2025/846

7.5.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/846

af 6. maj 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår grænseoverskridende identitetssammenkobling af fysiske personer

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 11a, stk. 3, og

ud fra følgende betragtninger:

(1) I henhold til forordning (EU) nr. 910/2014 skal europæiske digitale identitetstegnebøger (»tegnebøger«) og anmeldte elektroniske identifikationsmidler være til rådighed som en mulighed for autentifikation for at få adgang til grænseoverskridende offentlige onlinetjenester, der udbydes af medlemsstaterne. I sådanne grænseoverskridende autentifikationstilfælde er fortegnelser, der indeholder oplysninger om brugeren af tegnebogen eller brugeren af anmeldte elektroniske identifikationsmidler, sommetider allerede tilgængelige for modtagerparten via modtagerpartens eget register eller et eksternt register og ofte i form af en brugerkonto. I disse tilfælde kan visse oplysninger vedrørende brugeren, der er indhentet fra tegnebøgerne eller fra det anmeldte elektroniske identifikationsmiddel, sammenkobles af eller på vegne af den pågældende modtagerpart. Dette kan f.eks. opnås ved at benytte en centraliseret løsning, der drives af en offentlig myndighed, og de oplysninger, som allerede findes hos modtagerparten eller i et register, som modtagerparten anvender, f.eks. et folkeregister eller en database med brugerkontooplysninger.

(2) 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 ([2]), og navnlig den tekniske struktur og referenceramme, som er en del heraf. I overensstemmelse med betragtning 75 i Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([3]) 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.

(3) For at sikre, at identitetssammenkoblingsprocessen fungerer på en pålidelig måde i alle medlemsstater, bør de medlemsstater, der fungerer som modtagerparter, foretage den indledende identitetssammenkobling, når en fysisk person første gang anmoder om at få adgang til en tjeneste, der drives af modtagerparten, på grundlag af enten det minimum af data, der er fastsat i Kommissionens gennemførelsesforordning (EU) 2015/1501 ([4]), eller det personiden-

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

([2]) 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).

([3]) 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]) Kommissionens gennemførelsesforordning (EU) 2015/1501 af 8. september 2015 om interoperabilitetsrammen i henhold til artikel 12, stk. 8, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 235 af 9.9.2015, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2015/1501/oj).

tifikationsdatasæt, der er fastsat i Kommissionens gennemførelsesforordning (EU) 2024/2977 ([5]). Nærværende forordning fokuserer på medlemsstater, der fungerer som modtagerparter, mens forordning (EU) nr. 910/2014 overlader det til medlemsstaterne at beslutte, om identitetssammenkoblingssystemet også skal gøres tilgængeligt for private modtagerparter. Hvis medlemsstaterne lader identitetssammenkobling omfatte modtagerparter, der ikke er offentlige myndigheder, bør de i videst muligt omfang anvende de mekanismer og procedurer, der er fastsat i nærværende forordning.

(4) Med henblik på grænseoverskridende identitetssammenkobling ved anvendelse af tegnebøgerne bør de oplysninger, der anvendes til entydig identitetssammenkobling, være de obligatoriske dataidentifikatorer i personidentifikationsdatasættet i afsnit 1 i bilaget til gennemførelsesforordning (EU) 2024/2977 sammen med eventuelle fakultative data, der er nødvendige for at sikre, at sættet af personidentifikationsdata er unikt.

(5) Med henblik på grænseoverskridende identitetssammenkobling ved anvendelse af anmeldte elektroniske identifikationsmidler bør de oplysninger, der anvendes til entydig identitetssammenkobling, være de obligatoriske attributter i det minimum af data for en fysisk person, der er fastsat i afsnit 1 i bilaget til gennemførelsesforordning (EU) 2015/1501. Henvisningen til de obligatoriske attributter i minimummet af data for en fysisk person bør forstås inden for rammerne af gennemførelsesforordning (EU) 2015/1501, hvor en attribut beskrives som en komponent i minimummet af personidentifikationsdata, i modsætning til definitionen af attribut i artikel 3, nr. 43), i forordning (EU) nr. 910/2014, som ændret ved forordning (EU) 2024/1183.

