2025/2532

17.12.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/2532

af 16. december 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår referencestandarder og specifikationer for kvalificerede elektroniske arkiveringstjenester

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 45j, stk. 2, og

ud fra følgende betragtninger:

(1) Ved Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([2]) blev der i forordning (EU) nr. 910/2014 indført en liste over nye tillidstjenester og kvalificerede tillidstjenester, herunder kvalificeret elektronisk arkiveringstjeneste. Kommissionen skal fastsætte en liste over referencestandarder og, hvor det er nødvendigt, specifikationer for disse tjenester.

(2) Elektronisk arkivering er en tjeneste til modtagelse, lagring, hentning og sletning af elektroniske data og elektroniske dokumenter med henblik på at sikre deres holdbarhed og læsbarhed samt at bevare deres integritet, fortrolighed og oprindelsesbevis i hele opbevaringsperioden. Kvalificerede elektroniske arkiveringstjenester spiller en afgørende rolle i det digitale erhvervsmiljø ved at fremme overgangen fra traditionelle papirbaserede processer til tilsvarende elektroniske processer. For at opretholde formodningen om elektroniske datas og elektroniske dokumenters integritet og oprindelse i hele opbevaringsperioden hos den kvalificerede tillidstjenesteudbyder og for at opnå en høj grad af gennemsigtighed og tillid blandt alle deltagere i oplysningernes livscyklus er det nødvendigt at fastsætte et fælles sæt specifikationer for kvalificerede elektroniske arkiveringstjenester.

(3) For at øge kvalificerede elektroniske arkiveringstjenesters bevisværdi, sikkerhed og troværdighed bør der anvendes kvalificerede tillidstjenester, når elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler anvendes til at oprette, underskrive, forsegle eller attestere dato og klokkeslæt for f.eks. arkivering af bevismateriale, fortegnelser over bevismateriale, fortegnelser over hændelsesforløb, fortegnelser over korrekt gennemførelse af procedurer eller arkivering af bekræftelsesrapporter.

(4) Den formodning om overholdelse, der er fastsat i artikel 45j, stk. 2, i forordning (EU) nr. 910/2014, bør kun finde anvendelse, hvis kvalificerede elektroniske arkiveringstjenester opfylder de krav, der er fastsat i nærværende forordning. Referencestandarderne for kvalificerede elektroniske arkiveringstjenester bør afspejle etableret praksis og være bredt anerkendte inden for de relevante sektorer. De bør tilpasses, så de omfatter yderligere kontroller, der sikrer de kvalificerede elektroniske arkiveringstjenesters sikkerhed og troværdighed.

(5) Hvis en tillidstjenesteudbyder opfylder kravene i denne forordning, bør tilsynsorganerne formode, at de relevante krav i forordning (EU) nr. 910/2014 er opfyldt, og tage behørigt hensyn til denne formodning i forbindelse med tildeling eller bekræftelse af tillidstjenestens status som kvalificeret. En kvalificeret tillidstjenesteudbyder kan dog stadig benytte anden praksis til at påvise opfyldelse af kravene i forordning (EU) nr. 910/2014.

(6) For at bevare integriteten af og oprindelsesbeviset for elektroniske data og elektroniske dokumenter, der indeholder en eller flere kvalificerede elektroniske signaturer eller segl, bør kvalificerede elektroniske arkiveringstjenester anvende procedurer og teknologi, der kan forlænge disse elektroniske signaturers og segls troværdighed ud over den teknologiske gyldighedsperiode, som minimum i hele opbevaringsperioden.

([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) 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).

(7) Kommissionen vurderer regelmæssigt nye teknologier, praksisser, standarder og tekniske specifikationer. I overensstemmelse med betragtning 75 til forordning (EU) 2024/1183 bør Kommissionen revidere og om nødvendigt ajourføre nærværende forordning for at sikre, at den er i overensstemmelse med den globale udvikling, nye teknologier, praksisser, standarder eller tekniske specifikationer, og for at følge bedste praksis på det indre marked.

(8) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([3]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([4]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning.

(9) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([5]) og afgav udtalelse den 21. oktober 2025 ([6]).

