2024/1183

30.4.2024

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

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

under henvisning til udtalelse fra Regionsudvalget ([2]),

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) I Kommissionens meddelelse af 19. februar 2020 med titlen »Europas digitale fremtid i støbeskeen« bebudes en revision af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([4]) for at forbedre dens effektivitet, lade dens fordele omfatte den private sektor og fremme pålidelige digitale identiteter for alle europæere.

(2) I sine konklusioner af 1.-2. oktober 2020 opfordrede Det Europæiske Råd Kommissionen til at foreslå, at der udvikles en EU-dækkende ramme for sikker offentlig elektronisk identifikation, herunder interoperable digitale signaturer, for at give borgerne kontrol over deres onlineidentitet og -data og muliggøre adgang til offentlige, private og grænseoverskridende digitale tjenester.

(3) I politikprogrammet for det digitale årti 2030, der blev etableret ved Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 ([5]), fastsættes målsætningerne og de digitale mål for en EU-ramme, som senest i 2030 har til formål at føre til en bred indførelse af en pålidelig, frivillig og brugerkontrolleret digital identitet, der er anerkendt i hele Unionen, og som giver alle brugere kontrol over deres data i onlineinteraktioner.

(4) I »Europæisk erklæring om digitale rettigheder og principper for det digitale årti«, som Europa-Parlamentet, Rådet og Kommissionen har proklameret ([6]) (»erklæringen«), understreges det, at alle har ret til at få adgang til digitale teknologier, produkter og tjenester, der er udformet således, at de er sikre og trygge og beskytter privatlivets fred. Dette omfatter sikring af, at alle personer, der bor i Unionen, tilbydes en tilgængelig, sikker og pålidelig digital identitet, der giver adgang til en bred vifte af online- og offlinetjenester, der er beskyttet mod cybersikkerhedsrisici og cyberkriminalitet, herunder brud på datasikkerheden og identitetstyveri eller -manipulation. I erklæringen fastsættes det også, at enhver har ret til beskyttelse af sine personoplysninger. Denne ret omfatter kontrol over, hvordan oplysningerne anvendes, og hvem de deles med.

([1]) EUT C 105 af 4.3.2022, s. 81.
([2]) EUT C 61 af 4.2.2022, s. 42.
([3]) Europa-Parlamentets holdning af 29.2.2024 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 26.3.2024.
([4]) 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 (EUT L 257 af 28.8.2014, s. 73).
([5]) Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030 (EUT L 323 af 19.12.2022, s. 4).
([6]) EUT C 23 af 23.1.2023, s. 1.

(5) Unionsborgere og indbyggere i Unionen bør have ret til en digital identitet, som er under deres enekontrol, og som sætter dem i stand til at udøve deres rettigheder i det digitale miljø og deltage i den digitale økonomi. For at nå dette mål bør der etableres en europæisk ramme for digital identitet, der gør det muligt for unionsborgere og indbyggere i Unionen at få adgang til offentlige og private online- og offlinetjenester i hele Unionen.

(6) En harmoniseret ramme for digital identitet bør bidrage til at skabe en mere digitalt integreret Union ved at mindske de digitale barrierer mellem medlemsstaterne og ved at sætte unionsborgere og indbyggerne i Unionen i stand til at nyde godt af fordelene ved digitalisering, samtidig med at gennemsigtigheden og beskyttelsen af deres rettigheder øges.

(7) En mere harmoniseret tilgang til elektronisk identifikation bør mindske risiciene og omkostningerne ved den nuværende fragmentering som følge af divergerende nationale løsninger eller, i nogle medlemsstater, manglen på sådanne elektroniske identifikationsløsninger. En sådan tilgang bør styrke det indre marked ved at gøre det muligt for unionsborgere, indbyggere i Unionen som defineret i national ret og virksomheder at identificere sig selv og sørge for autentifikation af deres identitet online og offline på en sikker, pålidelig, brugervenlig, bekvem, tilgængelig og harmoniseret måde i hele Unionen. Den europæiske digitale identitetstegnebog bør give fysiske og juridiske personer i hele Unionen et harmoniseret elektronisk identifikationsmiddel, der muliggør autentifikation og deling af data, der er knyttet til deres identitet. Alle bør kunne få adgang til offentlige og private tjenester på sikker vis ved hjælp af et forbedret økosystem for tillidstjenester og verificerede identitetsbeviser og elektroniske attesteringer af attributter, såsom akademiske kvalifikationer, herunder universitetsgrader, eller andre uddannelses- eller erhvervsmæssige kvalifikationer. Den europæiske ramme for digital identitet har til formål at opnå et skifte fra benyttelse af udelukkende nationale digitale identitetsløsninger til leveringen af elektroniske attesteringer af attributter, der er gyldige og juridisk anerkendte i hele Unionen. Udbydere af elektroniske attesteringer af attributter bør drage fordel af et klart og ensartet regelsæt, samtidig med at offentlige forvaltninger bør kunne forlade sig på elektroniske dokumenter i et givet format.

(8) Flere medlemsstater har indført og anvender elektroniske identifikationsmidler, som accepteres af tjenesteudbydere i Unionen. Desuden er der foretaget investeringer i både nationale og grænseoverskridende løsninger på grundlag af forordning (EU) nr. 910/2014, herunder anmeldte elektroniske identifikationsordningers interoperabilitet i henhold til nævnte forordning. For at sikre komplementaritet og at de nuværende brugere af anmeldte elektroniske identifikationsmidler hurtigt tager europæiske digitale identitetstegnebøger til sig, og for at minimere indvirkningen på eksisterende tjenesteudbydere forventes det, at de europæiske digitale identitetstegnebøger kan nyde godt af at bygge videre på de indhøstede erfaringer med eksisterende elektroniske identifikationsmidler og fra den infrastruktur for anmeldte elektroniske identifikationsordninger, der anvendes på EU-plan og nationalt plan.

(9) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([7]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([8]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til forordning (EU) nr. 910/2014. Løsningerne inden for den interoperabilitetsramme, der fastsættes i denne forordning, er også i overensstemmelse med de pågældende regler. Unionens databeskyttelsesret indeholder databeskyttelsesprincipper såsom princippet om dataminimering og formålsbegrænsning og forpligtelser såsom databeskyttelse gennem design og gennem standardindstillinger.

(10) For at støtte EU-virksomheders konkurrenceevne bør både online- og offlinetjenesteudbydere kunne benytte digitale identitetsløsninger, der er anerkendt i hele Unionen, uanset i hvilken medlemsstat disse løsninger er leveret, og således drage fordel af en harmoniseret EU-tilgang til tillid, sikkerhed og interoperabilitet. Både brugere og tjenesteudbydere bør kunne nyde godt af, at elektroniske attesteringer af attributter tillægges samme juridiske værdi i hele Unionen. En harmoniseret ramme for digital identitet har til formål at skabe økonomisk værdi ved at give lettere adgang til varer og tjenester og ved i væsentlig grad at reducere de driftsomkostninger, der er forbundet med elektroniske identifikations- og autentifikationsprocedurer, f.eks. i forbindelse med onboarding af nye kunder, ved at reducere muligheden for cyberkriminalitet, f.eks. identitets- og datatyveri og onlinesvindel, og dermed fremme effektivitetsgevinster og en sikker digital omstilling af Unionens mikrovirksomheder og små og mellemstore virksomheder (SMV'er).

([7]) 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).

([8]) 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).

(11) Europæiske digitale identitetstegnebøger bør lette anvendelsen af engangsprincippet og dermed mindske den administrative byrde og støtte grænseoverskridende mobilitet for unionsborgere, indbyggere i Unionen og virksomheder i hele Unionen og fremme udviklingen af interoperable e-forvaltningstjenester i hele Unionen.

(12) Forordning (EU) 2016/679 og Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([9]) samt direktiv 2002/58/EF finder anvendelse på behandling af personoplysninger i forbindelse med gennemførelsen af nærværende forordning. Derfor bør der i nærværende forordning fastsættes specifikke garantier for at forhindre udbydere af elektroniske identifikationsmidler og elektroniske attesteringer af attributter i at kombinere personoplysninger, der er indhentet ved levering af andre tjenester, med personoplysninger, som behandles med henblik på at levere de tjenester, der er omfattet af nærværende forordnings anvendelsesområde. Personoplysninger vedrørende levering af europæiske digitale identitetstegnebøger bør opbevares logisk adskilt fra alle andre data, der opbevares af udbyderen af den europæiske digitale identitetstegnebog. Nærværende forordning bør ikke forhindre udbydere af europæiske digitale identitetstegnebøger i at anvende yderligere tekniske foranstaltninger, der bidrager til at beskytte personoplysninger, såsom fysisk adskillelse af personoplysninger vedrørende leveringen af europæiske digitale identitetstegnebøger fra andre oplysninger, som udbyderen er i besiddelse af. Uden at det berører forordning (EU) 2016/679 præciserer nærværende forordning anvendelsen af principperne om formålsbegrænsning, dataminimering og databeskyttelse gennem design og gennem standardindstillinger.

(13) Europæiske digitale identitetstegnebøger bør have en funktion bestående af et fælles dashboard, der er indbygget i designet, for at sikre brugerne en højere grad af gennemsigtighed, privatlivsbeskyttelse og kontrol over deres personoplysninger. Denne funktion bør give en let og brugervenlig grænseflade med overblik over alle modtagerparter, som brugeren deler data med, herunder attributter, og typen af data, der deles med hver modtagerpart. Den vil gøre det muligt for brugerne at spore alle transaktioner, der udføres gennem den europæiske digitale identitetstegnebog, med følgende data som minimum: transaktionstidspunktet og -datoen, modpartens identifikation, de personoplysninger, der er anmodet om og de delte data. Disse oplysninger bør lagres, også selv om transaktionen ikke blev gennemført. Det bør ikke være muligt at afvise ægtheden af oplysningerne i transaktionshistorikken. En sådan funktion bør være aktiv som standard. Det bør gøre det let for brugerne at anmode om en modtagerparts omgående sletning af personoplysninger i henhold til artikel 17 i forordning (EU) 2016/679 og nemt at indberette modtagerparten til den kompetente nationale databeskyttelsesmyndighed, hvis der modtages en angiveligt ulovlig eller mistænkelig anmodning om personoplysninger, direkte via den europæiske digitale identitetstegnebog.

(14) Medlemsstaterne bør integrere forskellige teknologier til beskyttelse af privatlivets fred såsom nulvidenbevis i den europæiske digitale identitetstegnebog. Disse kryptografiske metoder bør gøre det muligt for en modtagerpart at validere, hvorvidt en given erklæring baseret på personens identifikationsdata og attestering af attributter er sand, uden at afsløre nogen af de data, som erklæringen er baseret på, således at brugerens privatliv beskyttes.

(15) Denne forordning fastsætter harmoniserede betingelser for fastlæggelsen af en ramme for europæiske digitale identitetstegnebøger, der skal stilles til rådighed af medlemsstaterne. Alle unionsborgere og indbyggere i Unionen som defineret i national ret bør have beføjelse til på sikker vis at anmode om, udvælge, kombinere, lagre, slette, dele og fremlægge data vedrørende deres identitet og anmode om sletning af deres personoplysninger på en brugervenlig og bekvem måde under brugerens enekontrol, samtidig med at der gives mulighed for selektiv videregivelse af personoplysninger. Denne forordning afspejler fælles europæiske værdier og respekterer grundlæggende rettigheder, retsgarantier og ansvar og beskytter dermed demokratiske samfund, unionsborgere og indbyggere i Unionen. Der bør udvikles teknologier, der anvendes til at nå disse mål, med det sigte at opnå det højeste niveau af sikkerhed, privatlivsbeskyttelse, brugerbekvemmelighed, tilgængelighed, udbredt anvendelighed og gnidningsløs interoperabilitet. Medlemsstaterne bør sikre lige adgang til elektronisk identifikation for alle deres borgere og indbyggere. Medlemsstaterne bør ikke direkte eller indirekte begrænse adgangen til offentlige eller private tjenester for fysiske eller juridiske personer, som vælger ikke at anvende europæiske digitale identitetstegnebøger, og bør stille passende alternative løsninger til rådighed.

([9]) 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 nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

(16) Medlemsstaterne bør gøre brug af de muligheder, som denne forordning giver, for under deres ansvar at levere europæiske digitale identitetstegnebøger til brug for fysiske og juridiske personer, der er hjemmehørende på deres område. For at give medlemsstaterne fleksibilitet og udnytte den nyeste teknologi bør denne forordning give mulighed for levering af europæiske digitale identitetstegnebøger direkte af en medlemsstat, på grundlag af et mandat fra en medlemsstat eller uafhængigt af en medlemsstat, men anerkendt af denne medlemsstat.

(17) Med henblik på registrering bør modtagerparter give de oplysninger, der er nødvendige for at muliggøre elektronisk identifikation og autentifikation af dem med henblik på europæiske digitale identitetstegnebøger. Når modtagerparterne angiver deres påtænkte anvendelse af den europæiske digitale identitetstegnebog, bør de give oplysninger om de data, som de vil anmode om, hvis sådanne forefindes, med henblik på levering af deres tjenester, og begrundelsen for anmodningen. Registrering af modtagerparter letter medlemsstaternes kontrol for så vidt angår lovligheden af modtagerparternes aktiviteter i overensstemmelse med EU-retten. Forpligtelsen til at registrere sig, der fastsættes i denne forordning, bør ikke berøre de forpligtelser, der er fastsat i anden EU-ret eller national ret, såsom de oplysninger, der skal gives til de registrerede i henhold til forordning (EU) 2016/679. Modtagerparterne bør overholde de garantier, der er fastsat i nævnte forordnings artikel 35 og 36, navnlig ved at foretage konsekvensanalyser vedrørende databeskyttelse og ved at høre de kompetente databeskyttelsesmyndigheder forud for databehandlingen, hvis konsekvensanalyserne vedrørende databeskyttelse viser, at behandlingen indebærer en høj risiko. Sådanne garantier bør understøtte modtagerparternes lovlige behandling af personoplysninger, navnlig for så vidt angår særlige kategorier af oplysninger såsom sundhedsoplysninger. Registreringen af modtagerparter har til formål at øge gennemsigtigheden af og tilliden til brugen af europæiske digitale identitetstegnebøger. Registreringen bør være omkostningseffektiv og stå i et rimeligt forhold til de dermed forbundne risici for at sikre udbredelsen blandt tjenesteudbydere. I den forbindelse bør registreringen omfatte anvendelse af automatiserede procedurer, herunder medlemsstaternes benyttelse og anvendelse af eksisterende registre, og bør ikke indebære en forhåndsgodkendelsesproces. Registreringsprocessen bør muliggøre en række forskellige brugstilfælde, der kan variere med hensyn til betjeningsmåde, uanset om det er online eller offline, eller med hensyn til kravet om at autentificere enheder med henblik på at kommunikere med den europæiske digitale identitetstegnebog. Registrering bør udelukkende finde anvendelse på modtagerparter, der leverer tjenester ved hjælp af digital interaktion.

(18) Beskyttelse af unionsborgere og indbyggere i Unionen mod uautoriseret eller svigagtig brug af europæiske digitale identitetstegnebøger er af stor betydning for at sikre tilliden til og den brede udbredelse af europæiske digitale identitetstegnebøger. Brugerne bør sikres effektiv beskyttelse mod et sådant misbrug. Navnlig når en national judiciel myndighed i forbindelse med en anden procedure konstaterer forhold, der danner grundlag for svigagtig eller anden ulovlig brug af en europæisk digital identitetstegnebog, bør de tilsynsorganer, der er ansvarlige for udstedere af europæiske digitale identitetstegnebøger, efter anmeldelse træffe de nødvendige foranstaltninger til at sikre, at registreringen af modtagerparten og medtagelsen af modtagerparter i autentifikationsmekanismen trækkes tilbage eller suspenderes, indtil den anmeldende myndighed bekræfter, at de konstaterede uregelmæssigheder er afhjulpet.

(19) Alle europæiske digitale identitetstegnebøger bør give brugerne mulighed for elektronisk identifikation af dem selv og autentifikation online og offline på tværs af grænser for at få adgang til en bred vifte af offentlige og private tjenester. Europæiske digitale identitetstegnebøger kan også imødekomme institutionelle behov hos offentlige forvaltninger, internationale organisationer og Unionens institutioner, organer, kontorer og agenturer, uden at det berører medlemsstaternes beføjelser med hensyn til identifikation af deres borgere og indbyggere. Autentifikation offline vil være vigtig i mange sektorer, herunder i sundhedssektoren, hvor tjenester ofte leveres gennem personlig interaktion, og der bør i forbindelse med e-recepter kunne benyttes QR-koder eller lignende teknologier til at kontrollere autenticiteten. Idet de forlader sig på sikringsniveauet »høj« for så vidt angår elektroniske identifikationsordninger, bør de europæiske digitale identitetstegnebøger for at opfylde sikkerhedskravene i denne forordning nyde godt af det potentiale, som manipulationssikrede løsninger såsom sikre elementer indeholder. Europæiske digitale identitetstegnebøger bør også give brugerne mulighed for at oprette og anvende kvalificerede elektroniske signaturer og segl, der accepteres i hele Unionen. Når fysiske personer er onboarded i en europæisk digital identitetstegnebog, bør de som standard og gratis kunne bruge den til at underskrive med kvalificerede elektroniske signaturer uden at skulle igennem yderligere administrative procedurer. Brugerne bør kunne underskrive eller forsegle erklæringer eller attributter, som de selv påberåber sig. For at give personer og virksomheder i hele Unionen fordele med hensyn til forenkling og besparelse af omkostninger, herunder ved at give mulighed for repræsentationsbeføjelser og e-mandater, bør medlemsstaterne levere europæiske digitale identitetstegnebøger, der benytter fælles standarder og tekniske specifikationer, for at sikre gnidningsløs interoperabilitet og for at højne IT-sikkerhedsniveauet tilstrækkeligt, styrke robustheden mod cyberangreb og dermed væsentligt reducere de potentielle risici ved den igangværende digitalisering for unionsborgere, indbyggere i Unionen og virksomheder. Kun medlemsstaternes kompetente myndigheder kan give en høj grad af tillid, når en persons

identitet skal fastslås, og dermed garantere, at den person, der påberåber sig eller gør en bestemt identitet gældende, faktisk er den person, som vedkommende hævder at være. Det er derfor nødvendigt, at leveringen af europæiske digitale identitetstegnebøger er baseret på den juridiske identitet af unionsborgere, indbyggere i Unionen eller juridiske personer. Benyttelse af den juridiske identitet bør ikke hindre brugere af europæiske digitale identitetstegnebøger i at få adgang til tjenester under et pseudonym, hvis der ikke er noget retligt krav om en juridisk identitet med henblik på autentifikation. Tillid til europæiske digitale identitetstegnebøger vil blive styrket, hvis de udstedende og forvaltende parter er forpligtede til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre det højest mulige sikkerhedsniveau, der står i et rimeligt forhold til risiciene for fysiske personers rettigheder og frihedsrettigheder i overensstemmelse med forordning (EU) 2016/679.

(20) Anvendelsen af en kvalificeret elektronisk signatur bør være gratis for alle fysiske personer til ikkeerhvervsmæssige formål. Det bør være muligt for medlemsstaterne at træffe foranstaltninger til at forhindre fysiske personers gratis anvendelse af kvalificerede elektroniske signaturer til erhvervsmæssige formål, samtidig med at det sikres, at sådanne foranstaltninger står i et rimeligt forhold til de identificerede risici og er berettigede.

(21) Det er gavnligt at lette udbredelsen og anvendelsen af europæiske digitale identitetstegnebøger ved gnidningsløst at integrere dem i det økosystem af offentlige og private digitale tjenester, der allerede er indført på nationalt, lokalt eller regionalt plan. For at nå dette mål bør det være muligt for medlemsstaterne at fastsætte retlige og organisatoriske foranstaltninger med henblik på at øge fleksibiliteten for udbydere af europæiske digitale identitetstegnebøger og for at give mulighed for yderligere funktionaliteter i europæiske digitale identitetstegnebøger udover dem, der er fastsat i denne forordning, herunder gennem øget interoperabilitet med eksisterende nationale elektroniske identifikationsmidler. Sådanne yderligere funktionaliteter bør på ingen måde være til skade for leveringen af europæiske digitale identitetstegnebøgers centrale funktioner, der er fastsat i denne forordning, eller fremme eksisterende nationale løsninger frem for europæiske digitale identitetstegnebøger. Da sådanne yderligere funktionaliteter rækker ud over, hvad der er fastsat i denne forordning, er de ikke omfattet af forordningens bestemmelser om grænseoverskridende benyttelse af europæiske digitale identitetstegnebøger.

(22) Europæiske digitale identitetstegnebøger bør indeholde en funktionalitet til generering af brugervalgte og -forvaltede pseudonymer, der autentificeres ved adgang til onlinetjenester.

(23) For at opnå et højt sikkerheds- og pålidelighedsniveau fastsætter denne forordning kravene til europæiske digitale identitetstegnebøger. De europæiske digitale identitetstegnebøgers overensstemmelse med disse krav bør certificeres af akkrediterede overensstemmelsesvurderingsorganer, som udpeges af medlemsstaterne.

(24) For at undgå divergerende tilgange og harmonisere gennemførelsen af de krav, der fastsættes i denne forordning, bør Kommissionen med henblik på certificering af europæiske digitale identitetstegnebøger vedtage gennemførelsesretsakter for at fastlægge en liste af referencestandarder og, hvor det er nødvendigt, fastlægge specifikationer og procedurer med henblik på at angive detaljerede tekniske specifikationer for disse krav. I det omfang certificeringen af europæiske digitale identitetstegnebøgers overensstemmelse med relevante cybersikkerhedskrav ikke er omfattet af eksisterende cybersikkerhedscertificeringsordninger, der er omhandlet i denne forordning, og for så vidt angår ikkecybersikkerhedsrelaterede krav, der er relevante for europæiske digitale identitetstegnebøger, bør medlemsstaterne indføre nationale certificeringsordninger i henhold til de harmoniserede krav, der er fastsat i og vedtaget i henhold til denne forordning. Medlemsstaterne bør fremsende deres udkast til nationale certificeringsordninger til den europæiske samarbejdsgruppe for digital identitet, som bør kunne afgive udtalelser og udstede henstillinger.

(25) Certificering af overensstemmelse med de cybersikkerhedskrav, der er fastsat i denne forordning, bør, hvor det er muligt, baseres på de relevante europæiske cybersikkerhedscertificeringsordninger, der er fastlagt i henhold til Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([10]), som fastlægger en frivillig europæisk ramme for cybersikkerhedscertificering af IKT-produkter, -processer og -tjenester.

([10]) 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).

(26) For løbende at vurdere og afbøde sikkerhedsrelaterede risici bør certificerede europæiske digitale identitetstegnebøger underkastes regelmæssige sårbarhedsvurderinger, der sigter mod afdækning af eventuelle sårbarheder i den europæiske digitale identitetstegnebogs certificerede produkt-, proces- og tjenesterelaterede komponenter.

(27) Ved at beskytte brugere og virksomheder mod cybersikkerhedsrisici bidrager de grundlæggende cybersikkerhedsrelaterede krav i denne forordning også til at forbedre beskyttelsen af personoplysninger og privatlivets fred for enkeltpersoner. Synergier med hensyn til både standardisering og certificering af cybersikkerhedsaspekter bør overvejes inden for rammerne af samarbejdet mellem Kommissionen, de europæiske standardiseringsorganisationer, Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), Det Europæiske Databeskyttelsesråd oprettet ved forordning (EU) 2016/679 og de nationale databeskyttelsestilsynsmyndigheder.