(6) På grund af afhængigheden af allerede eksisterende oplysninger, som modtagerparten benytter til at sikre entydig identitetssammenkobling, kan identitetssammenkoblingsprocessen muligvis ikke gennemføres i alle tilfælde. For at give modtagerparterne en passende grad af fleksibilitet kan medlemsstaterne indføre supplerende processer, der sikrer en tilsvarende grad af tillid til resultatet af identitetssammenkoblingsprocessen.

(7) Hvis identitetssammenkoblingsprocessen anses for at være vellykket i henhold til bestemmelserne i nærværende forordning, bør modtagerparten eller den part, der handler på dennes vegne, eller et register, som modtagerparterne anvender, eller det centraliserede system sikre, at brugeren informeres om den vellykkede registrering, herunder ved forevisning af brugerens navn eller pseudonym og, hvis det er relevant, af f.eks. mulighederne for at lagre resultatet af identitetssammenkoblingsprocessen. Disse muligheder kan omfatte lagring af en tilknytning i et register, der drives af modtagerparten, og/eller i et register, som modtagerparten anvender, og/eller udstedelse af en særlig elektronisk attestering af attributter, der indeholder en tilknytning, der kan genbruges i fremtiden, og/eller anvendelse af alternative muligheder, som stilles til rådighed af modtagerparten eller den part, der handler på vegne af modtagerparten. Hvor det er relevant, bør brugeren kunne vælge mellem flere muligheder, og opbevaringstiden bør være under brugerens kontrol, så det sikres, at brugerne kan genbruge afsluttede identitetssammenkoblingsprocesser i fremtiden.

(8) For at øge gennemsigtigheden og brugerkontrollen, når brugeren ikke kan sammenkobles, bør brugeren gives en klar begrundelse for, hvorfor sammenkoblingen ikke lykkedes. Derudover bør brugeren informeres om eventuelle næste skridt. Dette bør omfatte de oplysninger, der blev anvendt i identitetssammenkoblingsprocessen, og eventuelle uoverensstemmelser, der blev konstateret, med tydelige forklaringer og instrukser til brugerne om mulige afhjælpende foranstaltninger og supplerende processer.

(9) For at sikre passende klagemekanismer, når der foretages identitetssammenkobling, bør modtagerparterne eller de parter, der handler på deres vegne, eller de registre, som modtagerparterne anvender, føre passende logfiler over identitetssammenkoblingsprocessen, de oplysninger, der anvendes til sammenkobling, og enhver anden støttedokumentation fra den fysiske person samt resultatet af identitetssammenkoblingsprocessen. Disse logfiler bør opbevares i mindst seks måneder og højst 12 måneder med henblik på registrering og behandling af klager fra brugerne. Opbevaringstiden kan forlænges, hvis det kræves i henhold til EU-retten eller national ret.

([5]) Kommissionens gennemførelsesforordning (EU) 2024/2977 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår personidentifikationsdata og elektronisk attestering af attributter udstedt til europæiske digitale identitetstegnebøger (EUT L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

(10) For at undgå, at tegnebogsbrugerne skal foretage identitetssammenkoblingsprocessen flere gange, kan medlemsstaterne kræve, at identitetssammenkoblingssystemer skal kunne udstede en elektronisk attestering af attributter med et link mellem tegnebogsbrugeren og et register, hvor den pågældende bruger er registreret som en kendt bruger. Alternativt kan medlemsstaterne lagre en tilknytning som en henvisning til et register, der er tilgængeligt for modtagerparten eller andre hjælpeforanstaltninger.