(10) Foranstaltningerne i denne 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

Elektronisk arkivering af dokumenter med en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl

1. Ved arkivering af elektroniske data eller elektroniske dokumenter, der indeholder kvalificerede elektroniske signaturer eller kvalificerede elektroniske segl, sikrer udbydere af kvalificerede elektroniske arkiveringstjenester, at disse kvalificerede elektroniske signaturers eller kvalificerede elektroniske segls troværdighed opretholdes, inklusive ud over deres teknologiske gyldighedsperiode, og at integriteten af de kvalificerede elektroniske signaturer og segl og nøjagtigheden af deres oprindelse bevares, som minimum indtil udløbet af den lovbestemte eller kontraktlige opbevaringsperiode.

2. Med henblik på stk. 1 kan udbydere af kvalificerede elektroniske arkiveringstjenester benytte en kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer eller en kvalificeret tjeneste til bevaring af kvalificerede elektroniske segl.

Artikel 2

Referencestandarder og specifikationer for levering af kvalificerede elektroniske arkiveringstjenester

De referencestandarder og specifikationer, der er omhandlet i artikel 45j, stk. 2, i forordning (EU) nr. 910/2014, er anført i bilaget til nærværende forordning.

([3]) 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).

([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]) 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).

([6]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services.

Artikel 3

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 hver medlemsstat.

Udfærdiget i Bruxelles, den 16. december 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

Liste over referencestandarder og specifikationer for kvalificerede elektroniske arkiveringstjenester

CEN/TS 18170:2025 (»CEN/TS 18170«) finder anvendelse med følgende tilpasninger:

a) Normative references (punkt 2)

— ETSI EN 319 401 V3.1.1 (2024-06), Elektroniske signaturer og infrastrukturer (ESI) — Generelle policykrav til trust serviceudbydere

— ETSI EN 319 421 V1.3.1 (2025-07), Elektroniske signaturer og infrastrukturer (ESI) — Generelle policy- og sikkerhedskrav til trust service-udbydere, der udsteder tidsstempler

— ISO 14721:2025, Space Data System Practices — Reference model for an open archival information system (OAIS)

— ACM-ECCG, Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms«, offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«).

— CIR (EU) 2024/482, Kommissionens gennemførelsesforordning (EU) 2024/482 ([1]).

— CIR (EU) 2024/3144, Kommissionens gennemførelsesforordning (EU) 2024/3144 ([2]).

— ISO/IEC 15408:2022 (del 1-5), »Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse — Evalueringskriterier for IT-sikkerhed«.

— FIPS PUB 140-3 (2019), »Security Requirements for Cryptographic Modules«.

b) Policy and practice statement (punkt 6.1)

— Kravene i CEN/TS 18170, punkt 6.1, finder anvendelse.

— Kravene i ETSI EN 319 401, punkt 5, finder anvendelse.

— EATSP fastlægger procedurer for underretning af tilsynsorganet om eventuelle ændringer i leveringen af elektroniske tillidstjenester til arkivering og for hensigten om at indstille disse aktiviteter i overensstemmelse med forretningsmæssige krav og relevante love og bestemmelser, herunder i overensstemmelse med kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) nr. 910/2014 [i.2].

— EATSP underretter det kompetente tilsynsorgan som minimum:

  — én måned før gennemførelsen af en ændring

  — tre måneder før den planlagte indstilling af leveringen af en tillidstjeneste.

c) Terms and Conditions (punkt 6.2)

— Kravene i CEN/TS 18170, punkt 6.2, finder anvendelse.

— Abonnenter og parter, der benytter den elektroniske tillidstjeneste til arkivering, informeres på en klar, fyldestgørende og lettilgængelig måde, på et offentligt tilgængeligt sted og individuelt, om de præcise vilkår og betingelser, inden der indgås et kontraktforhold.

([1]) Kommissionens gennemførelsesforordning (EU) 2024/482 af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (»EUCC«) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Kommissionens gennemførelsesforordning (EU) 2024/3144 af 18. december 2024 om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning (EUT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Human resources (punkt 7.3)

— Kravene i CEN/TS 18170, punkt 7.3, finder anvendelse.

— EATSP's personale i betroede roller og, hvis det er relevant, dennes underleverandører i betroede roller skal kunne opfylde kravet om at have opnået »ekspertviden, erfaring og kvalifikation« gennem formel uddannelse og eksaminer eller faktisk erfaring eller en kombination af de to. Dette omfatter regelmæssige opdateringer (mindst hver 12. måned) om nye trusler og aktuel sikkerhedspraksis.

e) Cryptographic controls and monitoring (punkt 7.6)

— Arkiveringssystemet skal garantere fortroligheden af data og dokumenter i hele arkivets livscyklus fra deponering til tilintetgørelse.

— De krav, der er specificeret i ETSI EN 319 401, underpunkt 7.5 »Cryptographic controls«, finder anvendelse.

— Oprindelsen af de data, der skal arkiveres i det elektroniske arkiveringssystem, fastlægges af EATSP. Hvis der anvendes elektroniske signaturer eller elektroniske segl til dette formål, skal disse elektroniske signaturer eller elektroniske segl være kvalificerede.

— Når EATSP digitalt underskriver (en del af) et digitalt objekt eller en digital post, skal den private EATSP-signeringsnøgle opbevares og anvendes i enten et kvalificeret elektronisk signatur- eller seglgenereringssystem eller en sikker kryptografisk enhed, der er et pålideligt system certificeret i overensstemmelse med:

  a) de fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 eller Fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2022, del 1-5, der er offentliggjort af deltagerne i ordningen vedrørende anerkendelse af certifikater for fælles kriterier inden for IT-sikkerhed, og certificeret til EAL 4 eller højere, eller

  b) den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (CIR (EU) 2024/482 og CIR (EU) 2024/3144), og certificeret til EAL 4 eller højere, eller

  c) indtil den 31. december 2030 FIPS PUB 140-3 niveau 3.

— Denne certificering skal omfatte et sikkerhedsmål eller en beskyttelsesprofil eller et moduldesign og sikkerheds-dokumentation, der opfylder kravene i dette dokument, på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikketekniske sikkerhedsforanstaltninger.

— Hvis den sikre kryptografiske enhed er omfattet af en certificering under EUCC (IR (EU) 2024/482 og CIR (EU) 2024/3144), skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— EATSP overvåger styrken af de kryptografiske algoritmer, der anvendes eller er blevet anvendt. Hvis en af de anvendte algoritmer eller parametre anses for at blive uegnet i henhold til risikostyringen, skal EATSP enten ajourføre den tilknyttede arkiveringspolitik eller oprette en ny arkiveringsprofil til håndtering af AIP'erne og fastlægge og gennemføre passende foranstaltninger.

— Evalueringen af de kryptografiske algoritmer og deres anvendelse hos EATSP skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA (ACM-ECCG).

— Tekniske komponenter i EATS skal autentificere hinanden på grundlag af kryptografiske teknikker forud for kommunikation.

f) Network (punkt 7.9)

— De krav, der er specificeret i ETSI EN 319 401, underpunkt 7.8 »Network security«, finder anvendelse.

— Den sårbarhedsscanning, der kræves i henhold til REQ-7.8-13 i ETSI EN 319 401, skal udføres mindst én gang pr. kvartal.

— Den penetrationstest, der kræves i henhold til REQ-7.8-17X i ETSI EN 319 401, skal udføres mindst én gang om året.

— Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for EATSP's drift.

g) Collection of evidence (punkt 7.11)

— De krav, der er specificeret i ETSI EN 319 401, underpunkt 7.10 »Collection of evidence«, finder anvendelse, herunder for kritiske og ikkekritiske hændelser (se underpunkt 13.2).

h) EATSP termination and termination plan (punkt 7.13)

— Kravene i CEN/TS 18170, punkt 7.13, finder anvendelse.

— EATSP's plan i tilfælde af virksomhedsafbrydelse skal opfylde kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) nr. 910/2014.

i) Reliable time of events (punkt 13.3.1)

— Kravene i CEN/TS 18170, punkt 13.3.1, finder anvendelse.

— Når der anvendes tidsstempler, skal EATSP anvende et kvalificeret tidsstempel.