(28) Onboarding af unionsborgere og indbyggere i Unionen til den europæiske digitale identitetstegnebog bør lettes ved hjælp af elektroniske identifikationsmidler, der er udstedt på sikringsniveauet »høj«. Elektroniske identifikationsmidler, der er udstedt på sikringsniveauet »betydelig«, bør kun anvendes, hvis harmoniserede tekniske specifikationer og procedurer, der benytter elektroniske identifikationsmidler udstedt på sikringsniveauet »betydelig« i kombination med supplerende identitetskontrolmidler, vil gøre det muligt at opfylde kravene i nærværende forordning for så vidt angår sikringsniveauet »høj«. Sådanne supplerende midler bør være pålidelige og lette at anvende og kunne bygge på muligheden for at anvende onboardingprocedurer på afstand, kvalificerede certifikater understøttet af kvalificerede elektroniske signaturer, kvalificeret elektronisk attestering af attributter eller en kombination heraf. For at sikre en tilstrækkelig udbredelse af europæiske digitale identitetstegnebøger bør der i gennemførelsesretsakter fastsættes harmoniserede tekniske specifikationer og procedurer for onboarding af brugere ved hjælp af elektroniske identifikationsmidler, herunder dem, der udstedes på sikringsniveauet »betydelig«.

(29) Formålet med denne forordning er at forsyne brugeren med en fuldt mobil, sikker og brugervenlig europæisk digital identitetstegnebog. Som en overgangsforanstaltning, indtil certificerede manipulationssikrede løsninger er tilgængelige såsom sikre elementer i brugernes enheder, bør europæiske digitale identitetstegnebøger kunne benytte certificerede eksterne sikre elementer til at beskytte kryptografisk materiale og andre følsomme oplysninger eller anmeldte elektroniske identifikationsmidler på sikringsniveauet »høj« med henblik på at påvise overensstemmelse med denne forordnings relevante krav for så vidt angår den europæiske digitale identitetstegnebogs sikringsniveau. Denne forordning bør ikke berøre nationale betingelser for så vidt angår udstedelsen og anvendelsen af et certificeret eksternt sikkert element, hvor overgangsforanstaltningen afhænger af det.

(30) Europæiske digitale identitetstegnebøger bør sikre det højeste databeskyttelses- og sikkerhedsniveau med henblik på elektronisk identifikation og autentifikation for at lette adgangen til offentlige og private tjenester, uanset om sådanne data lagres lokalt eller i cloudbaserede løsninger, under behørig hensyntagen til de forskellige risikoniveauer.

(31) Europæiske digitale identitetstegnebøger bør have sikkerhed gennem design og bør indføre avancerede sikkerhedselementer for at beskytte mod identitetstyveri og andet datatyveri, nægtelse af tjeneste og enhver anden cybertrussel. Sådan sikkerhed bør omfatte de nyeste krypterings- og lagringsmetoder, som er tilgængelige udelukkende for, og kan dekrypteres udelukkende af, brugeren, og som benytter end-to-end-krypteret kommunikation med andre europæiske digitale identitetstegnebøger og modtagerparter. Desuden bør europæiske digitale identitetstegnebøger kræve sikker, udtrykkelig og aktiv brugerbekræftelse for de operationer, der udføres via europæiske digitale identitetstegnebøger.

(32) Den gratis anvendelse af europæiske digitale identitetstegnebøger bør ikke føre til behandling af data ud over data, der er nødvendige for at levere europæiske digitale identitetstegnebogstjenester. Denne forordning bør ikke give mulighed for, at udbyderen af den europæiske digitale identitetstegnebog behandler personoplysninger, der er lagret i eller er et resultat af anvendelsen af den europæiske digitale identitetstegnebog, til andre formål end levering af europæiske digitale identitetstegnebogstjenester. For at sikre privatlivsbeskyttelse bør udbydere af europæiske digitale identitetstegnebøger sikre ikkeobserverbarhed ved ikke at indsamle data og ikke at have indsigt i transaktioner foretaget af brugerne af den europæiske digitale identitetstegnebog. Sådan ikkeobserverbarhed betyder, at udbyderne ikke er i stand til at se nærmere oplysninger om de transaktioner, som brugeren har foretaget. I særlige tilfælde baseret på brugerens udtrykkelige forudgående samtykke i hvert af disse særlige tilfælde og i fuld overensstemmelse med forordning (EU) 2016/679 vil udbydere af europæiske digitale identitetstegnebøger dog kunne få adgang til de

oplysninger, der er nødvendige for at levere en bestemt tjeneste i forbindelse med europæiske digitale identitetstegnebøger.

(33) Europæiske digitale identitetstegnebøgers gennemsigtighed og deres udbyderes ansvarlighed er centrale faktorer for at skabe social tillid og afstedkomme accept af rammen. De europæiske digitale identitetstegnebøger bør derfor fungere på en gennemsigtig måde og navnlig give mulighed for kontrollerbar behandling af personoplysninger. For at opnå dette bør medlemsstaterne offentliggøre kildekoden til brugerapplikationens softwarekomponenter i europæiske digitale identitetstegnebøger, herunder dem, der vedrører behandling af personoplysninger og data om juridiske personer. Offentliggørelse af denne kildekode med en open source-licens bør give samfundet, herunder brugere og udviklere, mulighed for at forstå, hvordan den fungerer, og revidere og gennemgå koden. Dette vil øge brugernes tillid til økosystemet og bidrage til europæiske digitale identitetstegnebøgers sikkerhed ved at give alle mulighed for at rapportere om sårbarheder og fejl i koden. Samlet set bør dette tilskynde udbyderne til at levere og opretholde et meget sikkert produkt. I visse tilfælde vil videregivelse af kildekoden til de anvendte biblioteker, kommunikationskanaler eller andre elementer, der ikke hostes på brugerenheden, dog kunne begrænses af medlemsstaterne af behørigt begrundede årsager, navnlig af hensyn til den offentlige sikkerhed.

(34) Brugen af europæiske digitale identitetstegnebøger og ophør heraf bør udelukkende være brugernes ret og valg. Medlemsstaterne bør udvikle enkle og sikre procedurer, så brugerne kan anmode om øjeblikkelig tilbagekaldelse af gyldigheden af europæiske digitale identitetstegnebøger, herunder i tilfælde af tab eller tyveri. Ved brugerens død eller ved ophør af en juridisk persons aktivitet bør der indføres en mekanisme, der gør det muligt for den myndighed, der er ansvarlig for at opgøre boet efter den fysiske person eller den juridiske persons aktiver, at anmode om den øjeblikkelige tilbagekaldelse af en europæisk digital identitetstegnebog.

(35) For at fremme udbredelsen af europæiske digitale identitetstegnebøger og den bredere anvendelse af digitale identiteter bør medlemsstaterne ikke blot fremme fordelene ved de relevante tjenester, men bør i samarbejde med den private sektor, forskere og den akademiske verden også udvikle uddannelsesprogrammer, der har til formål at styrke deres borgeres og indbyggeres digitale færdigheder, navnlig for sårbare grupper såsom personer med handicap og ældre. Medlemsstaterne bør øge bevidstheden om fordelene og risiciene ved europæiske digitale identitetstegnebøger ved hjælp af kommunikationskampagner.

(36) For at sikre, at den europæiske ramme for digital identitet er åben for innovation og teknologisk udvikling og er fremtidssikret, tilskyndes medlemsstaterne til i fællesskab at oprette sandkasser til afprøvning af innovative løsninger i et kontrolleret og sikkert miljø, navnlig for at forbedre løsningernes funktionalitet, beskyttelse af personoplysninger, sikkerhed og interoperabilitet og bidrage til fremtidige ajourføringer af tekniske referencer og retlige krav. Dette miljø bør fremme inddragelsen af SMV'er, nystartede virksomheder og individuelle innovatorer og forskere samt relevante interessenter i industrien. Sådanne initiativer bør bidrage til og styrke den reguleringsmæssige overholdelse og tekniske robusthed af europæiske digitale identitetstegnebøger, der skal leveres til unionsborgere og indbyggere i Unionen, og dermed forhindre udviklingen af løsninger, der ikke er overholder EU-retten om databeskyttelse, eller som er åbne for sikkerhedsmæssige sårbarheder.

(37) Europa-Parlamentet og Rådets forordning (EU) 2019/1157 ([11]) styrker sikkerheden af identitetskort med forbedrede sikkerhedselementer senest i august 2021. Medlemsstaterne bør overveje muligheden for at anmelde dem som led i elektroniske identifikationsordninger for at udvide den grænseoverskridende adgang til elektroniske identifikationsmidler.

(38) Proceduren for anmeldelse af elektroniske identifikationsordninger bør forenkles og fremskyndes for at fremme adgangen til bekvemme, pålidelige, sikre og innovative autentifikations- og identifikationsløsninger og, hvor det er relevant, tilskynde private identitetsudbydere til at udbyde elektroniske identifikationsordninger til medlemsstaternes myndigheder til anmeldelse som nationale elektroniske identifikationsordninger i henhold til forordning (EU) nr. 910/2014.

([11]) Europa-Parlamentets og Rådets forordning (EU) 2019/1157 af 20. juni 2019 om styrkelse af sikkerheden af unionsborgeres identitetskort og af opholdsdokumenter, der udstedes til unionsborgere og deres familiemedlemmer, som udøver deres ret til fri bevægelighed (EUT L 188 af 12.7.2019, s. 67).

(39) En strømlining af de nuværende procedurer for anmeldelse og peerevaluering vil forhindre uensartede tilgange til vurdering af forskellige anmeldte elektroniske identifikationsordninger og gøre det lettere at opbygge tillid mellem medlemsstaterne. Nye, forenklede mekanismer har til formål at fremme medlemsstaternes samarbejde om sikkerhed og interoperabilitet i deres anmeldte elektroniske identifikationsordninger.

(40) Medlemsstaterne bør nyde godt af nye, fleksible værktøjer til at sikre overholdelse af kravene i denne forordning og i de relevante gennemførelsesretsakter, der er vedtaget i medfør heraf. Denne forordning bør give medlemsstaterne mulighed for at anvende rapporter og vurderinger, der er udarbejdet eller udført af akkrediterede overensstemmelsesvurderingsorganer, som fastsat inden for rammerne af certificeringsordninger, der skal oprettes på EU-plan i henhold til forordning (EU) 2019/881, til at understøtte deres påstande om tilpasning af ordningerne eller dele heraf til forordning (EU) nr. 910/2014.

(41) Offentlige tjenesteudbydere anvender de personidentifikationsdata, der er tilgængelige fra elektroniske identifikationsmidler i henhold til forordning (EU) nr. 910/2014, til at matche den elektroniske identitet af brugere fra andre medlemsstater med de personidentifikationsdata, der gives til disse brugere i den medlemsstat, der udfører processen for identitetssammenkobling på tværs af grænserne. På trods af anvendelsen af det minimumsdatasæt, der stilles til rådighed i henhold til de anmeldte elektroniske identifikationsordninger, kræver det imidlertid i mange tilfælde yderligere oplysninger om brugeren og specifikke supplerende entydige identifikationsprocedurer, der skal gennemføres på nationalt plan, for at sikre en nøjagtig identitetssammenkobling, når medlemsstaterne fungerer som modtagerparter. For yderligere at støtte anvendeligheden af elektroniske identifikationsmidler, sikre bedre offentlige onlinetjenester og øge retssikkerheden i forbindelse med brugernes elektroniske identitet bør forordning (EU) nr. 910/2014 kræve, at medlemsstaterne skal træffe specifikke onlineforanstaltninger for at sikre utvetydig identitetssammenkobling, når brugerne agter at få adgang til grænseoverskridende offentlige onlinetjenester.

(42) Når der udvikles europæiske digitale identitetstegnebøger, er det afgørende at tage hensyn til brugernes behov. Meningsfulde brugstilfælde og onlinetjenester, der benytter europæiske digitale identitetstegnebøger bør stilles til rådighed. Af hensyn til brugernes bekvemmelighed og for at sikre sådanne tjenesters tilgængelighed på tværs af grænserne er det vigtigt at træffe tiltag med henblik på at fremme en ensartet tilgang til udformning, udvikling og gennemførelse af onlinetjenester i alle medlemsstater. Ikkebindende retningslinjer for udformning, udvikling og gennemførelse af onlinetjenester, der benytter europæiske digitale identitetstegnebøger, har potentiale til at blive et nyttigt redskab til at nå dette mål. Sådanne retningslinjer bør udarbejdes under hensyntagen til Unionens interoperabilitetsramme. Medlemsstaterne bør have en fremtrædende rolle i forbindelse med vedtagelsen af disse retningslinjer.

(43) I overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2019/882 ([12]) skal personer med handicap kunne anvende europæiske digitale identitetstegnebøger, tillidstjenester og de slutbrugerprodukter, der anvendes til levering af sådanne tjenester, på lige fod med andre brugere.

(44) For at sikre en effektiv håndhævelse af denne forordning bør der fastsættes et minimumsniveau for de maksimale administrative bøder for både kvalificerede og ikkekvalificerede tillidstjenesteudbydere. Medlemsstaterne bør fastsætte sanktioner, der er effektive, står i et rimeligt forhold til overtrædelsen og har afskrækkende virkning. Ved fastsættelsen af sanktionerne bør der tages behørigt hensyn til de berørte enheders størrelse, deres forretningsmodeller og alvoren af overtrædelsen.

(45) Medlemsstaterne bør fastsætte regler om sanktioner for overtrædelser såsom direkte eller indirekte praksis, der fører til forveksling mellem ikkekvalificerede og kvalificerede tillidstjenester eller til ikkekvalificerede tillidstjenesteudbyderes misbrug af EU-tillidsmærket. EU-tillidsmærket bør ikke anvendes på betingelser, der direkte eller indirekte fører til den opfattelse, at ikkekvalificerede tillidstjenester, der tilbydes af disse udbydere, er kvalificerede.

(46) Denne forordning bør ikke omfatte aspekter relateret til indgåelse og gyldighed af kontrakter eller andre retlige forpligtelser, som ifølge EU-retten eller national ret er undergivet formkrav. Den bør heller ikke berøre nationale formkrav til offentlige registre, navnlig handelsregistre og tingbøger.

([12]) Europa-Parlamentets og Rådets direktiv (EU) 2019/882 af 17. april 2019 om tilgængelighedskrav for produkter og tjenester (EUT L 151 af 7.6.2019, s. 70).

(47) Levering og anvendelse af tillidstjenester og fordelene i form af bekvemmelighed og retssikkerhed i forbindelse med grænseoverskridende transaktioner, navnlig når der anvendes kvalificerede tillidstjenester, er af stadig større betydning for international handel og internationalt samarbejde. Unionens internationale partnere fastlægger tillidsrammer inspireret af forordning (EU) nr. 910/2014. For at lette anerkendelsen af kvalificerede tillidstjenester og deres udbydere kan Kommissionen vedtage gennemførelsesretsakter for at fastsætte betingelser for, hvornår tredjelandes tillidsrammer kan anses for at svare til tillidsrammerne for kvalificerede tillidstjenester og udbydere heraf i denne forordning. En sådan tilgang bør supplere muligheden for gensidig anerkendelse af tillidstjenester og udbydere heraf, der er hjemmehørende i Unionen og i tredjelande i overensstemmelse med artikel 218 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Ved fastsættelsen af betingelserne for, hvornår tredjelandes tillidsrammer kan anses for at svare til tillidsrammerne for kvalificerede tillidstjenester og udbydere heraf i forordning (EU) nr. 910/2014, bør det sikres, at de relevante bestemmelser i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([13]) og forordning (EU) 2016/679 overholdes, samt at der anvendes positivlister som grundlæggende elementer for opbygning af tillid.

(48) Denne forordning bør fremme valgmuligheder og muligheden for at skifte mellem europæiske digitale identitetstegnebøger, hvis en medlemsstat har godkendt mere end én europæisk digital identitetstegnebogsløsning på sit område. For at undgå fastlåsning i sådanne situationer bør udbydere af europæiske digitale identitetstegnebøger, hvor det er teknisk muligt, sikre effektiv dataportabilitet efter anmodning fra brugere af europæiske digitale identitetstegnebøger og bør ikke kunne anvende kontraktlige, økonomiske eller tekniske hindringer for at forhindre eller afskrække fra effektive skift mellem forskellige europæiske digitale identitetstegnebøger.

(49) For at sikre, at europæiske digitale identitetstegnebøger fungerer korrekt, har udbydere af europæiske digitale identitetstegnebøger behov for effektiv interoperabilitet og retfærdige, rimelige og ikkediskriminerende betingelser for, at de europæiske digitale identitetstegnebøger kan få adgang til specifikke hardware- og softwarefunktioner på mobile enheder. Disse komponenter vil navnlig kunne omfatte near-field-communication-antenner og sikre elementer, herunder universelle integrerede kredsløbskort, indbyggede sikre elementer, mikroSD-kort og Bluetooth Low Energy. Adgangen til disse komponenter vil kunne være kontrolleret af mobilnetoperatører og udstyrsfabrikanter. Hvor det er nødvendigt for at levere tjenester fra europæiske digitale identitetstegnebøger, bør fabrikanter af originaludstyr til mobile enheder eller udbydere af elektroniske kommunikationstjenester derfor ikke nægte adgang til sådanne komponenter. Desuden bør de virksomheder, der er udpeget som gatekeepere for centrale platformstjenester som anført af Kommissionen i medfør af Europa-Parlamentets og Rådets forordning (EU) 2022/1925 ([14]), fortsat være omfattet af de specifikke bestemmelser i nævnte forordning på grundlag af artikel 6, stk. 7, deri.

(50) For at strømline de forpligtelser vedrørende cybersikkerhed, der pålægges tillidstjenesteudbydere, og for at gøre det muligt for disse udbydere og deres respektive kompetente myndigheder at drage fordel af den retlige ramme, der er fastlagt ved direktiv (EU) 2022/2555, er tillidstjenester forpligtet til at træffe passende tekniske og organisatoriske foranstaltninger i medfør af nævnte direktiv såsom foranstaltninger til håndtering af systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener med henblik på at styre risiciene for sikkerheden i de net- og informationssystemer, som disse udbydere anvender som led i deres levering af tjenester, samt foretage underretninger om væsentlige hændelser og cybertrusler i overensstemmelse med nævnte direktiv. For så vidt angår underretning om hændelser bør tillidstjenesteudbydere underrette om alle hændelser, der har en væsentlig indvirkning på leveringen af deres tjenester, herunder som følge af tyveri eller tab af udstyr, skader på netkabler eller hændelser, der indtræffer i forbindelse med identifikation af personer. Kravene vedrørende risikostyring i forbindelse med cybersikkerhed og rapporteringsforpligtelserne i henhold til direktiv (EU) 2022/2555 bør betragtes som værende et supplement til de krav, der pålægges tillidstjenesteudbydere i henhold til denne forordning. Hvis det er relevant, bør fastsatte nationale praksisser eller retningslinjer i forbindelse med gennemførelsen af sikkerheds- og rapporteringskrav og tilsyn med overholdelsen af sådanne krav i henhold til forordning (EU) nr. 910/2014 fortsat anvendes af de kompetente myndigheder, der er udpeget i henhold til direktiv (EU) 2022/2555. Nærværende forordning berører ikke forpligtelsen til i medfør af forordning (EU) 2016/679 at anmelde brud på persondatasikkerheden.

([13]) 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).

([14]) Europa-Parlamentets og Rådets forordning (EU) 2022/1925 af 14. september 2022 om åbne og fair markeder i den digitale sektor og om ændring af direktiv (EU) 2019/1937 og (EU) 2020/1828 (forordningen om digitale markeder) (EUT L 265 af 12.10.2022, s. 1).

(51) Der bør tages behørigt hensyn til at sikre et effektivt samarbejde mellem de tilsynsorganer, der er udpeget i henhold til artikel 46b i forordning (EU) nr. 910/2014, og de kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555. Hvis et sådant tilsynsorgan er et andet end en sådan kompetent myndighed, bør de samarbejde tæt og på en rettidig måde ved at udveksle relevante oplysninger med henblik på at sikre et effektivt tilsyn med tillidstjenesteudbyderne og deres overholdelse af de krav, der er fastsat i forordning (EU) nr. 910/2014 og direktiv (EU) 2022/2555. Tilsynsorganer, der er udpeget i henhold til forordning (EU) nr. 910/2014, bør navnlig have ret til at anmode kompetente myndigheder, der er udpeget i henhold til direktiv (EU) 2022/2555, om at fremlægge de relevante oplysninger, der er nødvendige for at tildele status som kvalificeret og gennemføre tilsynsforanstaltninger for at kontrollere, at tillidstjenesteudbyderne overholder de i henhold til direktiv (EU) 2022/2555 relevante krav, eller pålægge dem at afhjælpe manglende overholdelse.

(52) Det er afgørende at fastlægge en retlig ramme for at lette grænseoverskridende anerkendelse mellem eksisterende nationale retlige systemer vedrørende elektroniske registrerede leveringstjenester. Denne ramme vil også kunne åbne nye markedsmuligheder for tillidstjenesteudbydere i Unionen med hensyn til at udbyde nye EU-dækkende tjenester for elektroniske registrerede leveringstjenester. For at sikre, at data via en kvalificeret elektronisk registreret leveringstjeneste leveres til den korrekte modtager, bør kvalificerede elektroniske registrerede leveringstjenester med fuldstændig sikkerhed sikre identifikation af modtageren, mens en høj grad af tillid vil være tilstrækkelig for så vidt angår identifikation af afsenderen. Medlemsstaterne bør tilskynde udbydere af kvalificerede elektroniske registrerede leveringstjenester til at gøre deres tjenester interoperable med kvalificerede elektroniske registrerede leveringstjenester, der leveres af andre kvalificerede tillidstjenesteudbydere, for at der nemt kan overføres elektronisk registrerede data mellem to eller flere kvalificerede tillidstjenesteudbydere, og for at fremme fair praksis på det indre marked.

(53) I de fleste tilfælde er unionsborgere og indbyggere i Unionen ikke i stand til at udveksle digitale oplysninger vedrørende deres identitet såsom deres adresser, alder, erhvervsmæssige kvalifikationer, kørekort og andre tilladelser og betalingsdata på tværs af grænserne på sikker vis og med et højt databeskyttelsesniveau.

(54) Det bør være muligt at udstede og håndtere pålidelige elektroniske attributter og bidrage til at mindske den administrative byrde og derved give unionsborgere og indbyggere i Unionen mulighed for at anvende dem i deres private og offentlige transaktioner. Unionsborgere og indbyggere i Unionen bør for eksempel være i stand til at dokumentere, at de er i besiddelse af et gyldigt kørekort, der er udstedt af en myndighed i én medlemsstat, hvilket de relevante myndigheder i andre medlemsstater kan kontrollere og have tillid til, og til at forlade sig på deres socialsikringsoplysninger eller fremtidige digitale rejsedokumenter i grænseoverskridende sammenhæng.

(55) Enhver tjenesteudbyder, der udsteder attesterede attributter i elektronisk form såsom eksamensbeviser, tilladelser og fødselsattester eller beføjelser og mandater til at repræsentere eller handle på vegne af fysiske eller juridiske personer bør betragtes som en tillidstjenesteudbyder af elektroniske attesteringer af attributter. En elektronisk attestering af attributter bør ikke nægtes retsvirkning alene af den grund, at den er i elektronisk form, eller at den ikke opfylder kravene til kvalificerede elektroniske attesteringer af attributter. Der bør fastsættes generelle krav for at sikre, at en kvalificeret elektronisk attestering af attributter har samme retsvirkning som lovligt udstedte attesteringer i papirform. Disse krav bør dog finde anvendelse, uden at det berører EU-ret eller national ret, der fastsætter yderligere sektorspecifikke krav for så vidt angår formkrav med underliggende retsvirkning og navnlig grænseoverskridende anerkendelse af kvalificerede elektroniske attesteringer af attributter, hvis det er relevant.

(56) Den brede tilgængelighed og anvendelighed af europæiske digitale identitetstegnebøger bør øge accepten heraf og tilliden til dem både hos privatpersoner og private tjenesteudbydere. De private modtagerparter, der leverer tjenester, f.eks. inden for transport, energi, banktjenester, finansielle tjenesteydelser, social sikring, sundhed, drikkevand, posttjenester, digital infrastruktur, telekommunikation eller uddannelse, bør derfor acceptere anvendelsen af europæiske digitale identitetstegnebøger til levering af tjenester, hvor stærk brugerautentifikation til online-identifikation er påkrævet i henhold til EU-retten eller national ret eller i henhold til en kontraktlig forpligtelse. Enhver anmodning fra modtagerparten om oplysninger fra brugeren af en europæisk digital identitetstegnebog bør være nødvendig for og stå i et rimeligt forhold til den påtænkte anvendelse i et givent tilfælde, bør være i overensstemmelse med princippet om dataminimering og bør sikre gennemsigtighed med hensyn til, hvilke data der deles, og til hvilke formål. For at lette anvendelsen og accepten af europæiske digitale identitetstegnebøger bør der i forbindelse med deres udbredelse tages hensyn til bredt anerkendte industristandarder og -specifikationer.