(11) For at sikre, at de tegnebøger, der skal leveres i overensstemmelse med kravene i artikel 5a, stk. 1, i forordning (EU) nr. 910/2014, og de anmeldte elektroniske identifikationsordninger kan drage fordel af velfungerende identitetssammenkoblingssystemer, er det nødvendigt at fastsætte en længere frist for anvendelsen af de respektive bestemmelser i nærværende forordning. For så vidt angår tegnebøger, bør hver medlemsstat levere mindst én tegnebog inden for 24 måneder fra datoen for ikrafttrædelsen af de gennemførelsesretsakter, der er omhandlet i artikel 5a, stk. 23, og artikel 5c, stk. 6, i forordning (EU) nr. 910/2014. Anvendelsen af de relevante bestemmelser i nærværende forordning om identitetssammenkobling baseret på tegnebøger bør derfor falde sammen med ovennævnte tidsramme. For så vidt angår anmeldte elektroniske identifikationsordninger bør der gives tilstrækkelig tid til at erstatte funktionerne til identitetssammenkobling.

(12) Da det skal være frivilligt at anvende tegnebogen, bør medlemsstaterne give brugerne alternative metoder til at få adgang til de tjenester, de leverer, når de fungerer som modtagerparter.

(13) Ved autentifikation i forbindelse med en elektronisk tjeneste, kan registreringen af en ny bruger være gnidningsfri og dermed fremstå visuelt og teknisk på samme måde, som hvis brugeren havde anvendt den elektroniske tjeneste før. Med henblik på nærværende forordning bør en ny brugerregistrering til en elektronisk tjeneste derfor anses for at svare til en vellykket identitetssammenkoblingsproces.

(14) Medlemsstaterne bør sikre, at identitetssammenkoblingsprocessen fungerer gnidningsløst, og at brugeren ikke oplever flere sessionsændringer og gentagne trin, selv hvis identitetssammenkoblingsprocessen i første omgang ikke lykkes, og der gennemføres supplerende processer.

(15) Medlemsstaterne kan frit udforme deres brugergrænseflader og notifikationer på en måde, der passer til deres nationale kontekst, under hensyntagen til ånden i kravene i nærværende forordning.

(16) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([6]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([7]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning.

(17) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([8]) og afgav udtalelse den 31. januar 2025.

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

([6]) 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).

([7]) 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).

([8]) 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).

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

Ved denne forordning fastsættes der regler for grænseoverskridende identitetssammenkobling af fysiske personer foretaget af offentlige myndigheder eller organer, der handler på vegne af en offentlig myndighed, der skal ajourføres regelmæssigt for at sikre overensstemmelse med den teknologiske udvikling og udviklingen af standarder og med det arbejde, der udføres på grundlag af henstilling (EU) 2021/946, navnlig den tekniske struktur og referencerammen.

Artikel 2

Generelle krav

1. Når en offentlig myndighed fungerer som modtagerpart i forbindelse med en grænseoverskridende onlinetjeneste, der udbydes af eller på vegne af den pågældende offentlige myndighed, sikrer medlemsstaterne, at den proces, der er fastsat i stk. 2, anvendes til at sikre entydig identitetssammenkobling af fysiske personer.

2. Entydig identitetssammenkobling foretages af, eller på vegne af, modtagerparten eller et register, som modtagerparterne anvender, eller et centraliseret system ved, alt efter hvad der er relevant, at anmode om, modtage og validere ægtheden af de oplysninger, der er omhandlet i stk. 3 eller 4.

3. Ved anvendelse af en tegnebog er de oplysninger, der skal anvendes til entydig identitetssammenkobling, de obligatoriske personidentifikationsdata, der er fastsat i afsnit 1 i bilaget til gennemførelsesforordning (EU) 2024/2977, sammen med eventuelle valgfri data, der er nødvendige for at sikre, at datasættet er unikt, herunder, hvis det er relevant, yderligere oplysninger eller supplerende procedurer.

4. Ved anvendelse af en anmeldt elektronisk identifikationsordning er de oplysninger, der skal anvendes til entydig identitetssammenkobling, de obligatoriske attributter i det minimum af data for en fysisk person, der er fastsat i afsnit 1 i bilaget til gennemførelsesforordning (EU) 2015/1501, herunder, hvis det er relevant, eventuelle yderligere oplysninger eller supplerende procedurer.

