhedsbruddet eller kompromitteringen ikke er blevet afhjulpet

g) kontaktoplysninger, herunder som minimum en e-mailadresse og et telefonnummer for den anmeldende medlemsstat og for den tegnebogsudbyder, der er omhandlet i litra (a), hvis disse ikke er den samme

h) en beskrivelse af sikkerhedsbruddet eller kompromitteringen

i) en beskrivelse af de kompromitterede data, herunder, hvis det er relevant, kategorierne af personoplysninger som specificeret i artikel 9, stk. 1, og artikel 10 i forordning (EU) 2016/679

j) hvis det er muligt, et skøn over det omtrentlige antal berørte tegnebogsbrugere og over andre berørte fysiske personer

k) en redegørelse for de potentielle virkninger for tegnebogsmodtagerne eller tegnebogsbrugerne og for sidstnævntes vedkommende, hvis det er relevant, en angivelse af, hvilke foranstaltninger tegnebogsbrugerne kan træffe for at afbøde disse potentielle virkninger

l) en redegørelse for de foranstaltninger, der er truffet eller planlagt for at overflytte de berørte tegnebogsbrugere til alternative tegnebogsløsninger eller, hvor det er relevant og hensigtsmæssigt, alternative tjenester.

Artikel 10

Informationssystem

Medlemsstaterne sender den information, der er omhandlet i artikel 3, 5, 7 og 9, til Kommissionen og medlemsstaternes centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, i forordning (EU) nr. 910/2014, via CIRAS, som drives af ENISA, eller et tilsvarende system som aftalt mellem medlemsstaterne og Kommissionen.

Artikel 11

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i alle medlemsstater, med undtagelse af artikel 10, som finder anvendelse fra den 7. maj 2026.

Udfærdiget i Bruxelles, den 6. maj 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

Kriterier for vurdering af et sikkerhedsbrud eller en kompromittering

1. Medlemsstaterne baserer deres vurdering af et sikkerhedsbrud eller en kompromittering på følgende kriterier:

a) bruddet eller kompromitteringen har forårsaget eller i stand til at forårsage en fysisk persons død eller betydelig skade på en fysisk persons helbred

b) der er opnået eller kan opnås formodet ondsindet eller uautoriseret adgang til net- og informationssystemerne hos en tegnebogsudbyder, en udbyder af valideringsmekanismer som omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014 eller en udbyder af den elektroniske identifikationsordning, efter hvilken en tegnebogsløsning leveres (»berørte enheder«), på en måde, der kan forårsage alvorlige driftsforstyrrelser, og disse systemer er kritiske komponenter i den berørte tegnebogsløsning, de berørte valideringsmekanismer som omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014 eller den berørte elektroniske identifikationsordning, efter hvilken en tegnebogsløsning leveres

c) en tegnebogsløsning, en valideringsmekanisme som omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014 eller en elektronisk identifikationsordning, efter hvilken en tegnebogsløsning leveres, eller en del af dem:

— er helt eller forventes at være helt utilgængelig for tegnebogsbrugerne eller tegnebogsmodtagerne i mere end 12 på hinanden følgende timer

— er utilgængelig eller forventes at være utilgængelig for tegnebogsbrugerne eller tegnebogsmodtagerne i mere end 16 timer beregnet på kalenderugebasis.

d) der er mistanke om, at mere end 1 % af tegnebogsbrugerne eller tegnebogsmodtagerne er berørt eller forventes at blive berørt af den begrænsede tilgængelighed af tegnebogsløsningen eller af de tjenester, der leveres af de berørte enheder for så vidt angår tegnebogsløsningen

e) der er mulighed for kompromittering, eller der er sket kompromittering, af fysisk adgang, der er begrænset til betroet personale hos de berørte enheder, eller af beskyttelsen af en sådan fysisk adgang, til en eller flere lokationer for de net- og informationssystemer, der understøtter tegnebogsløsningen, leveringen af de valideringsmekanismer som omhandlet i artikel 5a, stk. 8, i forordning (EU) nr. 910/2014, der er knyttet til en tegnebogsløsning, eller den elektroniske identifikationsordning, efter hvilken en tegnebogsløsning leveres

f) sikkerheden, integriteten, fortroligheden eller ægtheden af data, der er lagret, overført eller behandlet i tegnebogsløsningen er kompromitteret eller kan blive kompromitteret på en eller flere af følgende måder:

— kompromitteringen påvirker mere end 1 % af tegnebogsbrugerne af den berørte tegnebogsløsning eller mere end 100 000 af disse tegnebogsbrugere, alt efter hvilket antal der er lavest

— kompromitteringen er et resultat af en formodet ondsindet aktivitet

— kompromitteringen er et resultat eller sandsynligvis et resultat af en eller flere kendte sårbarheder, herunder sårbarheder, der håndteres i overensstemmelse med Kommissionens gennemførelsesforordning (EU) 2024/2981 ([1])

— kompromitteringen vil sandsynligvis påvirke personoplysninger på en måde, der sandsynligvis vil medføre en risiko for de berørte fysiske personers rettigheder og frihedsrettigheder, navnlig i tilfælde af brud på persondatasikkerheden som omhandlet i artikel 9, stk. 1, og artikel 10 i forordning (EU) 2016/679

([1]) Kommissionens gennemførelsesforordning (EU) 2024/2981 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår certificering af europæiske digitale identitetstegnebøger (EUT L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— kompromitteringen vil sandsynligvis påvirke personlig elektronisk kommunikation

— kompromitteringen vil sandsynligvis medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

— kompromitteringen vil sandsynligvis påvirke sårbare fysiske personer

g) certificeringen af tegnebogsløsningen er blevet annulleret eller forventes at blive annulleret

h) bruddet eller kompromitteringen har forårsaget eller er i stand til at forårsage direkte økonomiske tab for en berørt enhed, og disse tab overstiger 500 000 EUR eller, hvis det er relevant, 5 % af den berørte enheds samlede årsomsætning i det foregående regnskabsår, alt efter hvilket tal der er lavest.

2. Medlemsstaterne tager ikke planlagte konsekvenser af en vedligeholdelsesopgave, der udføres af eller på vegne af de berørte enheder, i betragtning, forudsat at en sådan vedligeholdelsesopgave:

a) på forhånd er blevet meddelt potentielt berørte tegnebogsbrugere, tegnebogsmodtagere og de relevante kompetente tilsynsorganer

b) ikke opfylder nogen af kriterierne i dette bilags punkt 1.

3. Med hensyn til punkt 1, litra (c), måles varigheden af en hændelse, der påvirker tilgængeligheden, fra det tidspunkt, hvor den korrekte levering af den berørte tjeneste forstyrres eller afbrydes, til det tidspunkt, hvor tjenesten genoprettes og sættes i drift igen. Hvis en berørt enhed ikke er i stand til at fastslå, hvornår forstyrrelsen eller afbrydelsen indtraf, måles hændelsens varighed fra det tidspunkt, hvor hændelsen blev opdaget, eller fra det tidspunkt, hvor hændelsen blev registreret i net- eller systemlogfiler eller andre datakilder, alt efter hvad der skete først. Fuldstændig utilgængelighed af en tjeneste måles fra det tidspunkt, hvor tjenesten er helt utilgængelig for brugerne, til det tidspunkt, hvor regelmæssige aktiviteter eller regelmæssig drift genoprettes til det serviceniveau, der blev leveret forud for hændelsen. Hvis en berørt enhed ikke er i stand til at fastslå, hvornår den fuldstændige utilgængelighed af en tjeneste indtraf, måles utilgængeligheden fra det tidspunkt, hvor den pågældende enhed opdagede den.

4. Med hensyn til punkt 1, litra (d), anses en tjeneste for at have begrænset tilgængelighed, navnlig når tjenesten er betydeligt langsommere end den gennemsnitlige svartid, eller når ikke alle tjenestens funktioner er tilgængelige. Hvor det er muligt, skal der til at vurdere forsinkelser i svartiden anvendes objektive kriterier baseret på tjenesters gennemsnitlige svartider.

5. For at fastslå de direkte økonomiske tab som følge af et sikkerhedsbrud eller en kompromittering, jf. punkt 1, litra (h), tager de berørte enheder alle økonomiske tab som følge af hændelsen i betragtning, som f.eks. omkostninger til udskiftning eller flytning af software, hardware eller infrastruktur, personaleomkostninger, herunder omkostninger i forbindelse med udskiftning eller flytning af personale, ansættelse af ekstra personale, aflønning af overarbejde og generhvervelse af tabte eller forringede færdigheder, gebyrer som følge af manglende overholdelse af kontraktlige forpligtelser, omkostninger til genopretning og kompensation til kunder, tab som følge af mistede indtægter, omkostninger i forbindelse med intern og ekstern kommunikation og rådgivningsomkostninger, herunder omkostninger i forbindelse med juridisk rådgivning, kriminaltekniske ydelser og afhjælpningsydelser. Omkostninger, der er nødvendige for den daglige virksomhedsdrift, såsom omkostninger til generel vedligeholdelse af infrastruktur, udstyr, hardware og software, forbedringer og risikovurderingsinitiativer samt forsikringspræmier, betragtes ikke som økonomiske tab som følge af en hændelse. De berørte enheder beregner størrelsen af de økonomiske tab på grundlag af de data, der er tilgængelige, og hvis de faktiske økonomiske tab ikke kan fastslås, anslår enhederne beløbene.