(57) Hvis meget store onlineplatforme i den i artikel 33, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2022/2065 ([15]) anvendte betydning kræver, at brugere autentificeres for at få adgang til onlinetjenester, bør disse platforme være forpligtet til at acceptere anvendelse af europæiske digitale identitetstegnebøger, når brugeren frivilligt anmoder herom. Brugere bør ikke være forpligtede til at anvende en europæisk digital identitetstegnebog for at få adgang til private tjenester, og deres adgang til tjenester bør ikke begrænses eller hindres med den begrundelse, at de ikke anvender en europæisk digital identitetstegnebog. Hvis brugerne imidlertid ønsker det, bør meget store onlineplatforme acceptere dem til dette formål, samtidig med at princippet om dataminimering og brugernes ret til frit valgte pseudonymer respekteres. I betragtning af den betydning, som meget store onlineplatforme har grundet deres rækkevidde, navnlig som udtrykt i antallet af modtagere af en tjeneste og økonomiske transaktioner, er forpligtelsen til at acceptere europæiske digitale identitetstegnebøger nødvendig for at øge beskyttelsen af brugerne mod svig og sikre et højt databeskyttelsesniveau.

(58) Der bør udarbejdes adfærdskodekser på EU-plan med henblik på at bidrage til udbredt tilgængelighed og anvendelighed af elektroniske identifikationsmidler, herunder europæiske digitale identitetstegnebøger, inden for denne forordnings anvendelsesområde. Adfærdskodekserne bør lette en bred accept af elektroniske identifikationsmidler, herunder europæiske digitale identitetstegnebøger, hos de tjenesteudbydere, der ikke betragtes som meget store platforme, og som benytter tredjeparters elektroniske identifikationstjenester til brugerautentifikation.

(59) Selektiv videregivelse er et begreb, der giver ejeren af data mulighed for kun at videregive visse dele af et større datasæt, således at den modtagende enhed kun modtager de oplysninger, som er nødvendige for leveringen af en tjeneste, som en bruger har anmodet om. Den europæiske digitale identitetstegnebog bør gøre selektiv videregivelse af attributter til modtagerparter teknisk mulig. Det bør være teknisk muligt for brugeren selektivt at videregive attributter, herunder fra flere særskilte elektroniske attesteringer, og kombinere og fremlægge dem gnidningsløst for modtagerparter. Denne funktion bør blive et grundlæggende element i udformningen af europæiske digitale identitetstegnebøger og derved styrke bekvemmeligheden og beskyttelsen af personoplysninger, herunder dataminimering.

(60) Medmindre specifikke regler i EU-retten eller national ret kræver, at brugerne identificerer sig selv, bør adgang til tjenester ved hjælp af et pseudonym ikke forbydes.

(61) Attributter, der leveres af kvalificerede tillidstjenesteudbydere som led i kvalificerede attesteringer af attributter, bør kontrolleres i forhold til autentiske kilder enten direkte af den kvalificerede tillidstjenesteudbyder eller ved hjælp af udpegede mellemmænd, der er anerkendt på nationalt plan i overensstemmelse med EU-retten eller national ret, med henblik på sikker udveksling af attesterede attributter mellem udbydere af identitetstjenester eller attesteringer af attributter og modtagerparter. Medlemsstaterne bør indføre passende mekanismer på nationalt plan for at sikre, at kvalificerede tillidstjenesteudbydere, der udsteder kvalificeret elektronisk attestering af attributter, er i stand til på grundlag af samtykke fra den person, som attesten er udstedt til, at kontrollere ægtheden af attributterne på grundlag af autentiske kilder. Det bør være muligt for passende mekanismer at omfatte anvendelsen af specifikke mellemmænd eller tekniske løsninger i overensstemmelse med national ret, der giver adgang til autentiske kilder. At sikre, at en mekanisme, der gør det muligt at kontrollere attributter i forhold til autentiske kilder, er til rådighed, har til formål at gøre det lettere for kvalificerede tillidstjenesteudbydere af kvalificeret elektronisk attestering af attributter at overholde deres forpligtelser i henhold til forordning (EU) nr. 910/2014. Et nyt bilag til nævnte forordning bør indeholde en liste over kategorier af attributter med hensyn til hvilke medlemsstaterne skal sikre, at der træffes foranstaltninger, der gør det muligt for kvalificerede udbydere af elektroniske attesteringer af attributter på brugerens anmodning elektronisk at kontrollere deres ægthed i forhold til den relevante autentiske kilde.

(62) Sikker elektronisk identifikation og levering af attesteringer af attributter bør give sektoren for finansielle tjenesteydelser yderligere fleksibilitet og løsninger, således at det bliver muligt at identificere kunder og udveksle specifikke attributter for at overholde f.eks. kundekendskabskravene i henhold til en fremtidig forordning om oprettelse af myndigheden for bekæmpelse af hvidvask af penge eller egnethedskrav, der følger af investorbeskyttelsesret, eller for at støtte opfyldelsen af krav om stærk kundeautentifikation til onlineidentifikation med henblik på kontologin og iværksættelse af transaktioner inden for betalingstjenester.

(63) Retsvirkningen af en elektronisk signatur skal ikke anfægtes, alene af den grund at den er i elektronisk form, eller at den ikke opfylder kravene til en kvalificeret elektronisk signatur. Elektroniske signaturers retsvirkning skal dog fastlægges i national ret, med undtagelse af kravene i denne forordning, der fastsætter, at retsvirkningen af en kvalificeret elektronisk signatur skal anses for at svare til en håndskreven underskrift. Ved fastlæggelsen af

([15]) Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EUT L 277 af 27.10.2022, s. 1).

elektroniske signaturers retsvirkning bør medlemsstaterne tage hensyn til princippet om proportionalitet mellem den retlige værdi af et dokument, der skal underskrives, og det sikkerhedsniveau og de omkostninger, som en elektronisk signatur kræver. For at øge tilgængeligheden og anvendelsen af elektroniske signaturer opfordres medlemsstaterne til at overveje at anvende avancerede elektroniske signaturer i de daglige transaktioner, for hvilke de giver et tilstrækkeligt niveau af sikkerhed og tillid.

(64) For at sikre ensartet certificeringspraksis i hele Unionen bør Kommissionen udstede retningslinjer for certificering og fornyet certificering af kvalificerede elektroniske signaturgenereringssystemer og af kvalificerede elektroniske seglgenereringssystemer, herunder deres gyldighed og tidsmæssige begrænsninger. Denne forordning forhindrer ikke offentlige eller private organer, der har certificerede kvalificerede elektroniske signaturgenereringssystemer, i midlertidigt at forny certificeringen af sådanne systemer for en kortvarig certificeringsperiode på grundlag af resultatet af den seneste certificeringsproces, hvor en sådan fornyet certificering ikke kan foretages inden for den lovbestemte tidsramme af andre årsager end et brud eller en sikkerhedshændelse, og uden at det berører forpligtelsen til at foretage en sårbarhedsvurdering, og uden at det berører gældende certificeringspraksis.

(65) Udstedelsen af certifikater for webstedsautentifikation har til formål at give brugere en sikkerhed med en høj grad af tillid til identiteten af den enhed, der står bag et websted, uanset hvilken platform der anvendes til at vise denne identitet. Disse certifikater bør bidrage til at opbygge tillid til at drive forretning online, da brugerne vil have tillid til et websted, som er autentificeret. Websteders brug af sådanne certifikater bør være frivillig. For at sådanne certifikater kan blive et middel til at fremme tillid, give brugeren en bedre oplevelse og fremme vækst på det indre marked, fastsættes der ved denne forordning en tillidsramme inklusive minimumsforpligtelser med hensyn til sikkerhed og ansvar for udbydere af kvalificerede certifikater for webstedsautentifikation og krav til udstedelsen af disse certifikater. Webstedsautentifikationstjenesters og deres tillidstjenesteudbyderes status som kvalificeret bør bekræftes af nationale positivlister, herunder deres fulde overholdelse af denne forordnings krav med hensyn til udstedelse af kvalificerede certifikater for webstedsautentifikation. Anerkendelsen af kvalificerede certifikater for webstedsautentifikation betyder, at webbrowserudbydere ikke bør nægte autenticiteten af kvalificerede certifikater for webstedsautentifikation med det ene formål at attestere tilknytningen mellem webstedets domænenavn og den fysiske eller juridiske person, som certifikatet er udstedt til, eller bekræfte den pågældende persons identitet. Webbrowserudbydere bør vise de certificerede identitetsdata og de øvrige attesterede attributter for slutbrugeren på en brugervenlig måde i browsermiljøet ved tekniske midler efter eget valg. Med henblik herpå bør webbrowserudbydere sørge for støtte af og interoperabilitet med kvalificerede certifikater for webstedsautentifikation udstedt under fuld overholdelse af denne forordning. Forpligtelsen til anerkendelse af, interoperabilitet med og støtte til kvalificerede certifikater for webstedsautentifikation berører ikke webbrowserudbyderes frihed til at sikre websikkerhed, domæneautentifikation og kryptering af webtrafik på en måde og ved brug af teknologi, som de anser for at være den mest hensigtsmæssige. For at bidrage til slutbrugernes onlinesikkerhed bør webbrowserudbydere under ekstraordinære omstændigheder kunne træffe forebyggende foranstaltninger, der er både nødvendige og forholdsmæssige, som reaktion på en begrundet mistanke om sikkerhedsbrud eller tab af integritet i forbindelse med et identificeret certifikat eller sæt af certifikater. Hvor webbrowserudbydere træffer sådanne forebyggende foranstaltninger, bør de uden unødigt ophold underrette Kommissionen, det nationale tilsynsorgan og den enhed, som certifikatet er udstedt til, samt den kvalificerede tillidstjenesteudbyder, der udstedte det pågældende certifikat eller sæt af certifikater, om enhver mistanke med hensyn til et sådant sikkerhedsbrud eller tab af integritet samt om de foranstaltninger, der er truffet i forbindelse med det enkelte certifikat eller sættet af certifikater. Disse foranstaltninger bør ikke berøre webbrowserudbyderes forpligtelse til at anerkende kvalificerede certifikater for webstedsautentifikation i overensstemmelse med de nationale positivlister. For yderligere at beskytte unionsborgerne og indbyggerne i Unionen og fremme brugen af kvalificerede certifikater for webstedsautentifikation bør offentlige myndigheder i medlemsstaterne overveje at indføre kvalificerede certifikater for webstedsautentifikation for deres websteder. De foranstaltninger, der er fastsat i denne forordning med henblik på at skabe større sammenhæng mellem medlemsstaternes forskellige tilgange og praksis vedrørende tilsynsprocedurer, har til formål at bidrage til at øge tilliden til sikkerheden, kvaliteten og tilgængeligheden af kvalificerede certifikater for webstedsautentifikation.

(66) Mange medlemsstater har indført nationale krav til tjenester, der leverer sikker og pålidelig elektronisk arkivering, for at gøre det muligt at opbevare elektroniske data og elektroniske dokumenter i lang tid, og tilknyttede tillidstjenester. For at sikre retssikkerhed, tillid og harmonisering på tværs af medlemsstaterne bør der fastlægges en retlig ramme for kvalificerede elektroniske arkiveringstjenester, der er inspireret af rammen for de andre tillidstjenester, der er fastsat i denne forordning. Denne retlige ramme for kvalificerede elektroniske arkiveringstjenester bør give tillidstjenesteudbydere og -brugere en effektiv værktøjskasse, der omfatter funktionelle krav til den elektroniske arkiveringstjeneste, samt klare retsvirkninger, når der anvendes en kvalificeret elektronisk arkiveringstjeneste. Disse bestemmelser bør gælde for elektroniske data og elektroniske dokumenter, der er oprettet i elektronisk form, og papirdokumenter, der er blevet scannet og digitaliseret. Når det kræves, bør det i henhold til disse bestemmelser være

tilladt at overføre de opbevarede elektroniske data og elektroniske dokumenter til forskellige medier eller formater med henblik på at forlænge deres holdbarhed og læsbarhed ud over den teknologiske gyldighedsperiode og samtidig i videst mulige omfang forebygge tab og ændringer. Når elektroniske data og elektroniske dokumenter, der indgives til den elektroniske arkivtjeneste, indeholder én eller flere kvalificerede elektroniske signaturer eller kvalificerede elektroniske segl, bør tjenesten anvende procedurer og teknologier, der kan forlænge deres pålidelighed for opbevaringsperioden for sådanne data, eventuelt ved brug af andre kvalificerede tillidstjenester, der er oprettet ved denne forordning. Der bør anvendes kvalificerede tillidstjenester med henblik på at frembringe opbevaringsdokumentation, hvor der anvendes elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler. I det omfang elektroniske arkiveringstjenester ikke er harmoniseret ved denne forordning, bør det være muligt for medlemsstaterne i overensstemmelse med EU-retten at opretholde eller indføre nationale bestemmelser vedrørende disse tjenester såsom specifikke bestemmelser for tjenester, der er integreret i en organisation og udelukkende anvendes til denne organisations interne arkiver. I denne forordning bør der ikke skelnes mellem elektroniske data og elektroniske dokumenter, der er oprettet i elektronisk form, og fysiske dokumenter, der er blevet digitaliseret.

(67) Nationale arkivers og hukommelsesinstitutioners aktiviteter er i deres egenskab af organisationer, der har til opgave at bevare den dokumenterede arv i offentlighedens interesse, normalt reguleret i national ret og ret, og de leverer ikke nødvendigvis tillidstjenester i den i denne forordning anvendte betydning. For så vidt sådanne institutioner ikke leverer sådanne tillidstjenester, berører denne forordning ikke deres drift.

(68) Elektroniske hovedbøger er en sekvens af elektroniske dataposter, der bør sikre deres integritet og nøjagtigheden af deres kronologiske rækkefølge. Elektroniske hovedbøger bør fastlægge en kronologisk sekvens af dataposter. Sammen med andre teknologier bør de bidrage til løsninger med henblik på mere effektive og transformative offentlige tjenester såsom elektronisk afstemning, grænseoverskridende samarbejde mellem toldmyndighederne, grænseoverskridende samarbejde mellem akademiske institutioner og registrering af ejerskab til fast ejendom i decentrale matrikelregistre. Kvalificerede elektroniske hovedbøger bør indføre en retlig formodning for den entydige og nøjagtige kronologiske rækkefølge og integritet af dataposterne i hovedbogen. På grund af deres særtræk såsom den sekventielle kronologiske rækkefølge af dataposterne bør elektroniske hovedbøger adskilles fra andre tillidstjenester såsom elektroniske tidsstempler og elektroniske registrerede leveringstjenester. For at sikre retssikkerhed og fremme innovation bør der fastlægges en EU-dækkende retlig ramme, der fastsætter grænseoverskridende anerkendelse af tillidstjenester med hensyn til registrering af data i elektroniske hovedbøger. Dette bør i tilstrækkelig grad forhindre, at det samme digitale aktiv kopieres og sælges mere end én gang til forskellige parter. Processen med at oprette og ajourføre en elektronisk hovedbog afhænger af, hvilken type hovedbog der anvendes, navnlig hvorvidt den er centraliseret eller distribueret. Denne forordning bør sikre teknologisk neutralitet, dvs. at den hverken begunstiger eller forskelsbehandler nogen teknologi, som anvendes til at gennemføre den nye tillidstjeneste for elektroniske hovedbøger. Desuden bør Kommissionen tage højde for bæredygtighedsindikatorer med hensyn til eventuelle negative indvirkninger på klimaet eller andre miljørelaterede negative indvirkninger ved hjælp af hensigtsmæssige metoder, når den udarbejder de gennemførelsesretsakter, der præciserer kravene til kvalificerede elektroniske hovedbøger.

(69) Tillidstjenesteudbyderes rolle i forbindelse med elektroniske hovedbøger bør være at fastslå den sekventielle registrering af data i hovedbogen. Denne forordning berører ikke eventuelle retlige forpligtelser, som brugere af elektroniske hovedbøger har i henhold til EU-retten eller national ret. F.eks. bør brugstilfælde, der involverer behandling af personoplysninger, overholde forordning (EU) 2016/679, og brugstilfælde, som vedrører finansielle tjenesteydelser, bør overholde relevant EU-ret om finansielle tjenesteydelser.

(70) For at undgå fragmentering af og hindringer på det indre marked som følge af divergerende standarder og tekniske restriktioner og for at sikre en koordineret proces, hvorved det undgås at påvirke gennemførelsen af den europæiske ramme for digital identitet, er der behov for en procedure for et tæt og struktureret samarbejde mellem Kommissionen, medlemsstaterne, civilsamfundet, den akademiske verden og den private sektor. For at nå dette mål bør medlemsstaterne og Kommissionen samarbejde inden for de rammer, der er fastsat i Kommissionens henstilling (EU) 2021/946 ([16]) om at udarbejde en fælles EU-værktøjskasse for den europæiske ramme for digital identitet. I den forbindelse bør medlemsstaterne nå til enighed om en omfattende teknisk struktur og referenceramme, et sæt fælles standarder og tekniske referencer, herunder anerkendte eksisterende standarder, og et sæt retningslinjer for og beskrivelser af bedste praksis, der som minimum dækker hele funktionaliteten og interoperabiliteten af europæiske digitale identitetstegnebøger, herunder e-signaturer, og af de kvalificerede tillidstjenesteudbydere af elektronisk attestering af attributter som fastsat i denne forordning. I den forbindelse bør medlemsstaterne også nå til enighed om fælles elementer med hensyn til en forretningsmodel og en gebyrstruktur for europæiske digitale

([16]) 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).

identitetstegnebøger for at lette udbredelsen, navnlig blandt SMV'er, i en grænseoverskridende sammenhæng. Værktøjskassens indhold bør udvikles parallelt med og bør afspejle resultatet af drøftelserne af og processen for vedtagelsen af den europæiske ramme for digital identitet.

(71) Denne forordning fastsætter et harmoniseret niveau af kvalitet, pålidelighed og sikkerhed for kvalificerede tillidstjenester, uanset hvor aktiviteterne udføres. En kvalificeret tillidstjenesteudbyder bør derfor have mulighed for at outsource sine aktiviteter i forbindelse med levering af en kvalificeret tillidstjeneste til et tredjeland, hvor dette tredjeland giver tilstrækkelige garantier, der sikrer, at tilsynsaktiviteter og revisioner kan håndhæves, som om de blev udført i Unionen. Når overholdelsen af denne forordning ikke kan sikres fuldt ud, bør tilsynsorganerne kunne vedtage forholdsmæssige og begrundede foranstaltninger, herunder inddragelse af status som kvalificeret for den udbudte tillidstjeneste.

(72) For at sikre retssikkerhed for så vidt angår gyldigheden af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater, er det afgørende at angive vurderingen, som udføres af den modtagerpart, som foretager valideringen af den pågældende avancerede elektroniske signatur, der er baseret på kvalificerede certifikater.

(73) Tillidstjenesteudbydere bør anvende kryptografiske metoder, der afspejler nuværende bedste praksis og pålidelige implementeringer af disse algoritmer, for at sikre deres tillidstjenesters sikkerhed og pålidelighed.

(74) Denne forordning fastsætter en forpligtelse for kvalificerede tillidstjenesteudbydere til at kontrollere identiteten af en fysisk eller juridisk person, som det kvalificerede certifikat eller den kvalificerede elektroniske attestering af attributter er udstedt til, på grundlag af forskellige harmoniserede metoder i hele Unionen. For at sikre, at kvalificerede certifikater og kvalificerede elektroniske attesteringer af attributter udstedes til den person, de tilhører, og at de attesterer det korrekte og unikke sæt data, der repræsenterer den pågældende persons identitet, bør kvalificerede tillidstjenesteudbydere, der udsteder kvalificerede certifikater eller udsteder kvalificerede elektroniske attesteringer af attributter, på tidspunktet for udstedelsen af disse certifikater og attesteringer med fuld sikkerhed sikre identifikationen af denne person. Ud over den obligatoriske kontrol af personens identitet, hvis det er relevant for udstedelse af kvalificerede certifikater, og når der udstedes en kvalificeret elektronisk attestering af attributter, bør kvalificerede tillidstjenesteudbydere desuden med fuld sikkerhed sikre korrektheden og nøjagtigheden af de attesterede attributter hos den person, som det kvalificerede certifikat eller den kvalificerede elektroniske attestering af attributter udstedes til. Disse forpligtelser til resultat og fuld sikkerhed i forbindelse med kontrollen af de attesterede data bør understøttes af passende midler, herunder ved hjælp af én metode eller, hvis det er nødvendigt, en kombination af specifikke metoder fastsat i denne forordning. Det bør være muligt at kombinere disse metoder for at skabe et passende grundlag for kontrol af identiteten af den person, som det kvalificerede certifikat eller en kvalificeret elektronisk attestering af attributter udstedes til. Det bør være muligt for en sådan kombination at omfatte benyttelse af elektroniske identifikationsmidler, der opfylder kravene til sikringsniveauet »betydelig«, kombineret med andre metoder til identitetskontrol. Sådan elektronisk identifikation vil gøre det muligt at opfylde de harmoniserede krav i denne forordning for så vidt angår sikringsniveauet »høj« som led i yderligere harmoniserede procedurer på afstand, hvilket sikrer identifikation med en høj grad af tillid. Disse metoder bør omfatte muligheden for, at den kvalificerede tillidstjenesteudbyder, som udsteder en kvalificeret elektronisk attestering af attributter, på brugerens anmodning kan kontrollere de attributter, der skal attesteres, herunder i forhold til autentiske kilder, ved hjælp af elektroniske midler i overensstemmelse med EU-retten eller national ret.

(75) For at sikre denne forordnings overensstemmelse med den globale udvikling og følge bedste praksis på det indre marked bør de delegerede retsakter og gennemførelsesretsakter, som Kommissionen vedtager, revideres og om nødvendigt ajourføres regelmæssigt. Ved vurderingen af nødvendigheden af disse ajourføringer bør der tages hensyn til nye teknologier, praksisser, standarder eller tekniske specifikationer.

(76) Målene for denne forordning, nemlig at udvikle den EU-dækkende europæiske ramme for digital identitet og en ramme for tillidstjenester, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af deres omfang og virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå disse mål.

(77) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725.

(78) Forordning (EU) nr. 910/2014 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE FORORDNING:

Artikel 1

Ændringer til forordning (EU) nr. 910/2014

I forordning (EU) nr. 910/2014 foretages følgende ændringer:

1) Artikel 1 affattes således:

»*Artikel 1*

Genstand

Denne forordning har til formål at sikre et velfungerende indre marked og et tilstrækkeligt sikkerhedsniveau for elektroniske identifikationsmidler og tillidstjenester, som anvendes i hele Unionen, for at muliggøre og lette fysiske og juridiske personers udøvelse af retten til at deltage sikkert i det digitale samfund og få adgang til offentlige og private onlinetjenester i hele Unionen. Med henblik herpå omfatter denne forordning:

a) fastsættelse af betingelser i henhold til hvilke medlemsstaterne skal anerkende fysiske og juridiske personers elektroniske identifikationsmidler, der er omfattet af en anmeldt elektronisk identifikationsordning i en anden medlemsstat, og levere og anerkende europæiske digitale identitetstegnebøger

b) fastsættelse af regler for tillidstjenester, navnlig for elektroniske transaktioner

c) fastlæggelse af et retsgrundlag for elektroniske signaturer, elektroniske segl, elektroniske tidsstempler, elektroniske dokumenter, elektroniske registrerede leveringstjenester, certificeringstjenester for webstedsautentifikation, elektronisk arkivering, elektronisk attestering af attributter, elektroniske signaturgenereringssystemer og elektroniske sejlgenereringssystemer samt elektroniske hovedbøger.«

2) I artikel 2 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Denne forordning finder anvendelse på elektroniske identifikationsordninger, der er anmeldt af en medlemsstat, på europæiske digitale identitetstegnebøger, der er leveret af en medlemsstat, og på tillidstjenesteudbydere, der er hjemmehørende i Unionen.«

b) Stk. 3 affattes således:

»3. Denne forordning påvirker ikke EU-ret eller national ret vedrørende kontrakters indgåelse og gyldighed, andre retlige eller proceduremæssige forpligtelser, der vedrører formkrav, eller sektorspecifikke krav, der vedrører formkrav.

4. Denne forordning berører ikke Europa-Parlamentets og Rådets forordning (EU) 2016/679 (*).

(*) 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).«

3) I artikel 3 foretages følgende ændringer:

a) Nr. 1)-5) affattes således:

»1) »elektronisk identifikation«: det at bruge personidentifikationsdata i elektronisk form, der entydigt repræsenterer enten en fysisk eller en juridisk person eller en fysisk person, der repræsenterer en anden fysisk person eller en juridisk person

2) »elektronisk identifikationsmiddel«: en materiel og/eller immateriel enhed, der indeholder personidentifikationsdata, og som bruges til autentifikation i forbindelse med en onlinetjeneste eller, hvis det er relevant, en offlinetjeneste

3) »personidentifikationsdata«: et sæt data, der er udstedt i overensstemmelse med EU-retten eller national ret, og som gør det muligt at fastslå identiteten på en fysisk eller juridisk person eller på en fysisk person, der repræsenterer en anden fysisk person eller en juridisk person

4) »elektronisk identifikationsordning«: et system til elektronisk identifikation, som led i hvilket der udstedes elektroniske identifikationsmidler til fysiske eller juridiske personer eller til fysiske personer, der repræsenterer andre fysiske personer eller juridiske personer

5) »autentifikation«: en elektronisk proces, der muliggør bekræftelse af den elektroniske identifikation af en fysisk eller juridisk person eller bekræftelse af oprindelsen og integriteten af data i elektronisk form«.

b) Følgende nummer indsættes:

»5a) »bruger«: en fysisk eller juridisk person eller en fysisk person, der repræsenterer en anden fysisk person eller en juridisk person, som anvender tillidstjenester eller elektroniske identifikationsmidler, der leveres i overensstemmelse med denne forordning«.

c) Nr. 6) affattes således:

»6) »modtagerpart«: en fysisk eller juridisk person, der er afhængig af elektronisk identifikation, europæiske digitale identitetstegnebøger eller andre elektroniske identifikationsmidler eller af en tillidstjeneste«.

d) Nr. 16) affattes således:

»16) »tillidstjeneste«: en elektronisk tjeneste, der normalt udføres mod betaling, og som består af et eller flere af følgende:

a) udstedelse af certifikater for elektroniske signaturer, certifikater for elektroniske segl, certifikater for webstedsautentifikation eller certifikater for levering af andre tillidstjenester

b) validering af certifikater for elektroniske signaturer, certifikater for elektroniske segl, certifikater for webstedsautentifikation eller certifikater for levering af andre tillidstjenester

c) generering af elektroniske signaturer eller elektroniske segl

d) validering af elektroniske signaturer eller elektroniske segl

e) bevaring af elektroniske signaturer, elektroniske segl, certifikater for elektroniske signaturer eller certifikater for elektroniske segl

f) forvaltning af elektroniske signaturgenereringssystemer på afstand eller elektroniske seglgenereringssystemer på afstand

g) udstedelse af elektroniske attesteringer af attributter

h) validering af elektronisk attestering af attributter

i) generering af elektroniske tidsstempler

j) validering af elektroniske tidsstempler

k) udførelse af elektroniske registrerede leveringstjenester

l) validering af data fremsendt via elektroniske registrerede leveringstjenester og tilhørende dokumentation

m) elektronisk arkivering af elektroniske data og elektroniske dokumenter

n) registrering af elektroniske data i en elektronisk hovedbog«.

e) Nr. 18) affattes således:

»18) »overensstemmelsesvurderingsorgan«: et overensstemmelsesvurderingsorgan som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008, der er akkrediteret i overensstemmelse med nævnte forordning med kompetence til at udføre overensstemmelsesvurderinger af en kvalificeret tillidstjenesteudbyder og de kvalificerede tillidstjenester, den udbyder, eller med kompetence til at udføre certificering af europæiske digitale identitetstegnebøger eller elektroniske identifikationsmidler«.

f) Nr. 21) affattes således:

»21) »produkt«: hardware eller software eller relevante hardware- eller softwarekomponenter, som er beregnet til at blive brugt til levering af elektroniske identifikationstjenester og tillidstjenester«.

g) Følgende numre indsættes:

»23a) »kvalificeret elektronisk signaturgenereringssystem på afstand«: et kvalificeret elektronisk signaturgenereringssystem, der i overensstemmelse med artikel 29a forvaltes af en kvalificeret tillidstjenesteudbyder på vegne af en underskriver

23b) »kvalificeret elektronisk seglgenereringssystem på afstand«: et kvalificeret elektronisk seglgenereringssystem, der i overensstemmelse med artikel 39a forvaltes af en kvalificeret tillidstjenesteudbyder på vegne af en forseglende part«.

h) Nr. 38) affattes således:

»38) »certifikat for webstedsautentifikation«: en elektronisk attestering, der gør det muligt at autentificere et websted og knytter webstedet til den fysiske eller juridiske person, som certifikatet er udstedt til«.

i) Nr. 41) affattes således:

»41) »validering«: en fremgangsmåde til at kontrollere og bekræfte gyldigheden af data i elektronisk form i overensstemmelse med kravene i denne forordning«.

j) Følgende numre tilføjes:

»42) »europæisk digital identitetstegnebog«: et elektronisk identifikationsmiddel, der gør det muligt for brugeren på sikker vis at lagre, forvalte og validere personidentifikationsdata og elektroniske attesteringer af attributter med henblik på at levere dem til modtagerparter og andre brugere af europæiske digitale identitetstegnebøger og at underskrive ved hjælp af kvalificerede elektroniske signaturer eller forsegle ved hjælp af kvalificerede elektroniske segl

43) »attribut«: en fysisk eller juridisk persons eller en genstands egenskab, kvalitet, rettigheder eller tilladelser

44) »elektronisk attestering af attributter«: en attestering i elektronisk form, der muliggør autentifikation af attributter

45) »kvalificeret elektronisk attestering af attributter«: en elektronisk attestering af attributter, der er udstedt af en kvalificeret tillidstjenesteudbyder, og som opfylder de krav, der er fastsat i bilag V

46) »elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde«: en elektronisk attestering af attributter, der er udstedt af en offentlig myndighed med ansvar for en autentisk kilde eller af en offentlig myndighed udpeget af medlemsstaten til at udstede sådanne attesteringer af attributter på vegne af de offentlige myndigheder med ansvar for autentiske kilder i overensstemmelse med artikel 45f og bilag VII

47) »autentisk kilde«: et register eller et system, som en offentlig myndighed eller en privat enhed har ansvaret for, og som indeholder og leverer attributter om en fysisk eller juridisk person eller genstand, og som anses for at være en primær kilde til disse oplysninger eller er anerkendt som autentisk i overensstemmelse med EU-retten eller national ret, herunder administrativ praksis

48) »elektronisk arkivering«: en tjeneste, der sikrer 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

49) »kvalificeret elektronisk arkiveringstjeneste«: en elektronisk arkiveringstjeneste, der ydes af en kvalificeret tillidstjenesteudbyder og som opfylder de krav, der er fastsat i artikel 45j

50) »EU-tillidsmærke for europæiske digitale identitetstegnebøger«: en kontrollerbar, simpel og genkendelig angivelse, der er meddelt på en tydelig måde, af, at en europæisk digital identitetstegnebog er udstedt i overensstemmelse med denne forordning

51) »stærk brugerautentifikation«: en autentifikation baseret på anvendelse af mindst to autentifikationsfaktorer fra forskellige kategorier af enten viden, noget kun brugeren ved, besiddelse, noget kun brugeren besidder, eller iboende egenskab, noget brugeren er, og som er uafhængige, i den betydning at et brud på et af dem ikke svækker de andres pålidelighed, og som desuden er udformet på en måde, der beskytter fortroligheden af autentifikationsdataene

52) »elektronisk hovedbog«: en sekvens af elektroniske dataposter, der sikrer integriteten af disse registreringer og nøjagtigheden af disse registres kronologiske rækkefølge

53) »kvalificeret elektronisk hovedbog«: en elektronisk hovedbog, der ydes af en kvalificeret tillidstjenesteudbyder og som opfylder de krav, der er fastsat i artikel 45l

54) »personoplysninger«: personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679

55) »identitetssammenkobling«: en proces, hvorved personidentifikationsdata eller personidentifikationsmidler sammenholdes med eller knyttes til en eksisterende konto, der tilhører den samme person

56) »datapost«: elektroniske data, der er registreret med tilhørende metadata til støtte for behandlingen af dataene

57) »offline«: for så vidt angår anvendelse af europæiske digitale identitetstegnebøger, interaktion mellem en bruger og en tredjepart på et fysisk sted ved hjælp af teknologier i umiddelbar nærhed, hvor det ikke er påkrævet, at den europæiske digitale identitetstegnebog kan få adgang til fjernsystemer via elektroniske kommunikationsnet med henblik på interaktionen«.

4) Artikel 5 affattes således:

»*Artikel 5*

Pseudonymer i elektroniske transaktioner

Uden at det berører specifikke regler i EU-retten eller national ret, der kræver, at brugere identificerer sig selv, eller den retsvirkning, der tillægges pseudonymer i henhold til national ret, må anvendelsen af de pseudonymer, som brugeren har valgt, ikke forbydes.«

5) I kapitel II indsættes følgende afdeling:

»AFDELING 1

EUROPÆISKE DIGITALE ID-TEGNEBØGER

Artikel 5a

Europæiske digitale identitetstegnebøger

1. Med henblik på at sikre, at alle fysiske og juridiske personer i Unionen har sikker, pålidelig og gnidningsløs grænseoverskridende adgang til offentlige og private tjenester og samtidig har fuld kontrol over deres data, skal hver medlemsstat sikre, at der leveres mindst én europæisk digital identitetstegnebog senest 24 måneder efter ikrafttrædelsesdatoen for de gennemførelsesretsakter, der er omhandlet i denne artikels stk. 23 og i artikel 5c, stk. 6.

2. Europæiske digitale identitetstegnebøger leveres på én eller flere af følgende måder:

a) direkte af en medlemsstat

b) i henhold til et mandat fra en medlemsstat

c) uafhængigt af en medlemsstat, men med anerkendelse fra, den medlemsstat.

3. Kildekoden for applikationens softwarekomponenter i de europæiske digitale identitetstegnebøger skal være open source-licensieret. Medlemsstaterne kan fastsætte, at kildekoden for andre specifikke komponenter end dem, der er installeret på brugerenheder, af behørigt begrundede årsager ikke skal oplyses.

4. Europæiske digitale identitetstegnebøger skal gøre det muligt for brugeren på en måde, der er brugervenlig, gennemsigtig og sporbar for brugeren:

a) på sikker vis og under brugerens enekontrol at anmode om, indhente, udvælge, kombinere, lagre, slette, dele og fremlægge personidentifikationsdata og, hvis det er relevant, i kombination med elektroniske attesteringer af attributter, til autentifikation over for modtagerparter online og, hvis det er relevant, offline med henblik på at få adgang til offentlige og private tjenester, samtidig med at det sikres, at selektiv videregivelse af data er mulig

b) at generere pseudonymer og lagre dem krypteret og lokalt i den europæiske identitetstegnebog

c) på sikker vis at autentificere en anden persons europæiske digitale identitetstegnebog og modtage og dele personidentifikationsdata og elektroniske attesteringer af attributter på en sikret måde mellem de to europæiske digitale identitetstegnebøger

d) at få adgang til en log over alle transaktioner, der gennemføres via den europæiske digitale identitetstegnebog, via et fælles dashboard, der gør det muligt for brugeren:

   i) at se en ajourført liste over modtagerparter, som brugeren har etableret en forbindelse med, og, hvis det er relevant, alle udvekslede data

   ii) let at anmode en modtagerpart om at slette personoplysninger i henhold til artikel 17 i forordning (EU) 2016/679

   iii) let at indberette en modtagerpart til den kompetente nationale databeskyttelsesmyndighed, hvis der modtages en angiveligt ulovlig eller mistænkelig anmodning om data

e) at underskrive ved hjælp af kvalificerede elektroniske signaturer eller forsegle ved hjælp af kvalificerede elektroniske segl

f) i det omfang det er teknisk muligt, at downloade brugerens data, elektroniske attestering af attributter og konfigurationer

g) at udøve brugerens ret til dataportabilitet.

5. Europæiske digitale identitetstegnebøger skal navnlig:

a) understøtte fælles protokoller og grænseflader:

   i) til udstedelse af personidentifikationsdata, kvalificerede og ikkekvalificerede elektroniske attesteringer af attributter eller kvalificerede og ikkekvalificerede certifikater til europæiske digitale identitetstegnebøger

   ii) således at modtagerparter kan anmode om og validere personidentifikationsdata og elektroniske attesteringer af attributter

   iii) til deling og forelæggelse for modtagerparter af personidentifikationsdata, af elektronisk attestering af attributter eller af selektivt videregivne relaterede data online og, hvis det er relevant, offline

iv) således at brugeren kan interagere med den europæiske digitale identitetstegnebog og fremvise et EU-tillidsmærke for europæiske digitale identitetstegnebøger

v) til på sikker vis at onboarde brugeren ved hjælp af et elektronisk identifikationsmiddel i overensstemmelse med artikel 5a, stk. 24

vi) til interaktion mellem to personers europæiske digitale identitetstegnebøger med henblik på at modtage, validere og dele personidentifikationsdata og elektroniske attesteringer af attributter på en sikker måde

vii) til autentifikation og identificering af modtagerparter ved at gennemføre autentifikationsmekanismer i overensstemmelse med artikel 5b

viii) til modtagerparters validering af autenticiteten og gyldigheden af europæiske digitale identitetstegnebøger

ix) til at anmode en modtagerpart om at slette personoplysninger i medfør af artikel 17 i forordning (EU) 2016/679

x) til indberetning af en modtagerpart til den kompetente nationale databeskyttelsesmyndighed, hvis der modtages en angiveligt ulovlig eller mistænkelig anmodning om data

xi) til oprettelse af kvalificerede elektroniske signaturer eller elektroniske segl ved hjælp af kvalificerede elektroniske signatur- eller elektroniske seglgenereringssystemer

b) ikke give tillidstjenesteudbydere af elektroniske attesteringer af attributter oplysninger om anvendelsen af disse elektroniske attesteringer

c) sikre, at modtagerparters identitet kan autentificeres og identificeres ved at indføre autentifikationsmekanismer i overensstemmelse med artikel 5b

d) opfylde de krav, der er fastsat i artikel 8, med hensyn til sikringsniveauet »høj«, navnlig hvad angår kravene til godtgørelse og kontrol af identitet og forvaltning og autentifikation af elektroniske identifikationsmidler

e) i tilfælde af elektronisk attestering af attributter med indbyggede videregivelsespolitikker, gennemføre en passende mekanisme til at underrette brugeren om, at modtagerparten eller brugeren af den europæiske digitale identitetstegnebog, der anmoder om denne elektronisk attestering af attributter, har tilladelse til at få adgang til en sådan attestering

f) sikre, at de personidentifikationsdata, der er tilgængelige fra den elektroniske identifikationsordning, i henhold til hvilken den europæiske digitale identitetstegnebog leveres, entydigt repræsenterer den fysiske person, den juridiske person eller den fysiske person, der repræsenterer den fysiske eller juridiske person, og er knyttet til den pågældende europæiske digitale identitetstegnebog

g) give alle fysiske personer mulighed for at underskrive ved hjælp af kvalificerede elektroniske signaturer som standard og gratis.

Uanset første afsnit, litra g), kan medlemsstaterne træffe forholdsmæssige foranstaltninger for at sikre, at fysiske personers gratis anvendelse af kvalificerede elektroniske signaturer begrænses til ikkeerhvervsmæssige formål.

6. Medlemsstaterne skal straks informere brugere om ethverts sikkerhedsbrud, der helt eller delvis vil kunne have kompromitteret deres europæiske digitale identitetstegnebog eller dens indhold, navnlig hvis det har resulteret i suspension eller ophævelse af deres europæiske digitale identitetstegnebogs gyldighed i medfør af artikel 5e.

7. Uden at det berører artikel 5f, kan medlemsstaterne i overensstemmelse med national ret indføre yderligere funktionaliteter i de europæiske digitale identitetstegnebøger, herunder interoperabilitet med eksisterende nationale elektroniske identifikationsmidler. Disse yderligere funktionaliteter skal overholde nærværende artikel.

8. Medlemsstaterne stiller valideringsmekanismer gratis til rådighed for at:

a) sikre, at de europæiske digitale identitetstegnebøgers autenticitet og gyldighed kan kontrolleres

b) gøre det muligt for brugere at kontrollere autenticiteten og gyldigheden af identiteten af modtagerparter, der er registreret i overensstemmelse med artikel 5b.

9. Medlemsstaterne sikrer, at gyldigheden af den europæiske digitale identitetstegnebog kan tilbagekaldes under følgende omstændigheder:

a) på brugerens udtrykkelige anmodning

b) hvis den europæiske digitale identitetstegnebogs sikkerhed er kompromitteret

c) ved brugerens død eller ved ophør af en juridisk persons aktivitet.

10. Udbydere af europæiske digitale identitetstegnebøger sikrer, at brugerne nemt kan anmode om teknisk støtte og indberette tekniske problemer eller andre hændelser, der har en negativ indvirkning på brugen af den europæiske digitale identitetstegnebog.

11. Europæiske digitale identitetstegnebøger leveres i henhold til en elektronisk identifikationsordning med sikringsniveauet »høj«.

12. Europæiske digitale identitetstegnebøger skal have sikkerhed gennem design.

13. Udstedelse, anvendelse og tilbagekaldelse af europæiske digitale identitetstegnebøger skal være gratis for alle fysiske personer.

14. Brugere har fuld kontrol over anvendelsen af og dataene i deres europæiske digitale identitetstegnebog. Udbyderen af den europæiske digitale identitetstegnebog indsamler hverken oplysninger om anvendelsen af den europæiske digitale identitetstegnebog, som ikke er nødvendige for leveringen af europæiske digitale identitetstegnebogstjenester, eller kombinerer personidentifikationsdata eller andre personoplysninger, der er lagret, eller som vedrører anvendelsen af den europæiske digitale identitetstegnebog, med personoplysninger fra andre tjenester, som udbydes af denne udbyder, eller fra tredjepartstjenester, som ikke er nødvendige for leveringen af europæiske digitale identitetstegnebogstjenester, medmindre brugeren udtrykkeligt har anmodet om noget andet. Personoplysninger vedrørende levering af den europæiske digitale identitetstegnebog opbevares logisk adskilt fra alle andre data, der opbevares af udbyderen af den europæiske digitale identitetstegnebog. Hvis den europæiske digitale identitetstegnebog er leveret af en privat part i overensstemmelse med denne artikels stk. 2, litra b) og c), finder bestemmelserne i artikel 45h, stk. 3, tilsvarende anvendelse.

15. Brugen af europæiske digitale identitetstegnebøger er frivillig. Adgangen til offentlige og private tjenester, adgang til arbejdsmarkedet og friheden til at oprette og drive forretning må ikke på nogen måde begrænses eller gøres ufordelagtig for fysiske eller juridiske personer, der ikke anvender europæiske digitale identitetstegnebøger. Det skal fortsat være muligt at få adgang til offentlige og private tjenester ved hjælp af andre eksisterende identifikations- og autentifikationsmidler.

16. Den tekniske ramme for den europæiske digitale identitetstegnebog:

a) må ikke give udbydere af elektroniske attesteringer af attributter eller enhver anden part efter udstedelsen af attesteringen af attributter mulighed for at indhente data, der gør det muligt for transaktioner eller brugeradfærd at blive sporet, forbundet, korrelere eller på anden måde opnå viden om transaktioner eller brugeradfærd, medmindre brugeren udtrykkeligt har givet tilladelse hertil

b) skal muliggøre teknikker til beskyttelse af privatlivets fred, som sikrer uforbindelighed, hvor attesteringen af attributter ikke kræver identifikation af brugeren.

17. Enhver behandling af personoplysninger, der foretages af medlemsstaterne eller på deres vegne af organer eller parter, der er ansvarlige for levering af europæiske digitale identitetstegnebøger som elektroniske identifikationsmidler, foretages i overensstemmelse med passende og effektive databeskyttelsesforanstaltninger. Sådanne behandlingsaktiviteters overholdelse af forordning (EU) 2016/679 skal påvises. Medlemsstaterne kan indføre nationale bestemmelser for yderligere at præcisere anvendelsen af sådanne foranstaltninger.

18. Medlemsstaterne meddeler uden unødigt ophold Kommissionen oplysninger om:

a) det organ, der er ansvarligt for at oprette og ajourføre listen over registrerede modtagerparter, der benytter de europæiske digitale identitetstegnebøger i overensstemmelse med artikel 5b, stk. 5, og hvor denne liste befinder sig

b) de organer, der er ansvarlige for leveringen af europæiske digitale identitetstegnebøger i overensstemmelse med artikel 5a, stk. 1

c) de organer, der er ansvarlige for at sikre, at personidentifikationsdataene har tilknytning til den europæiske digitale identitetstegnebog i overensstemmelse med artikel 5a, stk. 5, litra f)

d) den mekanisme, der gør det muligt at validere de personidentifikationsdata, der er omhandlet i artikel 5a, stk. 5, litra f), og modtagerparternes identitet

e) mekanismen til validering af autenticiteten og gyldigheden af europæiske digitale identitetstegnebøger.

Kommissionen stiller de oplysninger, der er meddelt i medfør af første afsnit, til rådighed for offentligheden via en sikker kommunikationsforbindelse og i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

19. Uden at det berører denne artikels stk. 22, finder artikel 11 tilsvarende anvendelse på europæiske digitale identitetstegnebøger.

20. Artikel 24, stk. 2, litra b) og d)-h), finder tilsvarende anvendelse på leverandører af europæiske digitale identitetstegnebøger.

21. De europæiske digitale identitetstegnebøger gøres tilgængelige til brug for personer med handicap på lige fod med andre brugere i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2019/882 (*).

22. Med henblik på levering af europæiske digitale identitetstegnebøger er europæiske digitale identitetstegnebøger og de elektroniske identifikationsordninger, efter hvilke de leveres, ikke omfattet af kravene i artikel 7, 9, 10, 12 og 12a.

23. Senest den 21. november 2024 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for de i denne artikels stk. 4, 5, 8 og 18 omhandlede krav for gennemførelsen af den europæiske digitale identitetstegnebog. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

24. Kommissionen fastsætter ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer med henblik på at lette brugernes onboarding af den europæiske digitale identitetstegnebog ved hjælp af enten elektroniske identifikationsmidler, der opfylder sikringsniveauet »høj«, eller elektroniske identifikationsmidler, der opfylder sikringsniveauet »betydelig«, sammenholdt med yderligere onboardingprocedurer på afstand, som tilsammen opfylder kravene til sikringsniveauet »høj«. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 5b

Modtagerparter i forbindelse med europæiske digitale identitetstegnebøger

1. Hvis en modtagerpart har til hensigt at benytte europæiske digitale identitetstegnebøger til levering af offentlige eller private tjenester ved hjælp af digital interaktion, registrerer modtagerparten sig i den medlemsstat, hvor den er hjemmehørende.

2. Registreringsprocessen skal være omkostningseffektiv og stå i et rimeligt forhold til risikoen. Modtagerparten skal som minimum meddele:

a) de oplysninger, der er nødvendige for autentifikation til europæiske digitale identitetstegnebøger, hvilket som minimum omfatter:

   i) den medlemsstat, hvor modtagerparten er hjemmehørende, og

ii) modtagerpartens navn og, hvis det er relevant, registreringsnummer, som det fremgår af et officielt register, sammen med dette officielle registers identifikationsdata

b) modtagerpartens kontaktoplysninger

c) den tilsigtede anvendelse af europæiske digitale identitetstegnebøger, herunder en angivelse af de data, som modtagerparten skal anmode brugere om.

3. Modtagerparter må ikke anmode brugere om at levere andre data end dem, der er angivet i beskrivelsen givet i medfør af stk. 2, litra c).

4. Stk. 1 og 2 berører ikke EU-retten eller national ret, der finder anvendelse på leveringen af specifikke tjenester.

5. Medlemsstaterne gør de oplysninger, der er omhandlet i stk. 2, offentligt tilgængelige online i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

6. Modtagerparter, der er registreret i overensstemmelse med denne artikel, underretter straks medlemsstaterne om ændringer af de oplysninger, der er meddelt ved registreringen i medfør af stk. 2.

7. Medlemsstaterne indfører en fælles mekanisme til identifikation og autentifikation af modtagerparter som omhandlet i artikel 5a, stk. 5, litra c).

8. Hvis modtagerparter har til hensigt at benytte europæiske digitale identitetstegnebøger, skal de identificere sig over for brugeren.

9. Modtagerparterne er ansvarlige for at gennemføre proceduren for autentifikation og validering af personidentifikationsdata og elektronisk attestering af attributter, som der er anmodet om fra europæiske digitale identitetstegnebøger. Modtagerparterne må ikke nægte anvendelsen af pseudonymer, hvis identifikation af brugeren ikke er påkrævet i henhold til EU-retten eller national ret.

10. Formidlere, der handler på vegne af modtagerparter, betragtes som modtagerparter og må ikke lagre data om transaktionens indhold.

11. Senest den 21. november 2024 fastsætter Kommissionen tekniske specifikationer og procedurer for de i denne artikels stk. 2, 5 og 6-9 omhandlede krav ved hjælp af gennemførelsesretsakter om gennemførelsen af europæiske digitale identitetstegnebøger som omhandlet i artikel 5a, stk. 23. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 5c

Certificering af europæiske digitale identitetstegnebøger

1. Overensstemmelsen af europæiske digitale identitetstegnebøger og den elektroniske identifikationsordning, i henhold til hvilken de leveres, med kravene i artikel 5a, stk. 4, 5 og 8, med kravet om logisk adskillelse i artikel 5a, stk. 14, og, hvor det er relevant, med de standarder og tekniske specifikationer, der er omhandlet i artikel 5a, stk. 24, certificeres af overensstemmelsesvurderingsorganer, der er udpeget af medlemsstaterne.

2. Certificering af europæiske digitale identitetstegnebøgers overensstemmelse med de i denne artikels stk. 1, omhandlede krav, eller dele deraf, som er relevante for cybersikkerhed, foretages i overensstemmelse med europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i medfør af Europa-Parlamentets og Rådets forordning (EU) 2019/881 (**), og som der henvises til i de gennemførelsesretsakter, der er omhandlet i denne artikels stk. 6.

3. For krav, der er omhandlet i denne artikels stk. 1, der ikke er relevante for cybersikkerhed, og for krav, der er omhandlet i denne artikels stk. 1, der er relevante for cybersikkerhed, i det omfang cybersikkerhedscertificeringsordninger som omhandlet i denne artikels stk. 2 ikke eller kun delvist dækker disse cybersikkerhedskrav, også for disse krav opretter medlemsstaterne nationale certificeringsordninger i overensstemmelse med de krav, der er fastsat i de gennemførelsesretsakter, der er omhandlet i denne artikels stk. 6. Medlemsstaterne fremsender deres udkast til nationale certificeringsordninger til den europæiske samarbejdsgruppe for digital identitet, der nedsættes i henhold til artikel 46e, stk. 1 (»samarbejdsgruppen«). Samarbejdsgruppen kan afgive udtalelser og udstede henstillinger.

4. Certificering i medfør af stk. 1 er gyldig i op til fem år, forudsat at der foretages en sårbarhedsvurdering hvert andet år. Hvis der konstateres en sårbarhed, og den ikke afhjælpes på en rettidig måde, annulleres certificeringen.

5. Overholdelse af kravene fastsat i denne forordnings artikel 5a for så vidt angår aktiviteter vedrørende behandling af personoplysninger kan certificeres i medfør af forordning (EU) 2016/679.

6. Senest den 21. november 2024 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for den i denne artikels stk. 1, 2 og 3 omhandlede certificering af den europæiske digitale identitetstegnebog. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

7. Medlemsstaterne meddeler Kommissionen navn og adresse på de i stk. 1 omhandlede overensstemmelsesvurderingsorganer. Kommissionen stiller disse oplysninger til rådighed for alle medlemsstaterne.

8. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 47, der fastsætter de særlige kriterier, som de i denne artikels stk. 1 omhandlede overensstemmelsesvurderingsorganer skal opfylde.

Artikel 5d

Offentliggørelse af en liste over certificerede europæiske digitale identitetstegnebøger

1. Medlemsstaterne underretter uden unødigt ophold Kommissionen og samarbejdsgruppen nedsat i medfør af artikel 46e, stk. 1, om de europæiske digitale identitetstegnebøger, der er leveret i henhold til artikel 5a og certificeret af de overensstemmelsesvurderingsorganer, der er omhandlet i artikel 5c, stk. 1. De underretter uden unødigt ophold Kommissionen og samarbejdsgruppen nedsat i medfør af artikel 46e, stk. 1, hvis certificering annulleres, og angiver årsagerne til annulleringen.

2. Uden at det berører artikel 5a, stk. 18, skal de i nærværende artikels stk. 1 omhandlede oplysninger fra medlemsstaterne mindst omfatte:

a) certifikatet og certificeringsvurderingsrapporten for den certificerede europæiske digitale identitetstegnebog

b) en beskrivelse af den elektroniske identifikationsordning, i henhold til hvilken den europæiske digitale identitetstegnebog leveres

c) den gældende tilsynsordning og oplysninger om erstatningsansvarsordningen med hensyn til den part, der leverer den europæiske digitale identitetstegnebog

d) oplysning om, hvilken eller hvilke myndigheder der er ansvarlige for den elektroniske identifikationsordning

e) ordninger for suspension eller spærring af den elektroniske identifikationsordning eller autentifikationen eller af de kompromitterede dele heraf.

3. Kommissionen opstiller, offentliggør i *Den Europæiske Unions Tidende* og opretholder i maskinlæsbar form på grundlag af de oplysninger, den modtager i medfør af stk. 1, en liste over certificerede europæiske digitale identitetstegnebøger.

4. En medlemsstat kan anmode Kommissionen om at fjerne en europæisk digital identitetstegnebog og den elektroniske identifikationsordning, i henhold til hvilken den leveres, fra den i stk. 3 omhandlede liste.

5. Hvis der sker ændringer i de oplysninger, der er indgivet i medfør af stk. 1, giver medlemsstaten Kommissionen ajourførte oplysninger.

6. Kommissionen ajourfører den i stk. 3 omhandlede liste ved at offentliggøre de tilsvarende ændringer af listen i *Den Europæiske Unions Tidende* senest én måned efter modtagelsen af en anmodning i medfør af stk. 4 eller af ajourførte oplysninger i medfør af stk. 5.

7. Senest den 21. november 2024 fastsætter Kommissionen de formater og procedurer, der finder anvendelse med henblik på denne artikels stk. 1, 4 og 5 ved hjælp af gennemførelsesretsakter om gennemførelsen af europæiske digitale identitetstegnebøger som omhandlet i artikel 5a, stk. 23. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 5e

Sikkerhedsbrud i europæiske digitale identitetstegnebøger

1. Hvis europæiske digitale identitetstegnebøger, der er leveret i medfør af artikel 5a, de valideringsmekanismer, der er omhandlet i artikel 5a, stk. 8, eller den elektroniske identifikationsordning, i henhold til hvilken de europæiske digitale identitetstegnebøger leveres, er udsat for sikkerhedsbrud eller er delvist kompromitteret på en måde, som har indvirkning på deres pålidelighed eller andre europæiske digitale identitetstegnebøgers pålidelighed, suspenderer den medlemsstat, der leverede de europæiske digitale identitetstegnebøger uden unødigt ophold leveringen og anvendelsen af europæiske digitale identitetstegnebøger.

Hvis det er begrundet i alvoren af sikkerhedsbruddet eller kompromitteringen omhandlet i første afsnit, trækker medlemsstaten europæiske digitale identitetstegnebøger tilbage uden unødigt ophold.

Medlemsstaten underretter de berørte brugere, de centrale kontaktpunkter, der er udpeget i henhold til artikel 46c, stk. 1, modtagerparterne og Kommissionen herom.

2. Hvis sikkerhedsbruddet eller kompromitteringen omhandlet i. denne artikels stk. 1, første afsnit, ikke er afhjulpet senest tre måneder efter suspensionen, trækker den medlemsstat, der leverede de europæiske digitale identitetstegnebøger, europæiske digitale identitetstegnebøger tilbage og tilbagekalder deres gyldighed. Medlemsstaten underretter de berørte brugere, de centrale kontaktpunkter, der er udpeget i medfør af artikel 46c, stk. 1, modtagerparterne og Kommissionen om tilbagetrækningen.

3. Hvor sikkerhedsbruddet eller kompromitteringen omhandlet i denne artikels stk. 1, først afsnit, er afhjulpet, genoptager den leverende medlemsstat leveringen og anvendelsen af europæiske digitale identitetstegnebog og underretter uden unødigt ophold de berørte brugere og modtagerparter, de centrale kontaktpunkter, der er udpeget i medfør af artikel 46c, stk. 1, og Kommissionen herom.

4. Kommissionen offentliggør uden unødigt ophold de tilsvarende ændringer af den i artikel 5d omhandlede liste i *Den Europæiske Unions Tidende*.

5. Senest den 21. november 2024 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarderne og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for de i denne artikels stk. 1, 2 og 3 omhandlede foranstaltninger. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 5f

Grænseoverskridende benyttelse af europæiske digitale identitetstegnebøger

1. Hvis medlemsstaterne kræver elektronisk identifikation og autentifikation for adgang til en onlinetjeneste, der udbydes af en offentlig myndighed, skal de også acceptere europæiske digitale identitetstegnebøger, der er leveret i overensstemmelse med denne forordning.

2. Hvis private modtagerparter, der udbyder tjenester, med undtagelse af mikrovirksomheder og små virksomheder som defineret i artikel 2 i bilaget til Kommissionens henstilling 2003/361/EF (***), i henhold til EU-retten eller national ret er forpligtede til at anvende stærk brugerautentifikation til onlineidentifikation, eller hvis stærk brugerautentifikation til onlineidentifikation er krævet i henhold til kontraktlige forpligtelser, herunder inden for transport, energi, banktjenester, finansielle tjenesteydelser, social sikring, sundhed, drikkevand, posttjenester, digital infrastruktur, uddannelse eller telekommunikation, skal disse private modtagerparter senest 36 måneder fra datoen for de i artikel 5a, stk. 23, og artikel 5c, stk. 6, omhandlede gennemførelsesretsakters ikrafttræden, og udelukkende efter brugerens frivillige anmodning acceptere europæiske digitale identitetstegnebøger, der er leveret i overensstemmelse med denne forordning.

3. Hvis udbydere af meget store onlineplatforme som omhandlet i artikel 33 i Europa-Parlamentets og Rådets forordning (EU) 2022/2065 (****) kræver autentifikation af brugere for adgang til onlinetjenester, skal de også acceptere og lette anvendelsen af europæiske digitale identitetstegnebøger, der er leveret i overensstemmelse med denne forordning, med henblik på brugerautentifikation, udelukkende efter brugerens frivillige anmodning og under hensyntagen til de minimumsdata, der er nødvendige for den specifikke onlinetjeneste, for hvilken der anmodes om autentifikation.

4. I samarbejde med medlemsstaterne fremmer Kommissionen udviklingen af adfærdskodekser i tæt samarbejde med alle relevante interessenter, herunder civilsamfundet, med henblik på at bidrage til bred tilgængelighed og anvendelighed af europæiske digitale identitetstegnebøger inden for denne forordnings anvendelsesområde og på at tilskynde tjenesteudbydere til at færdiggøre udviklingen af adfærdskodekser.

5. Senest 24 måneder efter indførelsen af europæiske digitale identitetstegnebøger vurderer Kommissionen efterspørgslen efter og tilgængeligheden og anvendeligheden af europæiske digitale identitetstegnebøger under hensyntagen til kriterier såsom udbredelse blandt brugerne, tjenesteudbydernes tilstedeværelse på tværs af grænserne, den teknologiske udvikling, udviklingen i forbrugsmønstre og forbrugerefterspørgslen.

(*) Europa-Parlamentets og Rådets direktiv (EU) 2019/882 af 17. april 2019 om tilgængelighedskrav for produkter og tjenester (EUT L 151 af 7.6.2019, s. 70).

(**) 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).

(***) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

(****) Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EUT L 277 af 27.10.2022, s. 1).«

6) Som overskrift indsættes før artikel 6:

»AFDELING 2

ELEKTRONISKE IDENTIFIKATIONSORDNINGER«.

7) Artikel 7, litra g), affattes således:

»g) senest seks måneder forud for anmeldelse i henhold til artikel 9, stk. 1, fremlægger den anmeldende medlemsstat med henblik på artikel 12, stk. 5, en beskrivelse af ordningen for de andre medlemsstater i overensstemmelse med de proceduremæssige ordninger, der er fastsat ved de gennemførelsesretsakter, der er vedtaget i medfør af i artikel 12, stk. 6«.

8) Artikel 8, stk. 3, første afsnit, affattes således:

»3. Senest den 18. september 2015 fastsætter Kommissionen, idet der tages hensyn til relevante internationale standarder og med forbehold af stk. 2, ved hjælp af gennemførelsesretsakter de tekniske minimumsspecifikationer, minimumsstandarder, og procedurer, der henvises til i forbindelse med fastsættelse af sikringsniveauerne »lav«, »betydelig« og »høj« for de elektroniske identifikationsmidler.«

9) Artikel 9, stk. 2 og 3, affattes således:

»2. Kommissionen offentliggør i *Den Europæiske Unions Tidende* uden unødigt ophold en liste over de elektroniske identifikationsordninger, der er anmeldt i henhold til stk. 1, sammen med grundlæggende oplysninger om disse ordninger.

3. Kommissionen offentliggør i *Den Europæiske Unions Tidende* de ændringer til den liste, der er omhandlet i stk. 2, senest én måned efter datoen for modtagelse af anmeldelsen.«

10) I artikel 10 affattes overskriften således:

»Sikkerhedsbrud i elektroniske identifikationsordninger«.

11) Følgende artikel indsættes:

»*Artikel 11a*

Grænseoverskridende identitetssammenkobling

1. Når medlemsstaterne fungerer som modtagerparter for grænseoverskridende tjenester, sikrer de en entydig identitetssammenkobling for fysiske personer ved hjælp af anmeldte elektroniske identifikationsmidler eller europæiske digitale identitetstegnebøger.

2. Medlemsstaterne indfører tekniske og organisatoriske foranstaltninger for at sikre et højt beskyttelsesniveau for personoplysninger, der anvendes til identitetssammenkobling, og for at forhindre profilering af brugere.

3. Senest den 21. november 2024, fastsætter Kommissionen en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for de i denne artikels stk. 1 omhandlede krav ved hjælp af gennemførelsesretsakter. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

12) I artikel 12 foretages følgende ændringer:

a) Overskriften affattes således:

»Interoperabilitet«.

b) I stk. 3 foretages følgende ændringer:

i) Litra c) affattes således:

»c) den letter gennemførelsen af privatlivsbeskyttelse og sikkerhed gennem design«.

ii) Litra d) udgår.

c) Stk. 4, litra d), affattes således:

»d) en henvisning til et minimum af personidentifikationsdata, der er nødvendige for entydigt at repræsentere en fysisk eller juridisk person eller en fysisk person, der repræsenterer en anden fysisk person eller en juridisk person, og som stilles til rådighed fra elektroniske identifikationsordninger«

d) Stk. 5 og 6 affattes således:

»5. Medlemsstaterne foretager peerevalueringer af de elektroniske identifikationsordninger, der er omfattet af denne forordnings anvendelsesområde, og som skal anmeldes i henhold til artikel 9, stk. 1, litra a).

6. Senest den 18. marts 2025 fastlægger Kommissionen ved hjælp af gennemførelsesretsakter de fornødne proceduremæssige ordninger for de peerevalueringer, der er omhandlet i denne artikels stk. 5, med henblik på at fremme et højt niveau af tillid og sikkerhed, der står i et passende forhold til risikoen. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

e) Stk. 7 udgår.

f) Stk. 8 affattes således:

»8. Senest den 18. september 2025 vedtager Kommissionen med forbehold af kriterierne i denne artikels stk. 3 og under hensyn til resultaterne af samarbejdet mellem medlemsstaterne gennemførelsesretsakter om interoperabilitetsrammen som fastsat i denne artikels stk. 4 med henblik på at fastsætte ensartede betingelser for gennemførelsen af kravet i denne artikels stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelses-proceduren, jf. artikel 48, stk. 2.«

13) I kapitel II indsættes følgende artikler:

»*Artikel 12a*

Certificering af elektroniske identifikationsordninger

1. Overensstemmelsen af elektroniske identifikationsordninger, der skal anmeldes, med de cybersikkerhedskrav, der er fastsat i denne forordning, herunder overensstemmelsen med de cybersikkerhedsrelevante krav, der er fastsat i artikel 8, stk. 2, vedrørende sikringsniveauerne for elektroniske identifikationsordninger, certificeres af overensstemmelsesvurderingsorganer, der er udpeget af medlemsstaterne.

2. Certificering i medfør af denne artikels stk. 1 udføres i overensstemmelse med en relevant cybersikkerheds-certificeringsordning i henhold til forordning (EU) 2019/881 eller dele heraf, for så vidt cybersikkerhedsattesten eller dele heraf omfatter disse cybersikkerhedskrav.

3. Certificering i medfør af stk. 1 er gyldig i op til fem år, forudsat at der foretages en sårbarhedsvurdering hvert andet år. Hvis der konstateres en sårbarhed, og den ikke afhjælpes inden for tre måneder efter en sådan konstatering, annulleres certificeringen.

4. Uanset stk. 2 kan medlemsstater i overensstemmelse med nævnte stykke anmode en anmeldende medlemsstat om yderligere oplysninger om elektroniske identifikationsordninger eller dele heraf, der er certificeret.

5. Peerevalueringen af elektroniske identifikationsordninger, der er omhandlet i artikel 12, stk. 5, finder ikke anvendelse på elektroniske identifikationsordninger eller dele af sådanne ordninger, der er certificeret i overensstemmelse med denne artikels stk. 1. Medlemsstaterne kan benytte et certifikat eller en erklæring om overensstemmelse med de ikkecybersikkerhedsrelaterede krav i artikel 8, stk. 2, der er udstedt i overensstemmelse med en relevant certificeringsordning eller dele af sådanne ordninger, for så vidt angår elektroniske identifikationsordningers sikringsniveau.

6. Medlemsstaterne meddeler Kommissionen navn og adresse på de i stk. 1 omhandlede overensstemmelses-vurderingsorganer. Kommissionen stiller disse oplysninger til rådighed for alle medlemsstaterne.

Artikel 12b

Adgang til hardware og softwarefunktioner

Hvis leverandører af europæiske digitale identitetstegnebøger og udstedere af anmeldte elektroniske identifikationsmidler, der handler i kommerciel eller professionel egenskab og anvender centrale platformstjenester som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets forordning (EU) 2022/1925 (*) med henblik på eller i forbindelse med levering af europæiske digitale identitetstegnebogstjenester og elektroniske identifikationsmidler til slutbrugere, er erhvervsbrugere som defineret i nævnte forordnings artikel 2, nr. 21), giver gatekeeperne navnlig dem effektiv interoperabilitet med og, med henblik på interoperabilitet, adgang til det samme styresystem eller de samme hardware- eller softwarefunktioner. Sådan effektiv interoperabilitet og adgang skal gives gratis, og uanset om hardware- eller softwarefunktionerne er en del af styresystemet, er tilgængelige for eller anvendes af den pågældende gatekeeper, når denne udbyder sådanne tjenester i den i artikel 6, stk. 7, i forordning (EU) 2022/1925 anvendte betydning. Nærværende artikel berører ikke nærværende forordnings artikel 5a, stk. 14.

(*) Europa-Parlamentets og Rådets forordning (EU) 2022/1925 af 14. september 2022 om åbne og fair markeder i den digitale sektor og om ændring af direktiv (EU) 2019/1937 og (EU) 2020/1828 (forordningen om digitale markeder) (EUT L 265 af 12.10.2022, s. 1).«

14) Artikel 13, stk. 1, affattes således:

»1. Uanset denne artikels stk. 2 og med forbehold af forordning (EU) 2016/679 er tillidstjenesteudbydere ansvarlige for skader, der forsætligt eller uagtsomt forvoldes en fysisk eller juridisk person som følge af manglende opfyldelse af forpligtelser i henhold til denne forordning. Enhver fysisk eller juridisk person, der har lidt materiel eller immateriel skade som følge af en tillidstjenesteudbyders overtrædelse af nærværende forordning, har ret til at kræve erstatning i overensstemmelse med EU-retten og national ret.

Den fysiske eller juridiske person, der hævder at have lidt skade som omhandlet i første afsnit, bærer bevisbyrden for, at en ikkekvalificeret tillidstjenesteudbyder har handlet forsætligt eller uagtsomt.

En kvalificeret tillidstjenesteudbyder formodes at have handlet forsætligt eller uagtsomt, medmindre den pågældende kvalificerede tillidstjenesteudbyder beviser, at den i første afsnit omhandlede skade indtraf uden den pågældende kvalificerede tillidstjenesteudbyders forsæt eller uagtsomhed.«

15) Artikel 14, 15 og 16 affattes således:

»*Artikel 14*

Internationale aspekter

1. Tillidstjenester, der udbydes af tillidstjenesteudbydere, som er hjemmehørende i et tredjeland, eller af en international organisation, anerkendes som retligt ligestillede med kvalificerede tillidstjenester, der udbydes af kvalificerede tillidstjenesteudbydere, der er hjemmehørende i Unionen, hvis tredjelandstillidstjenesterne eller den internationale organisation er anerkendt ved hjælp af gennemførelsesretsakter eller en aftale, som er indgået mellem Unionen og tredjelandet eller den internationale organisation i medfør af artikel 218 i TEUF.

De gennemførelsesretsakter, der er omhandlet i første afsnit, vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

2. De i stk. 1 omhandlede gennemførelsesretsakter og aftaler skal sikre, at tillidstjenesteudbyderne i det pågældende tredjeland eller de internationale organisationer og de tillidstjenester, som de udbyder, opfylder de krav, der gælder for kvalificerede tillidstjenesteudbydere, som er hjemmehørende i Unionen, og de kvalificerede tillidstjenester, som de udbyder. Tredjelande og internationale organisationer skal navnlig oprette, ajourføre og offentliggøre en positivliste over anerkendte tillidstjenesteudbydere.

3. De i stk. 1 omhandlede aftaler skal sikre, at de kvalificerede tillidstjenester, der udbydes af kvalificerede tillidstjenesteudbydere, som er hjemmehørende i Unionen, anerkendes som retligt ligestillede med tillidstjenester, der udbydes af tillidstjenesteudbydere i det tredjeland eller den internationale organisation, som aftalen indgås med.

Artikel 15

Tilgængelighed for personer med handicap og særlige behov

Leveringen af elektroniske identifikationsmidler, tillidstjenester og slutbrugerprodukter, der anvendes til levering af disse tjenester, skal gøres tilgængelige på et klart og forståeligt sprog i overensstemmelse med De Forenede Nationers konvention om rettigheder for personer med handicap og med tilgængelighedskravene i direktiv (EU) 2019/882, således at også personer, der oplever funktionelle begrænsninger, såsom ældre, og personer med begrænset adgang til digitale teknologier, får gavn heraf.

Artikel 16

Sanktioner

1. Uden at det berører artikel 31 i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 (*) fastsætter medlemsstaterne regler om sanktioner for overtrædelse af denne forordning. Disse sanktioner skal være effektive, forholdsmæssige og have afskrækkende virkning.

2. Medlemsstaterne sikrer, at kvalificerede og ikkekvalificerede tillidstjenesteudbyderes overtrædelser af denne forordning straffes med administrative bøder på mindst:

a) 5 000 000 EUR, hvis tillidstjenesteudbyderen er en fysisk person, eller

b) hvis tillidstjenesteyderen er en juridisk person, 5 000 000 EUR eller 1 % af den samlede globale årsomsætning i den virksomhed, som tillidstjenesteudbyderen tilhørte, i det regnskabsår, der går forud for det år, hvor overtrædelsen fandt sted, alt efter hvilket beløb der er højest.

3. Afhængigt af medlemsstaternes retssystem kan reglerne om administrative bøder anvendes på en sådan måde, at det kompetente tilsynsorgan tager skridt til bøden, og de kompetente nationale domstole pålægger bøden. Anvendelsen af sådanne regler i de pågældende medlemsstater skal sikre, at nævnte retsmidler er effektive, og at deres virkning svarer til virkningen af de administrative bøder, som pålægges direkte af tilsynsmyndigheder.

(*) 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).«

16) I kapitel III, afdeling 2, affattes overskriften således:

»Ikkekvalificerede tillidstjenester«.

17) Artikel 17 og 18 udgår.

18) I kapitel III, afdeling 2, indsættes følgende artikel:

»*Artikel 19a*

Krav til ikkekvalificerede tillidstjenesteudbydere

1. En ikkekvalificeret tillidstjenesteudbyder, der udbyder ikkekvalificerede tillidstjenester, skal:

a) indføre passende politikker og træffe tilsvarende foranstaltninger til at styre juridiske, erhvervsmæssige, operationelle og andre direkte eller indirekte risici i forbindelse med leveringen af den ikkekvalificerede tillidstjeneste, der uanset artikel 21 i direktiv (EU) 2022/2555 skal omfatte som minimum foranstaltninger vedrørende:

i) registrerings- og onboardingprocedurer for en tillidstjeneste

ii) den proceduremæssige eller administrative kontrol, der er nødvendig for at udbyde tillidstjenester

iii) forvaltning og gennemførelse af tillidstjenester

b) uden unødigt ophold og under alle omstændigheder senest 24 timer efter at være blevet opmærksom på et sikkerhedsbrud eller en forstyrrelse underrette tilsynsorganet, de identificerbare berørte enkeltpersoner, offentligheden, hvis det er i offentlighedens interesse, og, hvis det er relevant, andre relevante kompetente myndigheder om eventuelle sikkerhedsbrud eller forstyrrelser i leveringen af tjenesten eller gennemførelsen af de foranstaltninger, der er omhandlet i litra a), nr. i), ii) eller iii), som har en betydelig indvirkning på den tillidstjeneste, der udbydes, eller på de personoplysninger, der opbevares deri.

2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer med henblik på denne artikels stk. 1, litra a). Kravene i denne artikel anses for opfyldt, hvor disse standarder, specifikationer og procedurer er overholdt. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

19) I artikel 20 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Kvalificerede tillidstjenesteudbydere kontrolleres for egen regning af et overensstemmelsesvurderingsorgan mindst hver 24. måned. Formålet med kontrollen er at bekræfte, at de kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, som de udbyder, opfylder de krav, der er fastsat i denne forordning og i artikel 21 i direktiv (EU) 2022/2555. Kvalificerede tillidstjenesteudbydere forelægger den resulterende overensstemmelses-vurderingsrapport for tilsynsorganet senest tre arbejdsdage efter modtagelsen heraf.«

b) Følgende stykker indsættes:

»1a. Kvalificerede tillidstjenesteudbydere underretter tilsynsorganet senest én måned før planlagte kontroller og giver efter anmodning tilsynsorganet mulighed for at deltage som observatør.

1b. Medlemsstaterne meddeler uden unødigt ophold Kommissionen navn, adresse og akkrediteringsoplysninger for de overensstemmelsesvurderingsorganer, der er omhandlet i stk. 1, og eventuelle senere ændringer heraf. Kommissionen stiller disse oplysninger til rådighed for alle medlemsstaterne.«

c) Stk. 2, 3 og 4 erstattes af følgende:

»2. Uden at dette berører stk. 1, kan tilsynsorganet til enhver tid foretage kontrol hos eller anmode et overensstemmelsesvurderingsorgan om at udføre en overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere for disses tillidstjenesteudbyderes regning for at bekræfte, at de og deres kvalificerede tillidstjenester opfylder de krav, der er fastsat i denne forordning. Ved mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger underretter tilsynsorganet uden unødigt ophold de kompetente tilsynsmyndigheder oprettet i henhold til artikel 51 i forordning (EU) 2016/679.

3. Hvis den kvalificerede tillidstjenesteudbyder ikke opfylder hvilket som helst af de krav, der er fastsat i denne forordning, kræver tilsynsorganet, at udbyderen afhjælper denne mangel inden for en fastsat frist, hvis det er relevant.

Hvis udbyderen ikke afhjælper manglen og, hvis det er relevant, inden for den frist, der er fastsat af tilsynsorganet, tilbagetrækker tilsynsorganet, hvis det er berettiget navnlig ud fra omfanget, varigheden og konsekvenserne af manglen, den pågældende tjenesteudbyders eller den udbudte berørte tjenestes status som kvalificeret.

3a. Hvis de kompetente myndigheder, der er udpeget eller oprettet i medfør af artikel 8, stk. 1, i direktiv (EU) 2022/2555, underretter tilsynsorganet om, at den kvalificerede tillidstjenesteudbyder ikke opfylder hvilket som helst af de krav, der er fastsat i nævnte direktivs artikel 21, tilbagetrækker tilsynsorganet, hvis det er berettiget navnlig ud fra omfanget, varigheden og konsekvenserne af manglen, den pågældende tjenesteudbyders eller den udbudte berørte tjenestes status som kvalificeret.

3b. Hvis tilsynsmyndighederne oprettet i henhold til artikel 51 i forordning (EU) 2016/679 underretter tilsynsorganet om, at den kvalificerede tillidstjenesteudbyder ikke opfylder de krav, der er fastsat i nævnte forordning, tilbagetrækker tilsynsorganet, hvis det er berettiget navnlig ud fra omfanget, varigheden og konsekvenserne af manglen, den pågældende tjenesteudbyders eller den udbudte berørte tjenestes status som kvalificeret.

3c. Tilsynsorganet underretter den kvalificerede tillidstjenesteudbyder om tilbagetrækningen af vedkommendes eller den pågældende kvalificerede tjenestes status som kvalificeret. Tilsynsorganet underretter det organ, der er meddelt i henhold til denne forordnings artikel 22, stk. 3, med henblik på ajourføring af positivlisterne, der er omhandlet i nævnte artikels stk. 1, og den kompetente myndighed, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555.

4. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer med henblik på følgende:

a) akkreditering af overensstemmelsesvurderingsorganerne og for overensstemmelsesvurderingsrapporten omhandlet i stk. 1

b) revisionskrav, i henhold til hvilke overensstemmelsesvurderingsorganerne foretager overensstemmelsesvurderingen, herunder en samlet vurdering, af de kvalificerede tillidstjenesteudbydere som omhandlet i stk. 1

c) overensstemmelsesvurderingsordninger for overensstemmelsesvurderingsorganernes overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere og for udarbejdelse af rapporten omhandlet i stk. 1.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

20) I artikel 21 foretages følgende ændringer:

a) Stk. 1 og 2 affattes således:

»1. Ønsker tillidstjenesteudbydere at udbyde kvalificerede tillidstjenester, skal de anmelde deres hensigt til tilsynsorganet og indsende en overensstemmelsesvurderingsrapport udstedt af et overensstemmelsesvurderingsorgan, der bekræfter, at kravene i denne forordning og i artikel 21 i direktiv (EU) 2022/2555 er opfyldt.

2. Tilsynsorganet kontrollerer, om tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, opfylder de i denne forordning fastsatte krav, og navnlig kravene til kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, som de udbyder.

For at kontrollere, at tillidstjenesteudbyderen opfylder de krav, der er fastsat i artikel 21 i direktiv (EU) 2022/2555, anmoder tilsynsorganet de kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i nævnte direktiv, om at gennemføre tilsynsforanstaltninger med dette formål og fremlægge oplysninger om resultatet uden unødigt ophold og under alle omstændigheder senest to måneder efter modtagelsen af denne anmodning. Er kontrollen ikke afsluttet inden to måneder efter anmeldelsen, underretter disse kompetente myndigheder tilsynsorganet herom og forklarer årsagerne til forsinkelsen samt oplyser, hvornår kontrollen skal være afsluttet.

Hvis tilsynsorganet konkluderer, at tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, overholder de i denne forordning fastsatte krav, tildeler tilsynsorganet tillidstjenesteudbyderen og de tillidstjenester, som vedkommende udbyder, status som kvalificeret og underretter senest tre måneder efter anmeldelsen i overensstemmelse med nærværende artikels stk. 1, det i artikel 22, stk. 3, omhandlede organ med henblik på ajourføring af positivlisterne omhandlet i artikel 22, stk. 1.

Er kontrollen ikke afsluttet inden tre måneder efter anmeldelsen, underretter tilsynsorganet tillidstjenesteudbyderen herom og forklarer årsagerne til forsinkelsen samt oplyser, hvornår kontrollen skal være afsluttet.«

b) Stk. 4 affattes således:

»4. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter formater og procedurer for anmeldelse og kontrol med henblik på denne artikels stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

21) I artikel 24 foretages følgende ændringer:

a) Stk. 1erstattes af følgende:

»1. Når en kvalificeret tillidstjenesteudbyder udsteder et kvalificeret certifikat eller en kvalificeret elektronisk attestering af attributter, kontrollerer udbyderen identiteten af og, hvis det er relevant, attributter knyttet til den fysiske eller juridiske person, til hvem det kvalificerede certifikat eller den kvalificerede elektroniske attestering af attributter skal udstedes.

1a. Den kontrol af identiteten, der er omhandlet i stk. 1, udføres med hensigtsmæssige midler af den kvalificerede tillidstjenesteudbyder enten direkte eller via en tredjemand på grundlag af én af følgende metoder eller, når det er nødvendigt, en kombination heraf og i overensstemmelse med de gennemførelsesretsakter, der er omhandlet i stk. 1c:

a) ved hjælp af den europæiske digitale identitetstegnebog eller et anmeldt elektronisk identifikationsmiddel, der opfylder de krav, der er fastsat i artikel 8 med hensyn til sikringsniveauet »høj«

b) ved hjælp af et certifikat af en kvalificeret elektronisk signatur eller af et kvalificeret elektronisk segl udstedt under overholdelse af litra a), c) eller d)

c) ved hjælp af andre identifikationsmetoder, der sikrer identifikation af personen med en høj grad af tillid, og hvis overensstemmelse bekræftes af et overensstemmelsesvurderingsorgan

d) ved fysisk tilstedeværelse af den fysiske person eller af en bemyndiget repræsentant for den juridiske person, ved hjælp af passende dokumentation og procedurer, i overensstemmelse med national ret.

1b. Den kontrol af attributterne, der er omhandlet i stk. 1, udføres med hensigtsmæssige midler af den kvalificerede tillidstjenesteudbyder enten direkte eller via en tredjemand på grundlag af én af følgende metoder eller, når det er nødvendigt, en kombination heraf og i overensstemmelse med de gennemførelsesretsakter, der er omhandlet i stk. 1c:

a) ved hjælp af den europæiske digitale identitetstegnebog eller et anmeldt elektronisk identifikationsmiddel, der opfylder de krav, der er fastsat i artikel 8 med hensyn til sikringsniveauet »høj«

b) ved hjælp af et certifikat for en kvalificeret elektronisk signatur eller for et kvalificeret elektronisk segl, der er udstedt i overensstemmelse med stk. 1a, litra a), c) eller d)

c) ved hjælp af en kvalificeret elektronisk attestering af attributter

d) ved hjælp af andre metoder, der sikrer kontrol af attributterne med en høj grad af tillid, og hvis overensstemmelse bekræftes af et overensstemmelsesvurderingsorgan

e) ved fysisk tilstedeværelse af den fysiske person eller af en bemyndiget repræsentant for den juridiske person, ved hjælp af passende dokumentation og procedurer, i overensstemmelse med national ret.

1c. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, tekniske specifikationer og procedurer for kontrollen af identitet og attributter i overensstemmelse med denne artikels stk. 1, 1a og 1b. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

b) I stk. 2 foretages følgende ændringer:

i) Litra a) affattes således:

»a) informere tilsynsorganet mindst én måned, før der gennemføres ændringer i udbuddet af dennes kvalificerede tillidstjenester, eller mindst tre måneder før, hvis det er hensigten at ophøre med denne virksomhed«.

ii) Litra d) og e) affattes således:

»d) på en klar, udførlig og let forståelig måde underrette på et offentligt tilgængeligt sted eller individuelt de personer, der ønsker at gøre brug af en kvalificeret tillidstjeneste, om de nøjagtige vilkår og betingelser for anvendelsen af denne tjeneste, herunder eventuelle begrænsninger for anvendelsen heraf, inden de indgår i et kontraktforhold

e) anvende pålidelige systemer og produkter, som er beskyttet mod ændringer, og sikre den tekniske sikkerhed og pålidelighed i de processer, som disse systemer og produkter understøtter, herunder ved hjælp af passende kryptografiske teknikker«.

iii) Følgende litraer indsættes:

»fa) uanset artikel 21 i direktiv (EU) 2022/2555 indføre passende politikker og træffe tilsvarende foranstaltninger til at styre juridiske, erhvervsmæssige, operationelle og andre direkte eller indirekte risici i forbindelse med leveringen af den kvalificerede tillidstjeneste, herunder som minimum foranstaltninger vedrørende følgende:

i) registrerings- og onboardingprocedurer for en tjeneste

ii) proceduremæssig eller administrativ kontrol

iii) forvaltning og gennemførelse af tjenester

fb) uden unødigt ophold og under alle omstændigheder inden for 24 timer efter hændelsen underrette tilsynsorganet, de identificerbare berørte enkeltpersoner, andre relevante kompetente organer, hvis det er relevant, og efter anmodning fra tilsynsorganet offentligheden, hvis det er i offentlighedens interesse, om eventuelle sikkerhedsbrud eller forstyrrelser i leveringen af tjenester eller gennemførelsen af de foranstaltninger, der er omhandlet i litra fa), nr. i), ii) eller iii), som har en betydelig indvirkning på den tillidstjeneste, der udbydes, eller på de personoplysninger, der opbevares heri«.

iv) Litra g), h) og i) affattes således:

»g) træffe passende foranstaltninger mod forfalskning, tyveri eller misbrug af data eller sletning, ændring eller utilgængeliggørelse af data uden ret hertil

h) så længe det er nødvendigt, efter at den kvalificerede tillidstjenesteudbyder har indstillet sin virksomhed, registrere alle relevante oplysninger om de data, den kvalificerede tillidstjenesteudbyder har udstedt og modtaget, og sørge for, at de er tilgængelige, for at kunne fremlægge bevis i retssager og for at garantere tjenestens kontinuitet. Sådan registrering kan ske elektronisk

i) have en ajourført plan i tilfælde af virksomhedsafbrydelse for at sikre tjenestens kontinuitet i overensstemmelse med bestemmelser, der er kontrolleret af tilsynsorganet i henhold til artikel 46b, stk. 4, litra i)«.

v) Litra j) udgår.

vi) Følgende afsnit tilføjes:

»Tilsynsorganet kan anmode om oplysninger ud over de oplysninger, der er meddelt i medfør af første afsnit, litra a), eller om resultatet af en overensstemmelsesvurdering og kan stille betingelser for tilladelsen til at gennemføre de påtænkte ændringer af de kvalificerede tillidstjenester. Er kontrollen ikke afsluttet inden tre måneder efter anmeldelsen, underretter tilsynsorganet tillidstjenesteudbyderen herom og forklarer årsagerne til forsinkelsen samt oplyser, hvornår kontrollen skal være afsluttet.«

c) Stk. 5 erstattes af følgende:

»4a. Stk. 3 og 4 finder tilsvarende anvendelse på tilbagekaldelse af kvalificerede elektroniske attesteringer af attributter.

4b. Kommissionen tillægges beføjelse til at vedtage delegerede retsakter i overensstemmelse med artikel 47 vedrørende fastlæggelse af de i denne artikels stk. 2, litra fa), omhandlede yderligere foranstaltninger.

5. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for de i denne artikels stk. 2 omhandlede krav. Det formodes, at kravene i nærværende stykke er opfyldt, når disse standarder, specifikationer og procedurer er overholdt. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

22) I kapitel III, afdeling 3, indsættes følgende artikel:

»*Artikel 24a*

Anerkendelse af kvalificerede tillidstjenester

1. Kvalificerede elektroniske signaturer baseret på et kvalificeret certifikat, der er udstedt i én medlemsstat, og kvalificerede elektroniske segl baseret på et kvalificeret certifikat, der er udstedt i én medlemsstat, anerkendes som henholdsvis kvalificerede elektroniske signaturer og kvalificerede elektroniske segl i alle andre medlemsstater.

2. Kvalificerede elektroniske signaturgenereringssystemer og kvalificerede elektroniske seglgenereringssystemer, der er certificeret i én medlemsstat, anerkendes som henholdsvis kvalificerede elektroniske signaturgenereringssystemer og kvalificerede elektroniske seglgenereringssystemer i alle andre medlemsstater.

3. Et kvalificeret certifikat for elektroniske signaturer, et kvalificeret certifikat for elektroniske segl, en kvalificeret tillidstjeneste til forvaltning af kvalificerede elektroniske signaturgenereringssystemer på afstand og en kvalificeret tillidstjeneste til forvaltning af kvalificerede elektroniske seglgenereringssystemer på afstand, der udbydes i én medlemsstat, anerkendes som henholdsvis et kvalificeret certifikat for elektroniske signaturer, et kvalificeret certifikat for elektroniske segl, en kvalificeret tillidstjeneste til forvaltning af kvalificerede elektroniske signaturgenereringssystemer på afstand og en kvalificeret tillidstjeneste til forvaltning af kvalificerede elektroniske seglgenereringssystemer på afstand i alle andre medlemsstater.

4. En kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer og en kvalificeret valideringstjeneste for kvalificerede elektroniske segl, der udbydes i én medlemsstat, anerkendes som henholdsvis en kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer og en kvalificeret valideringstjeneste for kvalificerede elektroniske segl i alle andre medlemsstater.

5. En kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer og en kvalificeret tjeneste til bevaring af kvalificerede elektroniske segl, der udbydes i én medlemsstat, anerkendes som henholdsvis en kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer og en kvalificeret tjeneste til bevaring af kvalificerede elektroniske segl i alle andre medlemsstater.

6. Et kvalificeret elektronisk tidsstempel, der udbydes i én medlemsstat, anerkendes som et kvalificeret elektronisk tidsstempel i alle andre medlemsstater.

7. Et kvalificeret certifikat for webstedsautentifikation, der udstedes i én medlemsstat, anerkendes som et kvalificeret certifikat for webstedsautentifikation i alle andre medlemsstater.

8. En kvalificeret elektronisk registreret leveringstjeneste, der udbydes i én medlemsstat, anerkendes som en kvalificeret elektronisk registreret leveringstjeneste i alle andre medlemsstater.

9. En kvalificeret elektronisk attestering af attributter, der udstedes i én medlemsstat, anerkendes som en kvalificeret elektronisk attestering af attributter i alle andre medlemsstater.

10. En kvalificeret elektronisk arkiveringstjeneste, der udbydes i én medlemsstat, anerkendes som en kvalificeret elektronisk arkiveringstjeneste i alle andre medlemsstater.

11. En kvalificeret elektronisk hovedbog, der udbydes i én medlemsstat, anerkendes som en kvalificeret elektronisk hovedbog i alle andre medlemsstater.«

23) I artikel 25 udgår stk. 3.

24) I artikel 26 foretages følgende ændringer:

a) Det eneste stykke nummereres stk. 1.

b) Følgende stykke tilføjes:

»2. Senest den 21. maj 2026 vurderer Kommissionen, hvorvidt det er nødvendigt at vedtage gennemførelsesretsakter for at fastsætte en liste over referencestandarder og, hvor det er nødvendigt, fastsætte specifikationer og procedurer for avancerede elektroniske signaturer. På grundlag af denne vurdering kan Kommissionen vedtage sådanne gennemførelsesretsakter. En avanceret elektronisk signatur, der overholder disse standarder, specifikationer og procedurer, formodes at opfylde kravene til avancerede elektroniske signaturer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

25) I artikel 27 udgår stk. 4.

26) Artikel 28, stk. 6, affattes således:

»6. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for kvalificerede certifikater for elektroniske signaturer. Et kvalificeret certifikat for elektronisk signatur, der overholder disse standarder, specifikationer og procedurer, formodes at opfylde kravene i bilag I. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

27) I artikel 29 indsættes følgende stykke:

»1a. Generering eller forvaltning af elektroniske signaturgenereringsdata eller kopiering af sådanne signaturgenereringsdata til backupformål må kun foretages på underskriverens vegne, på underskriverens anmodning og af en kvalificeret tillidstjenesteudbyder, der udbyder en kvalificeret tillidstjeneste til forvaltning af et kvalificeret elektronisk signaturgenereringssystem på afstand.«

28) Følgende artikel indsættes:

»*Artikel 29a*

Krav til kvalificerede tjenester til forvaltning af kvalificerede elektroniske signaturgenereringssystemer på afstand

1. Forvaltning af kvalificerede elektroniske signaturgenereringssystemer på afstand som en kvalificeret tjeneste må kun varetages af en kvalificeret tillidstjenesteudbyder, som:

a) genererer eller forvalter elektroniske signaturgenereringsdata på underskriverens vegne

b) uagtet bilag II, punkt 1), litra d), kopierer de elektroniske signaturgenereringsdata udelukkende til backupformål, forudsat at følgende krav er opfyldt:

i) der opretholdes samme niveau af sikkerhed for de kopierede datasæt som for de originale datasæt

ii) antallet af kopierede datasæt overstiger ikke det minimum, der er nødvendigt for at sikre tjenestens kontinuitet

c) opfylder de krav, der er angivet i certificeringsrapporten for det specifikke kvalificerede elektroniske signaturgenereringssystem på afstand, der er udstedt i medfør af artikel 30.

2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og, hvor det er nødvendigt, specifikationer og procedurer med henblik på denne artikels stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

29) I artikel 30 indsættes følgende stykke:

»3a. Gyldigheden af en i stk. 1 omhandlet certificering må ikke overstige fem år, forudsat at der foretages sårbarhedsvurderinger hvert andet år. Hvis der konstateres sårbarheder, og disse ikke afhjælpes, annulleres certificeringen.«

30) Artikel 31, stk. 3, affattes således:

»3. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter formater og procedurer, der finder anvendelse med henblik på denne artikels stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

31) I artikel 32 foretages følgende ændringer:

a) I stykke 1 tilføjes følgende afsnit:

»En validering af kvalificerede elektroniske signaturer, der overholder de i stk. 3 omhandlede standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i dette stykkes første afsnit.«

b) Stk. 3 affattes således:

»3. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for validering af kvalificerede elektroniske signaturer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

32) Følgende artikel indsættes:

»*Artikel 32a*

Krav til validering af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater

1. Processen for validering af en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat skal bekræfte gyldigheden af en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, forudsat at:

a) det certifikat, der understøtter signaturen, på underskriftstidspunktet var et kvalificeret certifikat for elektronisk signatur, der overholder bilag I

b) det kvalificerede certifikat var udstedt af en kvalificeret tillidstjenesteudbyder og var gyldigt på underskriftstidspunktet

c) signaturvalideringsdataene stemmer overens med de data, der leveres til modtagerparten

d) det entydige sæt data, der repræsenterer underskriveren i certifikatet, leveres korrekt til modtagerparten

e) en eventuel anvendelse af et pseudonym fremgår klart for modtagerparten, hvis der på underskriftstidspunktet blev anvendt et pseudonym

f) de underskrevne datas integritet ikke er bragt i fare

g) kravene i artikel 26 er opfyldt på underskriftstidspunktet.

2. Det system, der anvendes til validering af den avancerede elektroniske signatur, der er baseret på et kvalificeret certifikat, skal levere det korrekte resultat af valideringsprocessen til modtagerparten og gøre det muligt for vedkommende at opdage eventuelle sikkerhedsproblemer.

3. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for validering af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater. En validering af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater, og som overholder disse standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i denne artikels stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

33) Artikel 33, stk. 2, affattes således:

»2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for den i denne artikels stk. 1 omhandlede kvalificerede valideringstjeneste. En kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer, der overholder disse standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i denne artikels stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

34) I artikel 34 foretages følgende ændringer:

a) Følgende stykke indsættes:

»1a. Ordninger for kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer, der overholder de i stk. 2 omhandlede standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i stk. 1.«

b) Stk. 2 affattes således:

»2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for den kvalificerede tjeneste til bevaring af kvalificerede elektroniske signaturer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

35) I artikel 35 udgår stk. 3.

36) I artikel 36 foretages følgende ændringer:

a) Det eneste stykke nummereres stk. 1.

b) Følgende stykke tilføjes:

»2. Senest den 21. maj 2026 vurderer Kommissionen, hvorvidt det er nødvendigt at vedtage gennemførelsesretsakter for at fastsætte en liste over referencestandarder og, hvor det er nødvendigt, fastsætte specifikationer og procedurer for avancerede elektroniske segl. På grundlag af denne vurdering kan Kommissionen vedtage sådanne gennemførelsesretsakter. Et avanceret elektronisk segl, der overholder disse standarder, specifikationer og procedurer, formodes at opfylde kravene til avancerede elektroniske segl. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

37) I artikel 37 udgår stk. 4.

38) Artikel 38, stk. 6, affattes således:

»6. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for kvalificerede certifikater for elektroniske segl. Et kvalificeret certifikat for elektronisk segl, der overholder disse standarder, specifikationer og procedurer, formodes at opfylde kravene i bilag III. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

39) Følgende artikel indsættes:

»*Artikel 39a*

Krav til kvalificerede tjenester til forvaltning af kvalificerede elektroniske seglgenereringssystemer på afstand

Artikel 29a finder tilsvarende anvendelse på kvalificerede tjenester til forvaltning af kvalificerede elektroniske seglgenereringssystemer på afstand.«

40) I kapitel III, afdeling 5, indsættes følgende artikel:

»*Artikel 40a*

Krav til validering af avancerede elektroniske segl, der er baseret på kvalificerede certifikater

Artikel 32a finder tilsvarende anvendelse på validering af avancerede elektroniske segl, der er baseret på kvalificerede certifikater.«

41) I artikel 41 udgår stk. 3.

42) I artikel 42 foretages følgende ændringer:

a) Følgende stykke indsættes:

»1a. Forbindelser af dato og tidspunkt med data og nøjagtighed af tidskilden, der overholder de i stk. 2 omhandlede standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i stk. 1.«

b) Stk. 2 affattes således:

»2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for forbindelser af dato og tidspunkt med data og for fastsættelse af nøjagtigheden af tidskilder. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

43) I artikel 44 foretages følgende ændringer:

a) Følgende stykke indsættes:

»1a. En dataafsendelses- og -modtagelsesproces, der overholder de i stk. 2 omhandlede standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i stk. 1.«

b) Stk. 2 affattes således:

»2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for dataafsendelses- og -modtagelsesprocesser. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

c) Følgende stykker indsættes:

»2a. Udbydere af kvalificerede elektroniske registrerede leveringstjenester kan nå til enighed om interoperabilitet mellem de kvalificerede elektroniske registrerede leveringstjenester, som de udbyder. En sådan interoperabilitetsramme skal opfylde kravene i stk. 1, og en sådan opfyldelse skal bekræftes af et overensstemmelsesvurderingsorgan.

2b. Kommissionen kan ved hjælp af gennemførelsesretsakter fastsætte en liste over referencestandarder og, hvor det er nødvendigt, fastsætte specifikationer og procedurer for den i denne artikels stk. 2a omhandlede interoperabilitetsramme. Standardernes tekniske specifikationer og indhold skal være omkostningseffektive og forholdsmæssige. Gennemførelsesretsakterne vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

44) Artikel 45 affattes således:

»*Artikel 45*

Krav til kvalificerede certifikater for webstedsautentifikation

1. Kvalificerede certifikater for webstedsautentifikation skal opfylde kravene i bilag IV. Evalueringen af opfyldelsen af de pågældende krav foretages i overensstemmelse med de standarder, specifikationer og procedurer, der er omhandlet i denne artikels stk. 2.

1a. De kvalificerede certifikater for webstedsautentifikation, der udstedes i overensstemmelse med denne artikels stk. 1, skal anerkendes af webbrowserudbydere. Webbrowserudbydere sikrer, at de identitetsdata, der attesteres i certifikatet, og yderligere attesterede attributter vises på en brugervenlig måde. Webbrowserudbydere sikrer støtte af og interoperabilitet med kvalificerede certifikater for webstedsautentifikation omhandlet i denne artikels stk. 1 med undtagelse af mikrovirksomheder eller små virksomheder som defineret i artikel 2 til bilaget til henstilling 2003/361/EF i de første fem år, hvor de fungerer som udbydere af webbrowsertjenester.

1b. Kvalificerede certifikater for webstedsautentifikation må ikke undergives andre ufravigelige krav end kravene i stk. 1.

2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for de i denne artikels stk. 1 omhandlede kvalificerede certifikater for webstedsautentifikation. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

45) Følgende artikel indsættes:

»*Artikel 45a*

Forebyggende foranstaltninger vedrørende cybersikkerhed

1. Webbrowserudbydere må ikke træffe foranstaltninger i strid med deres forpligtelser fastsat i artikel 45, navnlig kravene om at anerkende kvalificerede certifikater for webstedsautentifikation og vise de opgivne identitetsdata på en brugervenlig måde.

2. Uanset stk. 1 og kun i tilfælde af begrundet mistanke om sikkerhedsbrud eller tab af integritet for et identificeret certifikat eller sæt af certifikater kan webbrowserudbydere træffe forebyggende foranstaltninger vedrørende det pågældende certifikat eller sæt af certifikater.

3. Hvor en webbrowserudbyder træffer forebyggende foranstaltninger i medfør af stk. 2, underretter webbrowserudbyderen skriftligt og uden ugrundet ophold Kommissionen, det kompetente tilsynsorgan, den enhed, som certifikatet er udstedt til, og den kvalificerede tillidstjenesteudbyder, der har udstedt det pågældende certifikat eller sæt af certifikater, om sin mistanke sammen med en beskrivelse af de foranstaltninger, der er truffet for at afbøde denne mistanke. Når det kompetente tilsynsorgan modtager en sådan underretning, udsteder den en kvittering for modtagelsen til den pågældende webbrowserudbyder.

4. Det kompetente tilsynsorgan undersøger spørgsmålene i underretningen i overensstemmelse med artikel 46b, stk. 4, litra k). Når resultatet af denne undersøgelse ikke fører til inddragelse af certifikatets status som kvalificeret, underretter tilsynsorganet webbrowserudbyderen herom og anmoder den pågældende udbyder om at bringe de forebyggende foranstaltninger, der er omhandlet i nærværende artikels stk. 2, til ophør.«

46) I kapitel III tilføjes følgende afdelinger:

»AFDELING 9

ELEKTRONISK ATTESTERING AF ATTRIBUTTER

Artikel 45b

Retsvirkninger af elektronisk attestering af attributter

1. Retsvirkning eller antagelighed som bevis i retssager af elektroniske attesteringer af attributter må ikke nægtes alene af den grund, at attesteringen er i elektronisk form, eller at den ikke opfylder kravene til kvalificerede elektroniske attesteringer af attributter.

2. En kvalificeret elektronisk attestering af attributter og attesteringer af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, har samme retsvirkning som lovligt udstedte attesteringer i papirform.

3. En attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde i én medlemsstat, anerkendes som en attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde i alle medlemsstater.

Artikel 45c

Elektronisk attestering af attributter i offentlige tjenester

Hvis der i henhold til national ret kræves elektronisk identifikation ved hjælp af et elektronisk identifikationsmiddel og autentifikation for adgang til en onlinetjeneste, der leveres af en offentlig myndighed, erstatter personidentifikationsdata i den elektroniske attestering af attributter ikke elektronisk identifikation ved hjælp af et elektronisk identifikationsmiddel og autentifikation med elektronisk identifikation, medmindre medlemsstaten specifikt tillader dette. I disse tilfælde accepteres kvalificeret elektronisk attestering af attributter fra andre medlemsstater også.

Artikel 45d

Krav til kvalificeret elektronisk attestering af attributter

1. Kvalificeret elektronisk attestering af attributter skal opfylde kravene i bilag V.

2. Evalueringen af opfyldelsen af de krav, der er fastsat i bilag V, foretages i overensstemmelse med de standarder, specifikationer og procedurer, der er omhandlet i denne artikels stk. 5.

3. Kvalificerede elektroniske attesteringer af attributter er ikke omfattet af ufravigelige krav ud over de krav, der er fastsat i bilag V.

4. Hvis en kvalificeret elektronisk attestering af attributter er blevet tilbagekaldt efter den første udstedelse, mister den sin gyldighed fra tidspunktet for tilbagekaldelsen, og dens status kan under ingen omstændigheder genetableres.

5. Senest den 21. november 2024 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for kvalificerede elektroniske attesteringer af attributter. Disse gennemførelsesretsakter skal være i overensstemmelse med de i artikel 5a, stk. 23, omhandlede gennemførelsesretsakter om gennemførelsen af den europæiske digitale identitetstegnebog. De vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 45e

Kontrol af attributter i forhold til autentiske kilder

1. Medlemsstaterne sikrer senest 24 måneder fra ikrafttrædelsesdatoen for de i artikel 5a, stk. 23, og artikel 5c, stk. 6, omhandlede gennemførelsesretsakter, at der i det mindste for de i bilag VI anførte attributter, når disse attributter er afhængige af autentiske kilder i den offentlige sektor, træffes foranstaltninger til at gøre det muligt for kvalificerede tillidstjenesteudbydere af elektroniske attesteringer af attributter ved hjælp af elektroniske midler at kontrollere de pågældende attributter efter anmodning fra brugeren, i overensstemmelse med EU-retten eller national ret.

2. Senest den 21. november 2024 fastsætter Kommissionen under hensyntagen til relevante internationale standarder ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for kataloget over attributter samt ordninger for attestering af attributter og kontrolprocedurer for kvalificerede elektroniske attesteringer af attributter med henblik på denne artikels stk. 1. Disse gennemførelsesretsakter skal være i overensstemmelse med de i artikel 5a, stk. 23, omhandlede gennemførelsesretsakter om gennemførelsen af den europæiske digitale identitetstegnebog. De vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 45f

Krav til elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde

1. En elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, skal opfylde følgende krav:

a) dem, der er fastsat i bilag VII

b) det kvalificerede certifikat, der støtter den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl fra den i artikel 3, nr. 46), omhandlede offentlige myndighed, der er identificeret som den i bilag VII, litra b), omhandlede udsteder, indeholdende et specifikt sæt certificerede attributter i en form, der egner sig til automatisk behandling:

   i) med angivelse af, at den udstedende myndighed er etableret i overensstemmelse med EU-retten eller national ret som ansvarlig for den autentiske kilde, på grundlag af hvilken den elektroniske attestering af attributter udstedes, eller som den myndighed, der er udpeget til at handle på dens vegne

   ii) med tilvejebringelse af et sæt data, der utvetydigt repræsenterer den i nr. i) omhandlede autentiske kilde, og

   iii) med fastlæggelse af den i nr. i) omhandlede EU-ret eller nationale ret.

2. Den medlemsstat, hvori de i artikel 3, nr. 46), omhandlede offentlige myndigheder er hjemmehørende, sikrer, at de offentlige myndigheder, der udsteder elektroniske attesteringer af attributter, lever op til et pålideligheds- og troværdighedsniveau, der svarer til kvalificerede tillidstjenesteudbydere i overensstemmelse med artikel 24.

3. Medlemsstaterne underretter Kommissionen om de i artikel 3, nr. 46), omhandlede offentlige myndigheder. Denne underretning skal omfatte en overensstemmelsesvurderingsrapport udstedt af et overensstemmelsesvurderingsorgan, der bekræfter, at kravene i denne artikels stk. 1, 2 og 6 er opfyldt. Kommissionen stiller listen over de offentlige myndigheder, der er omhandlet i artikel 3, nr. 46), til rådighed for offentligheden via en sikker kommunikationsforbindelse og i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

4. Hvis en elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, er blevet tilbagekaldt efter den første udstedelse, mister den sin gyldighed fra tidspunktet for tilbagekaldelsen og dens status må ikke genetableres.

5. En elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, anses for at overholde kravene i stk. 1, hvis den opfylder de i stk. 6 omhandlede standarder, specifikationer og procedurer.

6. Senest den 21. november 2024 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde. Disse gennemførelsesretsakter skal være i overensstemmelse med den i artikel 5a, stk. 23, omhandlede gennemførelsesretsakt om gennemførelsen af den europæiske digitale identitetstegnebog. De vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

7. Senest den 21. november 2024 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer med henblik på denne artikels stk. 3. Disse gennemførelsesretsakter skal være i overensstemmelse med den i artikel 5a, stk. 23, omhandlede gennemførelsesretsakt om gennemførelsen af den europæiske digitale identitetstegnebog. De vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

8. De i artikel 3, nr. 46), omhandlede offentlige myndigheder, der udsteder elektronisk attestering af attributter, stiller en grænseflade til europæiske digitale identitetstegnebøger, der er leveret i overensstemmelse med artikel 5a, til rådighed.

Artikel 45g

Udstedelse af elektroniske attesteringer af attributter til europæiske digitale identitetstegnebøger

1. Udbydere af elektroniske attesteringer af attributter giver brugere af europæiske digitale identitetstegnebøger mulighed for at anmode om, indhente, lagre og forvalte den elektroniske attestering af attributter, uanset i hvilke medlemsstater den europæiske digitale identitetstegnebog leveres.

2. Udbydere af kvalificerede elektroniske attesteringer af attributter stiller en grænseflade med europæiske digitale identitetstegnebøger, der er leveret i overensstemmelse med artikel 5a, til rådighed.

Artikel 45h

Supplerende regler for levering af tjenester til elektronisk attestering af attributter

1. Udbydere af kvalificerede og ikkekvalificerede tjenester til elektronisk attestering af attributter må ikke kombinere personoplysninger relateret til leveringen af sådanne tjenester med personoplysninger fra andre tjenester, som de eller deres handelspartnere udbyder.

2. Personoplysninger, der er relateret til elektronisk attestering af attributter, holdes logisk adskilt fra andre data, der opbevares af udbyderen af elektronisk attestering af attributter.

3. Udbydere af tjenester til elektronisk attestering af attributter gennemfører leveringen af sådanne kvalificerede tillidstjenester på en måde, der er funktionelt adskilt fra andre tjenester, som de leverer.

AFDELING 10

ELEKTRONISKE ARKIVERINGSTJENESTER

Artikel 45i

Retsvirkning af elektronisk arkiveringstjeneste

1. Elektroniske data og elektroniske dokumenter, der opbevares ved hjælp af en elektronisk arkiveringstjeneste, må ikke nægtes retsvirkning eller antagelighed som bevismateriale under retssager alene af den grund, at de er i elektronisk form, eller at de ikke er opbevaret ved hjælp af en kvalificeret elektronisk arkiveringstjeneste.

2. Elektroniske data og elektroniske dokumenter, der opbevares ved hjælp af en kvalificeret elektronisk arkiveringstjeneste, formodes at have deres integritet og oprindelse i hele opbevaringsperioden af den kvalificerede tillidstjenesteudbyder.

Artikel 45j

Krav til kvalificerede elektroniske arkiveringstjenester

1. Kvalificerede elektroniske arkiveringstjenester skal opfylde følgende krav:

a) de udbydes af kvalificerede tillidstjenesteudbydere

b) de anvender procedurer og teknologier, der kan sikre elektroniske data og elektroniske dokumenters holdbarhed og læsbarhed ud over den teknologiske gyldighedsperiode og i det mindste i den lovbestemte eller kontraktlige opbevaringsperiode, samtidig med at deres integritet og nøjagtigheden af deres oprindelse bevares

c) de sikrer, at disse elektroniske data og elektroniske dokumenter opbevares på en sådan måde, at de beskyttes mod tab og ændringer, bortset fra ændringer vedrørende deres medium eller elektroniske format

d) de gør det muligt for bemyndigede modtagerparter automatisk at modtage en rapport, der bekræfter, at elektroniske data og elektroniske dokumenter, der hentes fra et kvalificeret elektronisk arkiv, er omfattet af formodningen om dataenes integritet fra begyndelsen af opbevaringsperioden til det tidspunkt, hvor de hentes.

Den i første afsnits litra d) omhandlede rapport skal leveres på en pålidelig og effektiv måde og være forsynet med den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl fra udbyderen af den kvalificerede elektroniske arkiveringstjeneste.

2. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for kvalificerede elektroniske arkiveringstjenester. En kvalificeret elektronisk arkiveringstjeneste, der overholder disse standarder, specifikationer og procedurer, formodes at opfylde kravene til kvalificerede elektroniske arkiveringstjenester. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

AFDELING 11

ELEKTRONISKE HOVEDBØGER

Artikel 45k

Retsvirkninger af elektroniske hovedbøger

1. Retsvirkning og antagelighed som bevis i retssager af elektroniske hovedbøger må ikke nægtes alene af den grund, at hovedbogen er i elektronisk form, eller at den ikke opfylder kravene til kvalificerede elektroniske hovedbøger.

2. Dataposter i kvalificerede elektroniske hovedbøger er omfattet af formodningen om deres entydige og nøjagtige kronologiske rækkefølge og om deres integritet.

Artikel 45l

Krav til kvalificerede elektroniske hovedbøger

1. Kvalificerede elektroniske hovedbøger skal opfylde følgende krav:

a) de er oprettet og forvaltes af én eller flere kvalificerede tillidstjenesteudbydere

b) de fastlægger oprindelsen af dataposterne i hovedbogen

c) de sikrer en entydig kronologisk rækkefølge af dataposterne i hovedbogen

d) de registrerer data på en sådan måde, at enhver efterfølgende ændring af dataene omgående kan konstateres, hvorved deres integritet over tid sikres.

2. En elektronisk hovedbog, der overholder de i stk. 3 omhandlede standarder, specifikationer og procedurer, formodes at opfylde de krav, der er fastsat i stk. 1.

3. Senest den 21. maj 2025, fastsætter Kommissionen ved hjælp af gennemførelsesretsakter en liste over referencestandarder og fastsætter, hvor det er nødvendigt, specifikationer og procedurer for de i denne artikels stk. 1 fastsatte krav. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

47) Følgende kapitel indsættes:

»KAPITEL IVa

STYRINGSRAMME

Artikel 46a

Tilsyn med rammen for den europæiske digitale identitetstegnebog

1. Hver medlemsstat udpeger et eller flere tilsynsorganer, der er hjemmehørende på deres område.

De tilsynsorganer, der er udpeget i medfør af første afsnit, tillægges de nødvendige beføjelser og tilstrækkelige ressourcer til varetagelsen af deres opgaver på en virkningsfuld, effektiv og uafhængig måde.

2. Medlemsstaterne meddeler Kommissionen navn og adresse på de tilsynsorganer, der er udpeget i medfør af stk. 1, og eventuelle senere ændringer heraf. Kommissionen offentliggør en liste over de meddelte tilsynsorganer.

3. De i medfør af stk. 1 udpegede tilsynsorganer har følgende rolle:

a) at føre tilsyn med udbydere af europæiske digitale identitetstegnebøger, der er hjemmehørende i den udpegende medlemsstat, og ved hjælp af forudgående og efterfølgende tilsynsvirksomhed at sikre, at disse udbydere og europæiske digitale identitetstegnebøger, som de udbyder, opfylder kravene i denne forordning

b) om nødvendigt at gribe ind over for udbydere af europæiske digitale identitetstegnebøger, der er hjemmehørende på den udpegende medlemsstats område, ved hjælp af efterfølgende tilsynsaktiviteter, når de får oplysninger om, at udbydere eller europæiske digitale identitetstegnebøger, som de udbyder, overtræder denne forordning.

4. De i medfør af stk. 1 udpegede tilsynsorganers opgaver omfatter navnlig følgende:

a) at samarbejde med andre tilsynsorganer og yde dem bistand i overensstemmelse med artikel 46c og 46e

b) at anmode om de oplysninger, der er nødvendige for at føre tilsyn med overholdelsen af denne forordning

c) at underrette de relevante kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555 i de berørte medlemsstater, om alle væsentlige sikkerhedsbrud eller tab af integritet, som de får kendskab til i forbindelse med udførelsen af sine opgaver, og i tilfælde af væsentlige sikkerhedsbrud eller tab af integritet, som vedrører andre medlemsstater, at underrette det centrale kontaktpunkt, der er udpeget eller oprettet i henhold til artikel 8, stk. 3, i direktiv (EU) 2022/2555, i den berørte medlemsstat, og de centrale kontaktpunkter, der er udpeget i henhold til denne forordnings artikel 46c, stk. 1, i de øvrige berørte medlemsstater, og at informere offentligheden eller pålægge udbydere af europæiske digitale identitetstegnebøger at gøre det, hvis tilsynsorganet fastslår, at det er i offentlighedens interesse, at sikkerhedsbruddet eller tabet af integritet offentliggøres

d) at foretage inspektioner på stedet og eksternt tilsyn

e) at pålægge udbydere af europæiske digitale identitetstegnebøger at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i denne forordning

f) at suspendere eller annullere registreringen og medtagelsen af modtagerparter i den mekanisme, der er omhandlet i artikel 5b, stk. 7, i tilfælde af ulovlig eller svigagtig anvendelse af den europæiske digitale identitetstegnebog

g) at samarbejde med de kompetente tilsynsmyndigheder, der er oprettet i henhold til artikel 51 i forordning (EU) 2016/679, navnlig ved uden unødigt ophold at underrette dem, hvor der er mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger, og om sikkerhedsbrud, der synes at udgøre brud på persondatasikkerheden.

5. Kræver det i medfør af stk. 1 udpegede tilsynsorgan, at udbyderen af en europæisk digital identitetstegnebog afhjælper enhver forsømmelse af at opfylde kravene i denne forordning i medfør af stk. 4, litra e), og handlet den pågældende udbyder ikke i overensstemmelse hermed og i givet fald inden for en af dette tilsynsorgan fastsat frist, kan det i medfør af stk. 1 udpegede tilsynsorgan under hensyntagen til navnlig denne forsømmelses omfang, varighed og konsekvenser pålægge udbyderen at suspendere eller ophøre med at levere den europæiske digitale identitetstegnebog. Tilsynsorganet underretter uden unødigt ophold tilsynsorganerne i andre medlemsstater, Kommissionen, modtagerparterne og brugerne af den europæiske digitale identitetstegnebog om afgørelsen om at kræve suspension eller ophør af leveringen af den europæiske digitale identitetstegnebog.

6. Senest den 31. marts hvert år forelægger de i medfør af stk. 1 udpegede tilsynsorganer Kommissionen en rapport om det foregående kalenderårs primære tilsynsvirksomhed. Kommissionen stiller disse årlige rapporter til rådighed for Europa-Parlamentet og Rådet.

7. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter formaterne og procedurerne for den i denne artikels stk. 6 omhandlede rapport. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 46b

Tilsyn med tillidstjenester

1. Hver medlemsstat udpeger et tilsynsorgan, der er oprettet på dens område, eller udpeger efter gensidig aftale med en anden medlemsstat et tilsynsorgan, der er hjemmehørende i den pågældende anden medlemsstat. Dette tilsynsorgan er ansvarligt for tilsynsopgaver i den udpegende medlemsstat for så vidt angår tillidstjenester.

De tilsynsorganer, der er udpeget i medfør af første afsnit, tillægges de nødvendige beføjelser og tilstrækkelige ressourcer til varetagelsen af deres opgaver.

2. Medlemsstaterne meddeler Kommissionen navn og adresse på deres tilsynsorganer, der er udpeget i medfør af stk. 1, og eventuelle senere ændringer heraf. Kommissionen offentliggør en liste over de meddelte tilsynsorganer.

3. De tilsynsorganer, der er udpeget i medfør af stk. 1, har følgende rolle:

a) at føre tilsyn med kvalificerede tillidstjenesteudbydere, der er hjemmehørende på den udpegende medlemsstats område, og at sikre ved hjælp af forudgående og efterfølgende tilsynsvirksomhed, at disse kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, de udbyder, opfylder kravene i denne forordning

b) om nødvendigt at gribe ind over for ikkekvalificerede tillidstjenesteudbydere, der er hjemmehørende på den udpegende medlemsstats område ved hjælp af efterfølgende tilsynsvirksomhed, når det underrettes om, at disse ikkekvalificerede tillidstjenesteudbydere eller de tillidstjenester, de udbyder, angiveligt ikke opfylder kravene i denne forordning.

4. Det tilsynsorgan, der er udpeget i medfør af stk. 1, har navnlig følgende opgaver:

a) at underrette de relevante kompetente myndigheder, der er udpeget eller oprettet i henhold til artikel 8, stk. 1, i direktiv (EU) 2022/2555 i de berørte medlemsstater, om væsentlige sikkerhedsbrud eller tab af integritet, som det får kendskab til i forbindelse med udførelsen af sine opgaver, og i tilfælde af væsentlige sikkerhedsbrud eller tab af integritet, som vedrører andre medlemsstater, at underrette det centrale kontaktpunkt, der er udpeget eller oprettet i henhold til artikel 8, stk. 3, i direktiv (EU) 2022/2555, i den berørte medlemsstat og de centrale kontaktpunkter, der er udpeget i henhold til denne forordnings artikel 46c, stk. 1, i de øvrige berørte medlemsstater, og at informere offentligheden eller pålægge tillidstjenesteudbyderen at gøre det, hvis tilsynsorganet fastslår, at det er i offentlighedens interesse, at sikkerhedsbruddet eller tabet af integritet offentliggøres

b) at samarbejde med andre tilsynsorganer og yde dem bistand i overensstemmelse med artikel 46c og 46e

c) at analysere de overensstemmelsesvurderingsrapporter, der er omhandlet i artikel 20, stk. 1, og artikel 21, stk. 1

d) at aflægge rapport til Kommissionen om sin primære virksomhed i overensstemmelse med denne artikels stk. 6

e) at foretage kontrolundersøgelser eller anmode et overensstemmelsesvurderingsorgan om at udføre en overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere i overensstemmelse med artikel 20, stk. 2

f) at samarbejde med de kompetente tilsynsmyndigheder, der er oprettet i henhold til artikel 51 i forordning (EU) 2016/679, navnlig ved uden unødigt ophold at underrette dem, hvor der er mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger, og om sikkerhedsbrud, der synes at udgøre brud på persondatasikkerheden

g) at tildele kvalificerede tillidstjenesteudbydere og de tjenester, de udbyder, status som kvalificeret og at trække denne status tilbage i overensstemmelse med artikel 20 og 21

h) at underrette det organ, der er ansvarligt for den nationale positivliste, der er omhandlet i artikel 22, stk. 3, om sine afgørelser om tildeling eller tilbagetrækning af status som kvalificeret, medmindre dette organ også er det tilsynsorgan, der er udpeget i medfør af nærværende artikels stk. 1

i) at kontrollere, at der findes bestemmelser om planer for virksomhedsafbrydelse, og at de anvendes korrekt, i tilfælde hvor den kvalificerede tillidstjenesteudbyder afbryder sin virksomhed, herunder hvordan oplysninger forbliver tilgængelige i overensstemmelse med artikel 24, stk. 2, litra h)

j) at pålægge tillidstjenesteudbydere at afhjælpe mangler i opfyldelsen af de krav, der er fastsat i denne forordning

k) at undersøge påstande fremsat af webbrowserudbydere i henhold til artikel 45a og om nødvendigt at gribe ind.

5. Medlemsstaterne kan kræve, at det tilsynsorgan, der er udpeget i medfør af stk. 1, opretter, vedligeholder og ajourfører en tillidsinfrastruktur i overensstemmelse med national ret.

6. Senest den 31. marts hvert år forelægger hvert tilsynsorganer, der er udpeget i medfør af stk. 1, Kommissionen en rapport om det foregående kalenderårs primære tilsynsvirksomhed. Kommissionen stiller disse årlige rapporter til rådighed for Europa-Parlamentet og Rådet.

7. Senest den 21. maj 2025 vedtager Kommissionen retningslinjer for de i medfør af denne artikels stk. 1 udpegede tilsynsorganers udførelse af de i denne artikels stk. 4 omhandlede opgaver, og fastsætter ved hjælp af gennemførelsesretsakter formater og procedurer for den i denne artikels stk. 6 omhandlede rapport. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

Artikel 46c

Centrale kontaktpunkter

1. Hver medlemsstat udpeger et centralt kontaktpunkt for tillidstjenester, europæiske digitale identitetstegnebøger og anmeldte elektroniske identifikationsordninger.

2. Hvert centralt kontaktpunkt udøver en forbindelsesfunktion for at lette det grænseoverskridende samarbejde mellem tilsynsorganerne for tillidstjenesteudbydere og mellem tilsynsorganerne for udbydere af europæiske digitale identitetstegnebøger og, hvor det er relevant, med Kommissionen og Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og med andre kompetente myndigheder i sin medlemsstat.

3. Hver medlemsstat offentliggør og meddeler uden unødig forsinkelse Kommissionen navn og adresse på det centrale kontaktpunkt, der er udpeget i medfør af stk. 1, og enhver efterfølgende ændring heraf.

4. Kommissionen offentliggør en liste over de centrale kontaktpunkter, der er meddelt i henhold til stk. 3.

Artikel 46d

Gensidig bistand

1. For at lette tilsynet med og håndhævelsen af forpligtelserne i henhold til denne forordning kan de tilsynsorganer, der er udpeget i medfør af artikel 46a, stk. 1, og artikel 46b, stk. 1, herunder gennem den samarbejdsgruppe, der er nedsat i medfør af artikel 46e, stk. 1, søge gensidig bistand fra tilsynsorganerne i en anden medlemsstat, hvor udbyderen af den europæiske digitale identitetstegnebog eller tillidstjenesteudbyderen er etableret, eller hvor dennes net- og informationssystemer befinder sig, eller dens tjenester leveres.

2. Den gensidige bistand skal som minimum indebære, at:

a) det tilsynsorgan, der anvender tilsyns- og håndhævelsesforanstaltninger i én medlemsstat, underretter og hører tilsynsorganet i den anden berørte medlemsstat

b) et tilsynsorgan kan anmode tilsynsorganet i en anden berørt medlemsstat om at træffe tilsyns- eller håndhævelsesforanstaltninger, herunder f.eks. anmodninger om at udføre inspektioner i forbindelse med de overensstemmelsesvurderingsrapporter, der er omhandlet i artikel 20 og 21 vedrørende levering af tillidstjenester

c) tilsynsorganerne, når det er hensigtsmæssigt, kan gennemføre undersøgelser i fællesskab med andre medlemsstaters tilsynsorganer.

Reglerne for og fremgangsmåden ved fælles tiltag i henhold til første afsnit undersøgelser aftales og fastlægges af de berørte medlemsstater i overensstemmelse med deres nationale ret.

3. Et tilsynsorgan, der modtager en anmodning om bistand, kan afvise denne anmodning med en af følgende begrundelser:

a) den bistand, der anmodes om, står ikke i rimeligt forhold til tilsynsorganets tilsynsopgaver, der udføres i overensstemmelse med artikel 46a og 46b

b) tilsynsorganet er ikke kompetent til at yde den bistand, der anmodes om

c) det ville være uforeneligt med denne forordning at yde den bistand, der anmodes om.

4. Senest den 21. maj 2025 og derefter hvert andet år udsteder den samarbejdsgruppe, der er nedsat i medfør af artikel 46e, stk. 1, retningslinjer for de organisatoriske aspekter og procedurer for den gensidige bistand, der er omhandlet i nærværende artikels stk. 1 og 2.

Artikel 46e

Den europæiske samarbejdsgruppe for digital identitet

1. For at støtte og lette medlemsstaternes grænseoverskridende samarbejde og udveksling af oplysninger om tillidstjenester, europæiske digitale identitetstegnebøger og anmeldte elektroniske identifikationsordninger nedsætter Kommissionen en europæisk samarbejdsgruppe for digital identitet (»samarbejdsgruppen«).

2. Samarbejdsgruppen består af repræsentanter udpeget af medlemsstaterne og Kommissionen. Samarbejdsgruppen ledes af Kommissionen. Kommissionen som varetager sekretariatsfunktionen for samarbejdsgruppen.

3. Repræsentanter for relevante interessenter kan på ad hoc-basis inviteres til at deltage i samarbejdsgruppens møder og til at deltage i dens arbejde som observatører.

4. ENISA opfordres til at deltage som observatør i samarbejdsgruppens arbejde, når den udveksler synspunkter, bedste praksis og oplysninger om relevante cybersikkerhedsaspekter såsom underretning om sikkerhedsbrud, og når anvendelsen af cybersikkerhedsattester eller -standarder drøftes.

5. Samarbejdsgruppen har følgende opgaver:

a) at udveksle rådgivning og samarbejde med Kommissionen om nye politiske initiativer inden for digitale identitetstegnebøger, elektroniske identifikationsmidler og tillidstjenester

b) i det omfang det er relevant, at rådgive Kommissionen tidligt i forberedelsen af udkast til gennemførelsesretsakter og delegerede retsakter, der skal vedtages i henhold til denne forordning

c) for at støtte tilsynsorganerne i gennemførelsen af bestemmelserne i denne forordning:

   i) at udveksle bedste praksis og oplysninger om gennemførelsen af bestemmelserne i denne forordning

   ii) at vurdere den relevante udvikling inden for europæisk digital identitetstegnebog, elektronisk identifikation og tillidstjenester

   iii) at tilrettelægge fælles møder med relevante interessenter fra hele Unionen for at drøfte aktiviteter, der gennemføres af samarbejdsgruppen, og indsamle input om nye politiske udfordringer

   iv) med støtte fra ENISA at udveksle synspunkter, bedste praksis og oplysninger om relevante cybersikkerheds-aspekter vedrørende europæiske digitale identitetstegnebøger, elektroniske identifikationsordninger og tillidstjenester

   v) at udveksle bedste praksis vedrørende udvikling og gennemførelse af politikker for anmeldelsen af sikkerhedsbrud og fælles foranstaltninger som omhandlet i artikel 5e og 10

   vi) at tilrettelægge fælles møder med NIS-samarbejdsgruppen, der er nedsat i medfør af artikel 14, stk. 1, i direktiv (EU) 2022/2555, for at udveksle relevante oplysninger vedrørende tillidstjenester og elektronisk identifikation og dertil relaterede cybertrusler, hændelser, sårbarheder, bevidstgørelsesinitiativer, uddannelse, øvelser og færdigheder, kapacitetsopbygning, kapaciteter med hensyn til standarder og tekniske specifikationer samt standarder og tekniske specifikationer

   vii) efter anmodning fra et tilsynsorgan at drøfte specifikke anmodninger om gensidig bistand som omhandlet i artikel 46d

   viii) at lette udvekslingen af oplysninger mellem tilsynsorganerne ved at give vejledning om de organisatoriske aspekter og procedurer for den gensidige bistand, der er omhandlet i artikel 46d

d) at tilrettelægge peerevalueringer af elektroniske identifikationsordninger, der skal anmeldes i henhold til denne forordning.

6. Medlemsstaterne sikrer et effektivt og virkningsfuldt samarbejde mellem deres udpegede repræsentanter i samarbejdsgruppen.

7. Senest den 21. maj 2025 fastsætter Kommissionen ved hjælp af gennemførelsesretsakter de fornødne proceduremæssige ordninger for at lette samarbejdet mellem medlemsstaterne, der er omhandlet i denne artikels stk. 5, litra d). Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.«

48) I artikel 47 foretages følgende ændringer:

a) Stk. 2 og 3 affattes således:

»2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 5c, stk. 7, artikel 24, stk. 4b, og artikel 30, stk. 4, tillægges Kommissionen for en ubegrænset periode fra den 17. september 2014.

3. Den i artikel 5c, stk. 7, artikel 24, stk. 4b, og artikel 30, stk. 4, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Afgørelsen får virkning fra dagen efter offentliggørelsen i *Den Europæiske Unions Tidende* eller fra en senere dato, der fastsættes nærmere i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.«

b) Stk. 5 affattes således:

»5. En delegeret retsakt vedtaget i henhold til artikel 5c, stk. 7, artikel 24, stk. 4b, og artikel 30, stk. 4, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret Kommissionen om, at de ikke agter at gøre indsigelse. Denne frist forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.«

49) I kapitel VI indsættes følgende artikel:

»*Artikel 48a*

Rapporteringskrav

1. Medlemsstaterne sikrer indsamling af statistikker vedrørende funktionen af europæiske digitale identitetstegnebøger og kvalificerede tillidstjenester, der leveres på deres område.

2. De statistikker, der indsamles i overensstemmelse med stk. 1, omfatter følgende:

a) antallet af fysiske og juridiske personer, der har en gyldig europæisk digital identitetstegnebog

b) typen og antallet af tjenester, der accepterer anvendelse af den europæiske digitale identitetstegnebog

c) antallet af klager fra brugere og antallet af hændelser vedrørende forbrugerbeskyttelse eller databeskyttelse for så vidt angår modtagerparter og kvalificerede tillidstjenester

d) en sammenfattende rapport, herunder data om hændelser, som forhindrer anvendelse af den europæiske digitale identitetstegnebog

e) en sammenfatning af væsentlige sikkerhedshændelser, brud på datasikkerheden og berørte brugere af europæiske digitale identitetstegnebøger eller kvalificerede tillidstjenester.

3. De i stk. 2 omhandlede statistikker stilles til rådighed for offentligheden i et åbent og almindeligt anvendt maskinlæsbart format.

4. Senest den 31. marts hvert år forelægger medlemsstaterne Kommissionen en rapport om de statistikker, der er indsamlet i overensstemmelse med stk. 2.«

50) Artikel 49 affattes således:

»*Artikel 49*

Revision

1. Kommissionen reviderer anvendelsen af denne forordning og forelægger senest den 21. maj 2026 en rapport for Europa-Parlamentet og Rådet. I denne rapport evaluerer Kommissionen navnlig, hvorvidt det er hensigtsmæssigt at ændre denne forordnings anvendelsesområde eller de specifikke bestemmelser heri, herunder navnlig artikel 5c, stk. 5, under hensyntagen til de erfaringer, der er gjort med anvendelsen af denne forordning, og til den teknologiske, markedsmæssige og retlige udvikling. Denne rapport ledsages, hvor det er nødvendigt, af et forslag til ændring af denne forordning.

2. Den i stk. 1 omhandlede rapport skal indeholde en vurdering af tilgængeligheden, sikkerheden og anvendeligheden af anmeldte elektroniske identifikationsmidler og europæiske digitale identitetstegnebøger, der er omfattet af denne forordnings anvendelsesområde, og skal vurdere, hvorvidt alle private onlinetjenesteudbydere, der benytter tredjeparters elektroniske identifikationstjenester til autentifikation af brugere, skal være forpligtede til at acceptere anvendelsen af anmeldte elektroniske identifikationsmidler og europæiske digitale identitetstegnebøger.

3. Senest den 21. maj 2030 og hver hvert fjerde år derefter forelægger Kommissionen en rapport for Europa-Parlamentet og Rådet en rapport om de fremskridt, der er gjort hen imod opfyldelse af målene for denne forordning.«

51) Artikel 51 affattes således:

»*Artikel 51*

Overgangsforanstaltninger

1. Sikre signaturgenereringssystemer, for hvilke det i overensstemmelse med artikel 3, stk. 4, i direktiv 1999/93/EF er afgjort, at de opfylder kravene, betragtes fortsat som værende kvalificerede elektroniske signaturgenereringssystemer i henhold til denne forordning indtil den 21. maj 2027.

2. Kvalificerede certifikater, der er udstedt til fysiske personer i henhold til direktiv 1999/93/EF, betragtes fortsat som værende kvalificerede certifikater for elektroniske signaturer i henhold til denne forordning indtil den 21. maj 2026.

3. Den forvaltning af kvalificerede elektroniske signatur- og seglgenereringssystemer på afstand, der foretages af andre kvalificerede tillidstjenesteudbydere end kvalificerede tillidstjenesteudbydere, der leverer kvalificerede tillidstjenester til forvaltning af kvalificerede elektroniske signatur- og seglgenereringssystemser på afstand i overensstemmelse med artikel 29a og 39a, kan udføres, uden at det er nødvendigt at opnå status som kvalificeret med hensyn til levering af disse forvaltningstjenester indtil den 21. maj 2026.

4. Kvalificerede tillidstjenesteudbydere, der har fået deres status som kvalificeret i henhold til denne forordning inden den 20. maj 2024, skal hurtigst muligt og under alle omstændigheder senest den 21. maj 2026 forelægge tilsynsorganet en overensstemmelsesvurderingsrapport, der dokumenterer overholdelsen af artikel 24, stk. 1, 1a og 1b.«

52) Bilag I-IV ændres i overensstemmelse med bilag I-IV til denne forordning.

53) Der tilføjes nye bilag V, VI og VII som angivet i bilag V, VI og VII til denne forordning.

Artikel 2

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 11. april 2024.

På Europa-Parlamentets vegne	*På Rådets vegne*
R. METSOLA	H. LAHBIB
Formand	*Formand*

BILAG I

Punkt i) i bilag I til forordning (EU) nr. 910/2014 affattes således:

»i) oplysninger om det kvalificerede certifikats gyldighedsstatus eller om, hvor de tjenester, hvortil der kan rettes forespørgsel herom, befinder sig«.

BILAG II

Punkt 3 og 4 i bilag II til forordning (EU) nr. 910/2014 udgår.

BILAG III

Punkt i) i bilag III til forordning (EU) nr. 910/2014 affattes således:

»i) oplysninger om det kvalificerede certifikats gyldighedsstatus eller om, hvor de tjenester, hvortil der kan rettes forespørgsel herom, befinder sig«.

BILAG IV

Bilag IV til forordning (EU) nr. 910/2014 ændres således:

1) Litra c) affattes således:

»c) for fysiske personer: som minimum navnet på den person, som certifikatet er udstedt til, eller et pseudonym; hvis der anvendes et pseudonym, en tydelig angivelse heraf

ca) for juridiske personer: et unikt sæt data, der entydigt repræsenterer den juridiske person, som certifikatet er udstedt til, med som minimum navnet på den juridiske person, som certifikatet er udstedt til, og, når det er relevant, registreringsnummer, som det fremgår af de officielle registre«.

2) Litra j) affattes således:

»j) oplysninger om det kvalificerede certifikats gyldighedsstatus eller om, hvor de certifikatgyldighedstjenester, hvortil der kan rettes forespørgsel herom, befinder sig.«

BILAG V

»BILAG V

KRAV TIL KVALIFICERET ATTESTERING AF ATTRIBUTTER

Kvalificeret elektronisk attestering af attributter indeholder:

a) en angivelse — som minimum i en form, der egner sig til automatiseret behandling — af, at attesteringen er udstedt som en kvalificeret elektronisk attestering af attributter

b) et sæt data, der entydigt repræsenterer den kvalificerede tillidstjenesteudbyder, der udsteder den kvalificerede elektroniske attestering af attributter, herunder som minimum oplysninger om, hvilken medlemsstat den pågældende udbyder er hjemmehørende i, og

   i) for en juridisk person: navn og, når det er relevant, registreringsnummer, som det fremgår af de officielle registre

   ii) for en fysisk person: personens navn

c) et sæt data, der entydigt repræsenterer den enhed, som de attesterede attributter henviser til; hvis der anvendes et pseudonym, en tydelig angivelse heraf

d) den attesterede attribut eller de attesterede attributter, herunder, hvis det er relevant, de oplysninger, der er nødvendige for at bestemme attributternes omfang

e) oplysninger om attesteringens ikrafttrædelses- og udløbsdato

f) attesteringens identifikationskode, som skal være entydig for den kvalificerede tillidstjenesteudbyder, og, hvis det er relevant, attesteringsordningen, som attesteringen af attributter er en del af

g) den udstedende kvalificerede tillidstjenesteudbyders kvalificerede elektroniske signatur eller kvalificerede elektroniske segl

h) oplysninger om, hvor certifikatet for den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl, der henvises til i litra g), er gratis tilgængeligt

i) oplysninger om den kvalificerede attesterings gyldighedsstatus eller om, hvor de tjenester, hvortil der kan rettes forespørgsel herom, befinder sig.«

BILAG VI

»BILAG VI

MINIMUMSLISTE OVER ATTRIBUTTER

I medfør af artikel 45e sikrer medlemsstaterne, at der træffes foranstaltninger til at gøre det muligt for kvalificerede tillidstjenesteudbydere af elektroniske attesteringer af attributter ved hjælp af elektroniske midler efter anmodning fra brugeren at kontrollere autenticiteten af følgende attributter i forhold til de relevante autentiske kilder på nationalt plan eller via udpegede mellemmænd, der er anerkendte på nationalt plan, i overensstemmelse med EU-retten eller national ret og hvor disse attributter er afhængige af autentiske kilder i den offentlige sektor:

1. adresse
2. alder
3. køn
4. civilstand
5. familiesammensætning
6. nationalitet eller statsborgerskab
7. uddannelsesmæssige kvalifikationer, titler og licenser
8. erhvervsmæssige kvalifikationer, titler og licenser
9. beføjelser og mandater til at repræsentere fysiske eller juridiske personer
10. offentlige tilladelser og licenser
11. for juridiske personer, finansielle data og virksomhedsoplysninger.«

BILAG VII

»BILAG VII

KRAV TIL ELEKTRONISK ATTESTERING AF ATTRIBUTTER, DER ER UDSTEDT AF ELLER PÅ VEGNE AF EN OFFENTLIG MYNDIGHED MED ANSVAR FOR EN AUTENTISK KILDE

En elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, skal indeholde:

a) en angivelse — som minimum i en form, der egner sig til automatiseret behandling — af, at attesteringen er udstedt som en elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde

b) et sæt data, der entydigt repræsenterer den offentlige myndighed, der udsteder den elektroniske attestering af attributter, herunder som minimum oplysninger om, hvilken medlemsstat den pågældende offentlige myndighed er hjemmehørende i, og dens navn og, hvis det er relevant, registreringsnummer, som det fremgår af de officielle registre

c) et sæt data, der entydigt repræsenterer den enhed, som de attesterede attributter henviser til; hvis der anvendes et pseudonym, en tydelig angivelse heraf

d) den attesterede attribut eller de attesterede attributter, herunder, hvis det er relevant, de oplysninger, der er nødvendige for at bestemme attributternes omfang

e) oplysninger om attesteringens ikrafttrædelses- og udløbsdato

f) attesteringens identifikationskode, som skal være entydig for den udstedende offentlige myndighed, og, hvis det er relevant, en angivelse af den attesteringsordning, som attesteringen af attributter er en del af

g) den udstedende myndigheds kvalificerede elektroniske signatur eller kvalificerede elektroniske segl

h) oplysninger om, hvor certifikatet for den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl, der henvises til i litra g), er gratis tilgængeligt

i) oplysninger om attesteringens gyldighedsstatus eller om, hvor de tjenester, hvortil der kan rettes forespørgsel herom, befinder sig.«