5. Ved vurderingen af, om der foreligger en entydig identitetssammenkobling, sammenholder modtagerparten eller den part, der handler på dennes vegne, de oplysninger, som brugeren har givet, med de oplysninger, som allerede er registreret hos modtagerparten eller en part, der handler på dennes vegne, eller i et register, som modtagerparterne anvender.

6. Resultatet af den proces, der er beskrevet i stk. 5, skal i videst muligt omfang være upåvirket af forskelle med hensyn til translitteration, blanktegn, orddeling, sammenkædning og lignende ortografiske variationer, der kræves i henhold til EU-retten eller medlemsstatens nationale ret.

7. Hvis der er et præcist sammenfald for de oplysninger, der er omhandlet i stk. 2, og sammenfaldet kun vedrører én fysisk person, eller hvis resultatet af processen fører til en ny registrering af brugeren, der i sin funktion svarer til en vellykket identitetssammenkoblingsproces, anses identitetssammenkoblingsprocessen for at være vellykket, hvilket resulterer i en utvetydig identitetssammenkobling. Hvis der ikke er et præcist sammenfald, eller hvis sammenfaldet vedrører mere end én fysisk person, eller hvis den part, der foretager identitetssammenkoblingen, ikke kan garantere, at den er entydig, anses identitetssammenkoblingsprocessen for at være mislykket.

8. Medlemsstaterne kan anvende centraliserede identitetssammenkoblingssystemer, der drives af en offentlig myndighed etableret i den pågældende medlemsstat, for at sikre, at anmeldte elektroniske identifikationsmidler eller tegnebøger fra en anden medlemsstat kan sammenkobles med eksisterende registreringer og fortegnelser ved hjælp af onlineprocedurer.

9. Hvis medlemsstaterne gør det muligt for tegnebogsmodtagere, der ikke er offentlige myndigheder, at foretage identitetssammenkobling, finder de mekanismer og procedurer, der er fastsat i nærværende forordning, anvendelse, hvor det er relevant.

Artikel 3

Modtagerparters forpligtelser, når identitetssammenkoblingsprocessen er vellykket

1. Første gang en bruger gennemfører identitetssammenkoblingsprocessen, og den anses for at være vellykket i henhold til artikel 2, stk. 7, sikrer modtagerparten eller den part, der handler på dennes vegne, eller et register, som modtagerparterne anvender, eller det centraliserede system, at brugeren informeres om, at vedkommende har fået adgang til den tjeneste, som der blev anmodet om adgang til.

2. Hvis det er relevant, informeres brugeren også, hvis vedkommende:

a) er blevet registreret som en ny bruger

b) er blevet sammenkoblet med en enkelt eksisterende bruger hos modtagerparten eller

c) er blevet sammenkoblet med en enkelt eksisterende bruger i et register, som modtagerparten eller den part, der handler på dennes vegne, anvender

d) kan genbruge afsluttede identitetssammenkoblingsprocesser i fremtiden ved at vælge en af følgende muligheder, inklusive opbevaringstiden:

— lagring af en tilknytning i et register, der drives af modtagerparten, eller i et register, som modtagerparten anvender, som kan genanvendes ved fremtidige anmodninger om adgang

— udstedelse af en særlig elektronisk attestering af attributter, der indeholder en tilknytning, som kan genanvendes ved fremtidige anmodninger om adgang

— alternative muligheder, som modtagerparten eller den part, der handler på vegne af modtagerparten, eller det centraliserede system stiller til rådighed, og som kan genanvendes ved fremtidige anmodninger om adgang.

Artikel 4

Modtagerparters forpligtelser, når identitetssammenkoblingsprocessen er mislykket

1. Hvis en identitetssammenkoblingsproces anses for at være mislykket i henhold til artikel 2, stk. 7, sikrer modtagerparten eller den part, der handler på dennes vegne, eller det centraliserede system, at brugeren af det anmeldte elektroniske identifikationsmiddel eller tegnebogen informeres, hvis:

a) de data, der blev opgivet, ikke er blevet sammenkoblet entydigt og på vellykket vis med en eksisterende bruger hos modtagerparten eller i et register, som modtagerparten eller den part, der handler på dennes vegne, anvender

b) der er andre muligheder for identitetssammenkobling eller andre metoder til at få adgang til tjenesten til rådighed for brugeren.

2. De muligheder eller andre metoder, der er omhandlet i stk. 1, litra b), kan omfatte:

a) et andet anmeldt elektronisk identifikationsmiddel eller en anden tegnebog

b) en ajourføring af oplysninger, der allerede er registreret hos modtagerparten, den part, der handler på dennes vegne, eller i et register, som modtagerparten anvender, eller det centraliserede identitetssammenkoblingssystem

c) yderligere oplysninger fra modtagerparten eller en part, der handler på dennes vegne med henblik på identitetssammenkobling, eller det centraliserede system.

3. Hvis de supplerende metoder resulterer i en vellykket og entydig sammenkobling eller registrering, skal resultatet være i overensstemmelse med forpligtelserne i artikel 3.

4. Hvis modtagerparten eller det centraliserede system enten indledningsvis eller efter forgæves at have udført de supplerende identitetssammenkoblingsprocesser fastslår, at brugeren ikke er blevet registreret tidligere, kan modtagerparten eller det centraliserede system betragte brugeren som en ny bruger og, hvis det er relevant, registrere brugeren i overensstemmelse med national ret eller administrativ praksis.

5. Hvis de supplerende metoder ikke resulterer i en vellykket og utvetydig sammenkobling, kan den part, der foretager identitetssammenkoblingen, vurdere, om brugeren ikke har haft nogen forudgående interaktion med modtagerparten eller et register, som modtagerparten anvender, og derfor skal betragtes som en ny bruger.

6. Når der er tale om nye brugere, anvender modtagerparterne den procedure, der er fastsat i artikel 3. Modtagerparterne kan registrere nye brugere i overensstemmelse med national ret eller administrativ praksis.

Artikel 5

Modtagerparters forpligtelser efter afslutningen af identitetssammenkoblingsprocessen

1. Når der gennemføres en identitetssammenkoblingsproces, jf. artikel 2, uanset om denne er vellykket eller mislykket, opbevarer modtagerparten eller den part, der handler på dennes vegne, eller det register, som modtagerparten anvender, logfilerne vedrørende identitetssammenkoblingsprocessen og resultatet heraf, herunder, hvis det er muligt, følgende:

a) de værdier, som brugeren og modtagerparten har opgivet, og som blev anvendt til at gennemføre identitetssammenkoblingsprocessen

b) dato og klokkeslæt for identitetssammenkoblingsprocessen

c) al relevant dokumentation, der er blevet fremlagt som led i de supplerende metoder, der er omhandlet i artikel 4, stk. 1 og 2, og som er nødvendig for tvistbilæggelse

d) hvor det er relevant, alle identifikatorer eller kontonumre vedrørende den fysiske person, der er blevet anvendt af modtagerparten, eller et register, som modtagerparterne anvender, eller den part, der handler på modtagerpartens vegne, eller det centraliserede identitetssammenkoblingssystem.

2. Modtagerparterne eller de parter, der handler på deres vegne, tager hensyn til principperne om indbygget sikkerhed og indbygget databeskyttelse i forbindelse med logning af de oplysninger, der er nævnt i stk. 1.

3. Modtagerparterne eller de parter, der handler på deres vegne, opbevarer logfilerne i mindst seks måneder og højst 12 måneder af sikkerhedshensyn. Opbevaringstiden kan forlænges med henblik på andre formål, herunder registrering og behandling af klager fra brugerne, hvis det kræves i henhold til EU-retten eller national ret.

Artikel 6

Ikrafttræden

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

Den finder anvendelse fra den 24. december 2026.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 6. maj 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand