



Bruxelles, den 25. november 2022  
(OR. en)

14959/22

LIMITE

TELECOM 473  
COMPET 919  
MI 844  
DATAPROTECT 321  
JAI 1497  
CODEC 1774

---

---

Interinstitutionel sag:  
2021/0136(COD)

---

---

#### NOTE

fra:	De Faste Repræsentanters Komité (1. afdeling)
til:	Rådet
Tidl. dok. nr.:	14344/22
Komm. dok. nr.:	9471/21
Vedr.:	Forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af en ramme for en europæisk digital identitet – Generel indstilling

#### I. INDLEDNING

1. Kommissionen vedtog forslaget til forordning om en europæisk digital identitet (**europæisk eID**) den 3. juni 2021<sup>1</sup>. Initiativet ændrer eIDAS-forordningen fra 2014<sup>2</sup>, som havde skabt det nødvendige grundlag for sikker adgang til tjenester og gennemførelse af transaktioner online og på tværs af grænserne i EU.

---

<sup>1</sup> Dok. 9471/21.

<sup>2</sup> [Forordning \(EU\) nr. 910/2014](#).

2. Forslaget, der er baseret på artikel 114 i TEUF, kræver, at medlemsstaterne udsteder en europæisk digital ID-tegnebog inden for rammerne af en anmeldt elektronisk identifikationsordning på grundlag af fælles tekniske standarder og efter en obligatorisk certificering. For at etablere den nødvendige tekniske arkitektur, fremskynde gennemførelsen af den reviderede forordning, udstikke retningslinjer til medlemsstaterne og undgå fragmentering er forslaget ledsaget af en henstilling om udvikling af en EU-værktøjskasse.
3. Den foreslåede forordning har til formål at sikre alle personer og virksomheder universel adgang til sikker og pålidelig elektronisk identifikation og autentifikation ved hjælp af en personlig digital tegnebog på mobiltelefonen.

## **II. ARBEJDET I DE ANDRE INSTITUTIONER**

1. I Europa-Parlamentet blev forslaget henvist til Udvalget om Industri, Forskning og Energi (ITRE) med tre associerede rådgivende udvalg, nemlig Udvalget om det Indre Marked og Forbrugerbeskyttelse (IMCO), Retsudvalget (JURI) og Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender (LIBE). Romana Jerković (S&D, Kroatien) er ordfører for sagen. ITRE-udvalget har endnu ikke vedtaget sin betænkning.
2. Det Europæiske Økonomiske og Sociale Udvalg blev den 15. juli 2021 anmodet om at afgive udtalelse om forslaget, som således blev afgivet den 20. oktober 2021. Det Europæiske Regionsudvalg afgav på eget initiativ udtalelse om forslaget den 12. oktober 2021.
3. Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) offentliggjorde formelle bemærkninger til forslaget den 28. juli 2021.

### III. STATUS OVER RÅDETS ARBEJDE

1. I Rådet er forslaget blevet behandlet i Gruppen vedrørende Telekommunikation og Informationssamfundet (i det følgende benævnt "Telekommunikationsgruppen"), som indledte drøftelserne under det portugisiske formandskab i juni 2021. Analysen af forslaget fortsatte i Telekommunikationsgruppen under det slovenske formandskab, og førstebehandlingen blev afsluttet med positivt resultat den 15. november 2021.
2. Det franske formandskab forelagde sit **første kompromisforslag** den 15. februar og den 5. april, og det **andet kompromisforslag** blev drøftet den 23. maj og den 9. juni. I forbindelse med en orienterende debat i Telekommunikationsgruppen den 19. juli 2022 fremhævede det tjekkiske formandskab – på grundlag af det franske formandskabs arbejde – vigtige udestående spørgsmål på højt plan og anmodede delegationerne om at give udtryk for deres foretrukne løsningsmodeller med henblik på at omformulere de relevante dele af det andet kompromisforslag i overensstemmelse hermed. Den reviderede udgave resulterede i et **tredje kompromisforslag**, som det tjekkiske formandskab forelagde på mødet i Telekommunikationsgruppen den 5. og 8. september. Takket være yderligere debatter og dermed forbundne tilpasninger lykkedes det at skabe en større grad af konvergens med hensyn til de fleste af de udestående spørgsmål.
3. Det **fjerde kompromisforslag**, som delegationerne fik forelagt på mødet i Telekommunikationsgruppen den 28. september, afslørede dog vedvarende meningsforskelle mellem medlemsstaterne vedrørende navnlig ét spørgsmål på højt plan, nemlig det valgte sikringsniveau for den europæiske digitale ID-tegnebog. Nogle af de medlemsstater, der allerede har et nationalt eID-system, indførte oprindeligt og investerede efterfølgende i sikringsniveauet "betydelig", mens der i det nuværende eID-forslag kræves sikringsniveauet "høj". Da det tjekkiske formandskab er opmærksom på, at der i nogle medlemsstater er udstedt et stort antal elektroniske identifikationsmidler med sikringsniveauet "betydelig", har det i forlængelse heraf foreslået en mekanisme, der skal lette onboarding af brugere og dermed bidrage til udbredelsen af europæiske digitale ID-tegnebøger. Bestemmelsen giver brugerne mulighed for at tilmelde sig den europæiske digitale ID-tegnebog ved hjælp af eksisterende nationale eID-midler med sikringsniveauet "betydelig" sammen med yderligere onboardingprocedurer på afstand, der tilsammen opfylder kravene til sikringsniveauet "høj". De tekniske og operationelle specifikationer er underlagt gennemførelseslovgivning, og overensstemmelsen med kravene skal certificeres.

4. Det **femte kompromisforslag** blev drøftet på mødet i Telekommunikationsgruppen den 25. oktober. På mødet i Telekommunikationsgruppen den 8. november 2022 forelagde det tjekkiske formandskab de begrænsede ændringer, der er foretaget, og udarbejdede i forlængelse af de supplerende bemærkninger og forslag til affattelse fra delegationerne den **endelige udgave af kompromisteksten** med henblik på forelæggelse for Coreper.
5. Den 18. november gennemgik Coreper dette kompromisforslag og **besluttede enstemmigt at forelægge det for TTE-Rådet (telekommunikation) uden ændringer med henblik på en generel indstilling** på samlingen den 6. december 2022.

#### IV. VIGTIGSTE ELEMENTER I KOMPROMISFORSLAGET

##### 1. Den europæiske digitale ID-tegnebog

Et af de vigtigste politiske mål med Kommissionens forslag til en europæisk digital ID-tegnebog ("tegnebog") er at give borgere og andre indbyggere som defineret i national ret et harmoniseret europæisk digitalt ID-middel baseret på konceptet en europæisk digital ID-tegnebog. Som et elektronisk identifikationsmiddel ("eID-middel") udstedt i henhold til nationale ordninger på sikringsniveauet "høj" bliver tegnebogen i sig selv et eID-middel baseret på medlemsstaternes udstedelse af personidentifikationsdata og tegnebogen.

##### 2. Europæiske digitale ID-tegnebøgers sikringsniveau

Sikringsniveauer bør afspejle graden af tillid til, at et elektronisk identifikationsmiddel kan fastslå identiteten på en person og således give sikkerhed for, at den person, der gør krav på en specifik identitet, faktisk er den person, hvortil identiteten er blevet knyttet. På grundlag af den brede støtte på gruppens møder og under Corepers drøftelser den 14. oktober skal tegnebogen udstedes inden for rammerne af et elektronisk identifikationssystem, der opfylder sikringsniveauet "høj". Desuden er der i **artikel 6a** blevet tilføjet en særlig bestemmelse om onboarding af brugere. Formålet med denne ændring er at imødekomme bekymringerne i de medlemsstater, hvor der allerede er udstedt et stort antal nationale eID-midler med sikringsniveauet "betydelig". Bestemmelsen gør det muligt for en bruger at anvende sine nationale eID-midler sammen med yderligere onboardingprocedurer på afstand for at gøre det

muligt at godtgøre identiteten på sikringsniveau "høj" og i sidste ende at få en tegnebog. Eftersom udkastet til eID-forordningen bygger på cybersikkerhedscertificeringsordninger, der bør skabe en harmoniseret grad af tillid til europæiske digitale ID-tegnebøgers sikkerhed, forventes sikker lagring af kryptografisk materiale også at blive genstand for cybersikkerhedscertificering. Formandskabet har derfor foreslået en ny **betragtning 10b**, der omhandler disse tekniske forudsætninger for at opnå sikringsniveauet "høj" og giver mulighed for en opfølgingsproces i forbindelse med gennemførelsen af europæiske digitale ID-tegnebøger.

### 3. Modtagerparters anmeldelse

3.1 **Artikel 6b** om modtagerparters anmeldelse er blevet omformuleret. Som hovedregel bør den anmeldelsesprocedure, hvorved modtagerparten meddeler sin hensigt om at benytte tegnebogen, være omkostningseffektiv, stå i et rimeligt forhold til risikoen og sikre, at modtagerparten som minimum giver de oplysninger, der er nødvendige for autentifikation, til tegnebogen. Som standard kræves der kun et minimum af oplysninger, og anmeldelsen bør gøre det muligt at anvende automatiserede eller enkle selvrporteringsprocedurer.

3.2 En særlig ordning kan imidlertid være nødvendigt på grund af sektorspecifikke krav såsom dem, der gælder for behandling af særlige kategorier af personoplysninger. Der er derfor indført en bestemmelse herom, der har til formål at dække tilfælde, hvor der kræves en strengere registrerings- eller autentifikationsprocedure. Hvis der i EU-retten eller national ret derimod ikke er fastsat specifikke krav med henblik på at få adgang til de oplysninger, der gives via tegnebogen, kan medlemsstaterne fritage sådanne modtagerparter fra forpligtelsen til at meddele, at de har til hensigt at benytte tegnebøger.

### 4. Certificering

4.1 Forordningen bør udnytte, basere sig på og give mulighed for at anvende relevante og eksisterende certificeringsordninger, der er omfattet af forordningen om cybersikkerhed, eller dele af sådanne ordninger til at certificere, at tegnebøger eller dele heraf opfylder de gældende cybersikkerhedskrav. Forordningen om cybersikkerhed finder således fuldt ud anvendelse, herunder peerreviewsystemet mellem nationale cybersikkerhedscertificeringsmyndigheder som omhandlet i forordningen om cybersikkerhed. For i videst muligt omfang at tilpasse eID-forordningen til forordningen om cybersikkerhed skal medlemsstaterne udpege offentlige og private organer, der er akkrediteret til at certificere tegnebogen, som fastsat i forordningen om cybersikkerhed.

4.2 Desuden opfordres Kommissionen til at give ENISA beføjelse til at udarbejde og vedtage en særlig ordning i henhold til forordningen om cybersikkerhed med henblik på cybersikkerhedscertificering af tegnebogen. Indtil der er udarbejdet en sådan ordning, vil den europæiske cybersikkerhedscertificeringsordning, der er baseret på de fælles kriterier og er offentliggjort i henhold til forordningen om cybersikkerhed, blive anvendt som referencemetode til certificering af tegnebøger. For krav, der ikke vedrører cybersikkerhed, navnlig krav, der dækker andre funktionelle og operationelle aspekter af tegnebogen, skal der udarbejdes en liste over specifikationer, procedurer og referencestandarder. Disse krav skal certificeres.

## 5. Gennemførelsesperiode for leveringen af tegnebogen

Det er på grundlag af vejledning fra medlemsstaterne blevet foreslået, at gennemførelsesperioden på 24 måneder regnes fra vedtagelsen af de gennemførelsesretsakter, der er omhandlet i **artikel 6a, stk. 11**, og **artikel 6c, stk. 4**.

## 6. Gebyrer

Det er blevet præciseret i **artikel 6a, stk. 6a**, og den tilsvarende betragtning, at udstedelse, anvendelse til autentifikation og tilbagekaldelse af tegnebøger bør være gratis for fysiske personer. Bortset fra når tegnebøger anvendes til autentifikation, kan tjenester, der er baseret på brugen af tegnebogen, medføre omkostninger, f.eks. udstedelse af elektroniske attesteringer af attributter til tegnebogen.

## 7. Adgang til hardware- og softwarefunktioner, herunder det sikre element

Formandskabet har foreslået, at der udtrykkeligt henvises til forordning (EU) 2022/1925, som sikrer adgang til hardware- og softwarefunktioner som en del af centrale platformstjenester, der leveres af gatekeepere. I **artikel 12b**, som for nylig blev tilføjet, præciseres det, at udbydere af tegnebøger og udstedere af anmeldte elektroniske identifikationsmidler, der handler i kommerciel eller professionel egenskab, er erhvervsbrugere af gatekeepere, jf. den respektive definition i forordningen om digitale markeder. Betragtningens ordlyd er blevet udvidet for at skitsere betydningen af koblingen til forordningen om digitale markeder, nemlig at det bør påhvile gatekeepere gratis at sikre effektiv interoperabilitet med og adgang med henblik på interoperabilitet til det samme styresystem, den samme hardware eller de samme softwarefunktioner, der er tilgængelige eller anvendes i forbindelse med, at de udbyder deres egne supplerende og understøttende tjenester.

## 8. Alternative muligheder for offentlige organer til at udstede elektroniske attesteringer af attributter

Det er blevet fastholdt, at kvalificerede elektroniske attesteringer af attributter skal udstedes af kvalificerede udbydere, herunder at medlemsstaterne har pligt til at sikre, at attributter kan kontrolleres mod en autentisk kilde i den offentlige sektor. Derudover er der indført en mulighed for, at elektronisk attestering af attributter med samme retsvirkning som kvalificeret elektronisk attestering af attributter kan udstedes til tegnebogen direkte af den offentlige myndighed, der er ansvarlig for den autentiske kilde, eller af en udpeget offentlig myndighed på vegne af en offentlig myndighed, der er ansvarlig for en autentisk kilde, forudsat at de nødvendige krav er opfyldt. Forslaget er afspejlet i den nye **artikel 45a** og **45da** samt i **bilag VII**.

## 9. Matchning af registreringer

Den oprindelige **artikel 11a** er blevet omdøbt til matchning af registreringer, da det bedre afspejler bestemmelsens formål. På grundlag af drøftelserne er begrebet entydig og vedvarende identifikator blevet fastholdt for tegnebøger. Den respektive definition præciserer, at identifikatoren kan bestå af en kombination af flere nationale og sektorspecifikke identifikatorer, så længe den tjener sit formål. Det er udtrykkeligt anført, at matchning af registreringer kan lattes gennem kvalificeret elektronisk attestering af attributter. Desuden er der indarbejdet en beskyttelsesbestemmelse i **artikel 11a**, ifølge hvilken medlemsstaterne skal sikre beskyttelsen af personoplysninger og forhindre profilering af brugere. Endelig skal medlemsstaterne i deres egenskab af modtagerparter sikre matchning af registreringer.

## VI. KONKLUSION

1. På baggrund af ovenstående opfordres Rådet til:
  - at gennemgå kompromisteksten, jf. bilaget til denne note
  - at bekræfte en generel indstilling til forslaget til forordning om en europæisk digital identitet (europæisk eID) på samlingen i TTE-Rådet (telekommunikation) den 6. december 2022.

Forslag til

## EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af en ramme for en europæisk 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<sup>3</sup>,

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

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

---

<sup>3</sup> EUT C af , s. .

<sup>4</sup> COM(2020) 67 final.



- (2) I sine konklusioner af 1.-2. oktober 2020<sup>5</sup> 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 Kommissionens meddelelse af 9. marts 2021 med titlen "Det digitale kompas 2030: Europas kurs i det digitale årti"<sup>6</sup> fastsættes målet om en EU-ramme, der senest i 2030 fører til en bred indførelse af en pålidelig, brugerkontrolleret identitet, der giver hver enkelt borger kontrol over sin egen onlineinteraktion og -tilstedeværelse.
- (4) En mere harmoniseret tilgang til digital identifikation bør mindske risiciene og omkostningerne ved den nuværende fragmentering som følge af divergerende nationale løsninger og vil styrke det indre marked ved at gøre det muligt for borgere, andre indbyggere som defineret i national ret og virksomheder at identificere sig online på en hensigtsmæssig og ensartet måde i hele Unionen. Den europæiske digitale ID-tegnebog vil give fysiske og juridiske personer i hele Unionen et harmoniseret elektronisk identifikationsmiddel, der vil sætte dem i stand til at autentificere og dele data, der er knyttet til deres identitet. Alle bør kunne få sikker adgang til offentlige og private tjenester ved hjælp af et forbedret økosystem for tillidstjenester og verificerede identitetsbeviser og attesteringer af attributter, såsom et eksamensbevis, der er juridisk anerkendt og accepteret i hele Unionen. Den europæiske ramme for digital identitet har til formål at opnå et skifte fra afhængighed af udelukkende nationale digitale identitetsløsninger til leveringen af elektroniske attesteringer af attributter, der er gyldige på europæisk plan. Udbydere af elektroniske attesteringer af attributter bør drage fordel af et klart og ensartet regelsæt, og offentlige forvaltninger bør kunne have tillid til elektroniske dokumenter i et givet format.

---

<sup>5</sup> <https://www.consilium.europa.eu/da/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/>.

<sup>6</sup> COM(2021) 118 final/2.

- (4a) Flere medlemsstater har indført og anvender i vid udstrækning elektroniske identifikationsmidler, som i dag accepteres af tjenesteudbydere i Unionen. Desuden er der foretaget investeringer i både nationale og grænseoverskridende løsninger på grundlag af den nuværende eIDAS-forordning, herunder den tekniske infrastruktur for interoperabilitet mellem eIDAS-knudepunkter. For at garantere komplementaritet og sikre, at de nuværende brugere af anmeldte elektroniske identifikationsmidler hurtigt tager europæiske digitale ID-tegnebøger til sig, og for at minimere indvirkningen på eksisterende tjenesteudbydere forventes det at blive henholdsvis gavnligt og fordelagtigt, at de europæiske digitale ID-tegnebøger kan bygge videre på erfaringerne med eksisterende elektroniske identifikationsmidler og udnytte den etablerede eIDAS-infrastruktur på europæisk og nationalt plan.
- (5) For at støtte de europæiske virksomheders konkurrenceevne bør onlinetjenesteudbydere kunne benytte digitale identitetsløsninger, der er anerkendt i hele Unionen, uanset i hvilken medlemsstat de er leveret, og således drage fordel af en harmoniseret europæisk 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.
- (6) Forordning (EU) 2016/679<sup>7</sup> 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 fra andre tjenester med personoplysninger relateret til de tjenester, der er omfattet af denne forordning. Personoplysninger vedrørende levering af europæiske digitale ID-tegnebøger bør opbevares logisk adskilt fra alle andre data, der opbevares af udstederen. Denne forordning forhindrer ikke udstedere af europæiske digitale ID-tegnebøger i at anvende yderligere tekniske foranstaltninger, der bidrager til at beskytte personoplysninger, såsom fysisk adskillelse af personoplysninger vedrørende leveringen af tegnebøger fra andre oplysninger, som udstederen er i besiddelse af.

---

<sup>7</sup> 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).

- (7) Det er nødvendigt at fastsætte harmoniserede betingelser for fastlæggelse af en ramme for europæiske digitale ID-tegnebøger, der skal leveres af medlemsstaterne, og denne ramme bør sætte alle EU-borgere og andre indbyggere som defineret i national ret i stand til at dele data vedrørende deres identitet på en sikker, brugervenlig og bekvem måde under brugerens enekontrol. Teknologier, der anvendes til at nå disse mål, bør udvikles med det sigte at opnå det højeste niveau af sikkerhed, privatlivsbeskyttelse, brugervenlighed og udbredt anvendelighed. Medlemsstaterne bør sikre lige adgang til digital identifikation for alle deres statsborgere og indbyggere.
- (8) For at sikre, at modtagerparter kan forlade sig på brugen af europæiske digitale ID-tegnebøger, og for at beskytte brugeren mod ulovlig brug af følsomme oplysninger bør modtagerparter registreres som led i en anmeldelsesprocedure. De anmeldelseskrav, der gælder for modtagerparter, bør i de fleste tilfælde være baseret på levering af en begrænset mængde oplysninger, der er nødvendige for modtagerpartens autentifikation med henblik på den europæiske digitale ID-tegnebog. Kravene bør også gøre det muligt at anvende automatiserede eller enkle selvrapporteringsprocedurer, herunder medlemsstaternes baseren på og brug af eksisterende registre. Samtidig kan der for kategorier af følsomme oplysninger findes særlige ordninger på nationalt plan eller EU-plan, som kan pålægge modtagerparter strengere registrerings- og godkendelseskrav for i sådanne tilfælde at forhindre ulovlig anvendelse af identitetsdata. I andre brugstilfælde kan modtagerparter undtages fra at anmelde deres hensigt om at benytte den europæiske digitale ID-tegnebog, f.eks. når en ret til at kontrollere specifikke attributter ikke kræver eller giver mulighed for modtagerpartens autentifikation ad elektronisk vej. I disse personlige scenarier er brugeren typisk i stand til at identificere modtagerparten takket være den konkrete situation, f.eks. når brugeren taler med en biludlejningsmedarbejder eller apoteker. Det er hensigten, at anmeldelsesprocessen skal være reguleret af sektorspecifik EU-lovgivning eller national lovgivning, da dette gør det muligt at tage højde for forskellige brugstilfælde, der kan variere med hensyn til registreringskrav og betjeningsmåde (online/offline) eller med hensyn til kravet om at autentificere enheder, der kan kommunikere med den europæiske digitale ID-tegnebog. Der bør ikke stilles krav om, at kontrollen med modtagerparternes brug af den europæiske digitale ID-tegnebog skal håndhæves på samme niveau som den europæiske digitale ID-tegnebog.

- (9) Alle europæiske digitale ID-tegnebøger bør for brugerne muliggøre elektronisk identifikation og autentifikation online og offline på tværs af grænserne for at få adgang til en bred vifte af offentlige og private tjenester. ID-tegnebøger 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 statsborgere og indbyggere. Anvendelse offline vil være vigtigt 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 autentificere. Med hensyn til sikringsniveauet "høj" bør de europæiske digitale ID-tegnebøger for at opfylde sikkerhedskravene i denne forordning drage fordel af det potentiale, som manipulationssikrede løsninger såsom sikre elementer giver. De europæiske digitale ID-tegnebøger bør også give brugerne mulighed for at oprette og anvende kvalificerede elektroniske signaturer og segl, der er accepteret i hele EU. For at give personer og virksomheder i hele EU fordele med hensyn til forenkling og besparelse af omkostninger, herunder ved at give mulighed for repræsentationsbeføjelser og e-mandater, bør medlemsstaterne udstede europæiske digitale ID-tegnebøger efter fælles standarder for at sikre en gnidningsløs interoperabilitet og et højt sikkerhedsniveau. 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 de europæiske digitale ID-tegnebøger er baseret på borgernes, andre indbygges eller juridiske enheders juridiske identitet. Tilliden til de europæiske digitale ID-tegnebøger vil blive styrket af det forhold, at de udstedende parter er forpligtede til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der står i et rimeligt forhold til risiciene for fysiske personers rettigheder og frihedsrettigheder i overensstemmelse med forordning (EU) 2016/679. Det er gratis for fysiske personer at udstede europæiske digitale ID-tegnebøger, at anvende dem til autentifikation og at tilbagekalde dem. Tjenester, der er baseret på brugen af tegnebogen, kan medføre omkostninger i forbindelse med f.eks. udstedelse af elektroniske attesteringer af attributter til tegnebogen.

- (9a) Det er gavnligt at lette udbredelsen og anvendelsen af europæiske digitale ID-tegnebøger ved gnidningsløst at integrere dem i økosystemet af offentlige og private digitale tjenester, der allerede er indført på nationalt, lokalt eller regionalt plan. For at nå dette mål kan medlemsstaterne fastsætte retlige og organisatoriske foranstaltninger for at øge fleksibiliteten for udstedere af europæiske digitale ID-tegnebøger og for at give mulighed for yderligere funktionaliteter i europæiske digitale ID-tegnebøger ud over, hvad der er fastsat i denne forordning, herunder gennem øget interoperabilitet med eksisterende nationale eID-midler. Dette bør på ingen måde ske på bekostning af leveringen af europæiske digitale ID-tegnebøgers centrale funktioner som fastsat i denne forordning eller føre til, at eksisterende nationale løsninger fremmes i højere grad end europæiske digitale ID-tegnebøger. Da disse yderligere funktioner rækker ud over, hvad der er fastsat i denne forordning, nyder de ikke fordel af forordningens bestemmelser om grænseoverskridende benyttelse af europæiske digitale ID-tegnebøger.

- (10) For at opnå et højt databeskyttelses-, sikkerheds- og pålidelighedsniveau bør der ved denne forordning fastsættes en harmoniseret ramme, der præciserer de fælles specifikationer og krav, der gælder for europæiske digitale ID-tegnebøger. De europæiske digitale ID-tegnebøgers opfyldelse af disse krav bør certificeres af akkrediterede overensstemmelsesvurderingsorganer, som er udpeget af medlemsstaterne. Certificering bør navnlig være baseret på de relevante europæiske cybersikkerhedscertificeringsordninger, eller dele heraf, der er oprettet i henhold til forordning (EU) 2019/881<sup>8</sup>, for så vidt de dækker de cybersikkerhedskrav, der gælder for europæiske digitale ID-tegnebøger. Der bør ved hjælp af europæiske cybersikkerhedscertificeringsordninger skabes en harmoniseret grad af tillid til europæiske digitale ID-tegnebøgers sikkerhed, uanset hvor i Unionen de er udstedt. Cybersikkerhedscertificeringen af europæiske digitale ID-tegnebøger bør bygge på de nationale cybersikkerhedscertificeringsmyndigheders opgave med at føre tilsyn med og overvåge, om de certifikater, der udstedes af overensstemmelsesvurderingsorganer i deres jurisdiktion, er i overensstemmelse med de relevante europæiske cybersikkerhedsordninger. Tilsvarende bør certificeringen, hvor det er relevant, udnytte de standarder og tekniske specifikationer, der er fastsat i forordning (EU) 2019/881. Sådanne specifikationer kan anvendes som statusdokumenter som angivet i de relevante cybersikkerhedscertificeringsordninger i henhold til forordning (EU) 2019/881. Hvis ingen relevant europæisk cybersikkerhedscertificeringsordning, der er oprettet i henhold til forordning (EU) 2019/881, dækker certificering af relevante tjenester eller processer, der bidrager til tegnebogens sikkerhed, bør der oprettes passende ordninger i overensstemmelse med afsnit III i forordning (EU) 2019/881. Der bør oprettes en fælles og harmoniseret ordning for certificering af europæiske digitale ID-tegnebøger med henblik på vurdering af deres overensstemmelse med de fælles specifikationer og krav, der er fastsat i nærværende forordning, bortset fra dem, der vedrører cybersikkerhed og databeskyttelse, navnlig dem, der dækker funktionelle og operationelle aspekter. Med hensyn til denne certificering bør der for at sikre en høj grad af tillid og gennemsigtighed fastsættes mekanismer og procedurer til fremme af peerlæring og samarbejde mellem medlemsstaterne om overvågning og revision af certificeringsorganerne og de certifikater og certificeringsrapporter, de udsteder. En sådan peerlæringsmekanisme bør ikke berøre forordning (EU) 2016/679 og forordning (EU) 2019/881. Certificering af tegnebogen i henhold til forordning (EU) 2016/679 er et af flere frivillige værktøjer, der kan anvendes til at påvise overholdelsen af kravene i forordning (EU) 2016/679, således som de finder anvendelse på europæiske digitale ID-tegnebøger og leveringen heraf til europæiske borgere.

---

<sup>8</sup> 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).

- (10a) Onboarding af borgere og indbyggere til den europæiske digitale ID-tegnebog bør lettes ved hjælp af elektroniske identifikationsmidler, der er udstedt på sikringsniveauet "høj". Elektroniske identifikationsmidler, der er udstedt på sikringsniveauet "betydelig", bør kun anvendes i tilfælde, hvor harmoniserede tekniske og operationelle specifikationer, der benytter elektroniske identifikationsmidler udstedt på sikringsniveauet "betydelig" i kombination med andre supplerende identitetskontrolmidler, vil gøre det muligt at opfylde kravene i nærværende forordning for så vidt angår sikringsniveauet "høj". Sådanne supplerende midler eller foranstaltninger bør være pålidelige og lette at anvende for brugerne og kan bygge på muligheden for at anvende onboardingprocedurer på afstand, kvalificerede certifikater understøttet af kvalificerede signaturer, kvalificeret elektronisk attestering af attributter eller en kombination heraf. For at sikre en tilstrækkelig udbredelse af europæiske digitale ID-tegnebøger bør der i gennemførelsesretsakter fastsættes harmoniserede tekniske og operationelle specifikationer for onboarding af brugere ved hjælp af elektroniske identifikationsmidler, herunder dem, der udstedes på sikringsniveauet "betydelig".
- (10b) Formålet med denne forordning er at forsyne brugeren med en fuldt mobil, sikker og brugervenlig europæisk digital ID-tegnebog. Som en overgangsforanstaltning, indtil certificerede manipulationssikrede løsninger er tilgængelige, f.eks. sikre elementer i brugernes enheder, kan de europæiske digitale ID-tegnebøger benytte certificerede eksterne sikre elementer til at beskytte kryptografisk materiale og andre følsomme oplysninger eller anmeldte nationale løsninger på sikringsniveauet "høj" til at påvise overholdelsen af forordningens relevante krav for så vidt angår tegnebogens sikringsniveau. Anvendelsen af ovennævnte overgangsforanstaltning bør begrænses til brugstilfælde, der kræver sikringsniveauet "høj", såsom onboarding af brugeren til tegnebogen og autentifikation til tjenester, der kræver sikringsniveauet "høj". I forbindelse med autentifikation til tjenester, der kræver sikringsniveauet "betydelig", bør europæiske digitale ID-tegnebøger ikke kræve, at ovennævnte overgangsforanstaltning anvendes. Hvis denne overgangsforanstaltning benytter et certificeret eksternt sikkert element, bør denne forordning ikke berøre nationale betingelser for udstedelse og anvendelse af sådant et element.

- (11) Europæiske digitale ID-tegnebøger bør sikre det højeste beskyttelses- og sikkerhedsniveau for de personoplysninger, der anvendes til autentifikation, uanset om disse data lagres lokalt eller i cloudbaserede løsninger, under hensyntagen til de forskellige risikoniveauer. Anvendelsen af biometriske oplysninger som en autentifikationsfaktor til stærk brugerautentifikation er en af de identifikationsmetoder, der giver en høj grad af tillid, navnlig i kombination med andre autentifikationselementer. Da biometriske oplysninger repræsenterer et entydigt kendetegn ved en person, er behandling af biometriske oplysninger kun tilladt i henhold til undtagelserne i artikel 9, stk. 2, i forordning (EU) 2016/679 og kræver passende garantier, der står i et rimeligt forhold til den risiko, som en sådan behandling kan indebære for fysiske personers rettigheder og frihedsrettigheder.
- (11a) De europæiske digitale ID-tegnebøger bør fungere på en gennemsigtig måde og give mulighed for kontrollerbar behandling af personoplysninger. For at opnå dette opfordres medlemsstaterne til at offentliggøre kildekoden til de softwarekomponenter i europæiske digitale ID-tegnebøger, der vedrører behandling af personoplysninger og oplysninger om juridiske personer. Offentliggørelse af en sådan kildekode giver samfundet, herunder brugere og udviklere, mulighed for at forstå, hvordan den fungerer. Dette vil også kunne øge brugernes tillid til økosystemet for tegnebogen og bidrage til tegnebogens sikkerhed ved at give alle mulighed for at rapportere om sårbarheder og fejl i koden. Dette tilskynder leverandørerne til at levere og opretholde et meget sikkert produkt. Derudover, og hvor det er relevant, opfordres medlemsstaterne også til at stille kildekoden til rådighed inden for rammerne af en open source-licens. En open source-licens gør det muligt for samfundet, herunder brugere og udviklere, at ændre og genbruge kildekoden.
- (12) For at sikre, at den europæiske ramme for digital identitet er åben for innovation og teknologisk udvikling og er fremtidssikret, bør medlemsstaterne tilskyndes til i fællesskab at oprette sandkasser til afprøvning af innovative løsninger i et kontrolleret og sikkert miljø, navnlig med henblik på at forbedre løsningernes funktionalitet, beskyttelse af personoplysninger, sikkerhed og interoperabilitet og bidrage til fremtidige ajourføringer af tekniske referencer og retlige krav. Et sådant miljø bør fremme inddragelsen af europæiske små og mellemstore virksomheder, startupvirksomheder og individuelle innovatorer og forskere.



- (13) Forordning (EU) 2019/1157<sup>9</sup> 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.
- (14) 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.
- (15) En strømning af de nuværende procedurer for anmeldelse og fagfællebedømmelse (peerreview) vil forhindre uensartede tilgange til vurdering af forskellige anmeldte elektroniske identifikationsordninger og gøre det lettere at opbygge tillid mellem medlemsstaterne. Nye, forenklede mekanismer bør fremme medlemsstaternes samarbejde om sikkerhed og interoperabilitet i deres anmeldte elektroniske identifikationsordninger.
- (16) Medlemsstaterne bør nyde godt af nye, fleksible værktøjer til at sikre overholdelse af kravene i denne forordning og i de relevante gennemførelsesretsakter. Denne forordning bør give medlemsstaterne mulighed for at anvende rapporter og vurderinger, der er udarbejdet og udført af akkrediterede overensstemmelsesvurderingsorganer, som fastsat i de 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 kravene i denne forordning vedrørende interoperabilitet og sikkerhed i de anmeldte elektroniske identifikationsordninger.

---

<sup>9</sup> 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).

- (17a) Anvendelsen af entydige og vedvarende identifikatorer, som er udstedt af medlemsstaterne eller genereret af den europæiske digitale ID-tegnebog, sammen med anvendelsen af personidentifikationsdata er afgørende for at sikre, at brugerens identitet kan kontrolleres, navnlig i den offentlige sektor, og når det er påkrævet i henhold til national ret eller EU-retten. Denne forordning bør sikre, at den europæiske digitale ID-tegnebog kan tilvejebringe en mekanisme, der giver mulighed for matchning af registreringer, herunder ved hjælp af kvalificerede elektroniske attesteringer af attributter, og gøre det muligt at medtage entydige og vedvarende identifikatorer i personidentifikationsdatasættet. En entydig og vedvarende identifikator kan bestå af enkelte eller flere identifikationsdata, som kan være sektorspecifikke, så længe den bruges til entydigt at identificere brugeren i hele Unionen. Den europæiske digitale ID-tegnebog bør også tilvejebringe en mekanisme, der gør det muligt at benytte modtagerpartsspecifikke identifikatorer i tilfælde, hvor anvendelsen af en unik og vedvarende identifikator er påkrævet i henhold til national ret eller EU-retten. I alle tilfælde bør den mekanisme, der tilvejebringes med henblik på at lette matchning af registreringer og brugen af unikke og vedvarende identifikatorer, sikre, at brugeren beskyttes mod misbrug af personoplysninger i henhold til nærværende forordning og gældende EU-ret, navnlig forordning (EU) 2016/679, herunder mod risikoen for profilering og sporing i forbindelse med anvendelsen af den europæiske digitale ID-tegnebog.
- (17aa) Det er afgørende at tage hensyn til brugernes behov og på den måde øge efterspørgslen efter europæiske digitale ID-tegnebøger. Der bør være meningsfulde brugstilfælde og onlinetjenester, der benytter europæiske digitale ID-tegnebøger. Af hensyn til brugerne og for at sikre, at sådanne tjenester er tilgængelige på tværs af grænserne, er det vigtigt at træffe foranstaltninger for 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 ID-tegnebøger, har potentiale til at blive et nyttigt redskab til at nå dette mål. Disse retningslinjer bør udarbejdes under behørig hensyntagen til Unionens interoperabilitetsramme. Medlemsstaterne bør have en fremtrædende rolle i forbindelse med deres vedtagelse.

- (18) I overensstemmelse med direktiv (EU) 2019/882<sup>10</sup> skal personer med handicap kunne anvende europæiske digitale ID-tegnebøger, tillidstjenester og de slutbrugerprodukter, der anvendes til levering af sådanne tjenester, på lige fod med andre brugere.
- (19) Denne forordning bør ikke omfatte aspekter relateret til indgåelse og gyldighed af kontrakter eller andre retlige forpligtelser, som ifølge national ret eller EU-retten er undergivet formkrav. Den bør heller ikke berøre nationale formkrav til offentlige registre, navnlig handelsregistre og tingbøger.
- (20) Levering og anvendelse af tillidstjenester er af stadig større betydning for international handel og internationalt samarbejde. EU's internationale partnere etablerer tillidsrammer inspireret af forordning (EU) nr. 910/2014. For at lette anerkendelsen af sådanne tjenester og deres udbydere kan der ved gennemførelseslovgivning derfor fastsættes betingelser for, hvornår tredjelandes tillidsrammer kan anses for at modsvare tillidsrammerne for kvalificerede tillidstjenester og udbydere heraf i denne forordning, som et supplement til muligheden for gensidig anerkendelse af tillidstjenester og udbydere, der er etableret i Unionen og i tredjelande, jf. traktatens artikel 218. Ved fastsættelsen af betingelserne for, at tredjelandes tillidsrammer kan anses for at være ækvivalente med tillidsrammen for kvalificerede tillidstjenester og udbydere i denne forordning, bør det også sikres, at de relevante bestemmelser i direktiv XXXX/XXXX (NIS 2-direktivet) og forordning (EU) 2016/679 overholdes, samt at positivlister anvendes som grundlæggende elementer for at opbygge tillid.

---

<sup>10</sup> 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).

- (21) Denne forordning bør bygge på EU-retsakter, der sikrer åbne og retfærdige markeder i den digitale sektor. Den bygger navnlig på forordning (EU) 2022/1925, ved hvilken der indføres regler for udbydere af centrale platformstjenester, der er udpeget som gatekeepere, og det blandt andet forbydes gatekeepere at kræve, at erhvervsbrugere anvender, udbyder eller interagerer med en identifikationstjeneste hos gatekeeperen i forbindelse med tjenester, der udbydes af erhvervsbrugere, der anvender den pågældende gatekeepers centrale platformstjenester. I henhold til artikel 6, stk. 7, i forordning (EU) 2022/1925 skal gatekeepere give erhvervsbrugere og udbydere af accessoriske tjenester adgang til og interoperabilitet med de samme styresystemer, hardware- eller softwarefunktioner, som er tilgængelige eller anvendes i gatekeeperens levering af eventuelle accessoriske tjenester. I henhold til artikel 2, nr. 15), i retsakten om digitale markeder udgør identifikationstjenester en type hjælpetjenester. Erhvervsbrugere og udbydere af hjælpetjenester bør derfor kunne få adgang til sådanne hardware- eller softwarefunktioner, som f.eks. sikre elementer i smartphones, og kunne fungere sammen med dem gennem europæiske digitale ID-tegnebøger eller medlemsstaternes anmeldte elektroniske identifikationsmidler.

(22) 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 XXXX/XXXX (NIS 2-direktivet), skal tillidstjenester træffe passende tekniske og organisatoriske foranstaltninger i overensstemmelse med direktiv XXXX/XXXX (NIS 2-direktivet), som f.eks. foranstaltninger til håndtering af systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener, med henblik på at styre de risici for sikkerheden i 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 direktiv XXXX/XXXX (NIS 2-direktivet). Med hensyn til 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 i forbindelse med identifikation af personer. Kravene vedrørende risikostyring i forbindelse med cybersikkerhed og rapporteringsforpligtelserne i direktiv XXXXXX [NIS 2] bør anses som supplerende til de krav, der pålægges tillidstjenesteudbydere i henhold til denne forordning. Hvis det er relevant, bør etablerede 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 XXXX/XXXX (NIS 2-direktivet). Krav i henhold til denne forordning berører ikke forpligtelsen til i henhold til forordning (EU) 2016/679 at anmelde brud på persondatasikkerheden.

- (23) Der bør tages behørigt hensyn til at sikre et effektivt samarbejde mellem NIS- og eIDAS-myndighederne. I tilfælde, hvor tilsynsorganet i henhold til denne forordning adskiller sig fra de kompetente myndigheder, der er udpeget i henhold til direktiv XXXX/XXXX [NIS 2], bør disse myndigheder samarbejde tæt og rettidigt ved at udveksle relevante oplysninger med henblik på at sikre et effektivt tilsyn med tillidstjenesteudbydere og deres overholdelse af de krav, der er fastsat i denne forordning og i direktiv XXXX/XXXX [NIS 2]. Tilsynsorganer i henhold til denne forordning bør navnlig have ret til at anmode den kompetente myndighed i henhold til direktiv XXXXX/XXXX [NIS 2] om at fremlægge de relevante oplysninger, der er nødvendige for at tildele status som kvalificeret og gennemføre tilsynsforanstaltninger for at kontrollere, at tillidstjenesteudbydere overholder de i henhold til NIS 2 relevante krav, eller pålægge dem at afhjælpe manglende overholdelse.
- (24) Det er vigtigt at fastlægge en retlig ramme for at lette grænseoverskridende anerkendelse mellem eksisterende nationale retsregler vedrørende elektroniske registrerede leveringstjenester. Denne ramme vil også kunne åbne nye markedsmuligheder for tillidstjenesteudbydere i Unionen med hensyn til at udbyde nye fælleseuropæiske 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 fuld sikkerhed sikre identifikationen af modtageren, samtidig med at en høj grad af tillid vil være tilstrækkelig med hensyn til identifikationen af afsenderen. Medlemsstaterne bør tilskynde udbydere af kvalificerede elektroniske registrerede leveringstjenester til at få deres tjenester gjort interoperable med kvalificerede elektroniske registrerede leveringstjenester, der leveres af andre kvalificerede tillidstjenesteudbydere, for nemt at overføre de elektroniske registrerede data mellem to eller flere kvalificerede tillidstjenesteudbydere og fremme fair praksis på det indre marked.
- (25) I de fleste tilfælde kan borgere og andre indbyggere ikke digitalt og på tværs af grænserne udveksle oplysninger vedrørende deres identitet, som f.eks. adresser, alder og erhvervs-mæssige kvalifikationer, kørekort og andre tilladelser og betalingsdata, på sikker vis og med et højt databeskyttelsesniveau.

- (26) Det bør være muligt at udstede og håndtere pålidelige digitale attributter og bidrage til at mindske den administrative byrde og derved give borgere og andre indbyggere mulighed for at anvende dem i deres private og offentlige transaktioner. Borgere og andre indbyggere bør for eksempel kunne dokumentere besiddelse af et gyldigt kørekort, der er udstedt af en myndighed i en medlemsstat, og som de relevante myndigheder i andre medlemsstater kan kontrollere og have tillid til, i forbindelse med deres socialsikringsoplysninger eller fremtidige digitale rejsedokumenter i en grænseoverskridende sammenhæng.
- (27) Enhver enhed, der indsamler, genererer og udsteder attesterede attributter såsom eksamensbeviser, tilladelser og fødselsattester bør kunne blive udbyder af elektroniske attesteringer af attributter. Modtagerparter bør anvende elektroniske attesteringer af attributter på lige fod med attesteringer i papirform. Derfor bør en elektronisk attestering af attributter 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. Med henblik herpå bør der 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 med forbehold for EU-retten eller national ret, der fastsætter yderligere sektorspecifikke krav for så vidt angår form med underliggende retsvirkning og navnlig grænseoverskridende anerkendelse af kvalificerede elektroniske attesteringer af attributter, hvis det er relevant.

(28) En bred tilgængelighed og anvendelighed af de europæiske digitale ID-tegnebøger kræver, at de accepteres af private tjenesteudbydere. De private modtagerparter, der leverer tjenester inden for transport, energi, banktjenester, finansielle tjenesteydelser, socialsikring, sundhed, drikkevand, posttjenester, digital infrastruktur, uddannelse eller telekommunikation, bør acceptere anvendelse af europæiske digitale ID-tegnebøger til levering af tjenester, hvor stærk brugerautentifikation er påkrævet i henhold til national ret eller EU-retten eller i henhold til en kontraktlig forpligtelse. For at lette anvendelsen og accepten af den europæiske digitale ID-tegnebog bør der tages hensyn til bredt anerkendte industristandarder og -specifikationer. Hvis meget store onlineplatforme som defineret i artikel 25, stk. 1, i forordning [retsakten om digitale tjenester] kræver, at brugere autentificeres for at få adgang til onlinetjenester, bør disse platforme pålægges at acceptere anvendelse af europæiske digitale ID-tegnebøger efter frivillig anmodning fra brugeren. Brugerne bør ikke være forpligtede til at anvende tegnebogen for at få adgang til private tjenester, men hvis de ønsker det, bør store onlineplatforme acceptere europæiske digitale ID-tegnebøger til dette formål, samtidig med at princippet om dataminimering respekteres. I betragtning af den betydning, meget store onlineplatforme har grundet deres rækkevidde, navnlig som udtrykt i antallet af modtagere af en tjeneste og økonomiske transaktioner, er dette nødvendigt for at øge brugernes beskyttelse mod svig og sikre et højt databeskyttelsesniveau. Der bør udarbejdes selvregulerende adfærdskodekser på EU-plan ("adfærdskodekser") med henblik på at bidrage til en bred tilgængelighed og anvendelighed af elektroniske identifikationsmidler, herunder europæiske digitale ID-tegnebøger, inden for denne forordnings anvendelsesområde. Adfærdskodekserne bør lette en bred accept af elektroniske identifikationsmidler, herunder europæiske digitale ID-tegnebøger, hos de tjenesteudbydere, der ikke betragtes som meget store platforme, og som benytter tredjeparters elektroniske identifikationstjenester til brugerautentifikation. Kodekserne bør udarbejdes senest 12 måneder efter vedtagelsen af denne forordning. Kommissionen bør vurdere effektiviteten af disse bestemmelser med hensyn til tilgængeligheden og anvendeligheden for brugerne af europæiske digitale ID-tegnebøger 24 måneder efter indførelsen heraf.



- (29) 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 kan indhente de oplysninger, der kræves, f.eks. at en bruger kun må videregive de data til en modtagerpart, som er nødvendige for levering af en tjeneste, som en bruger har anmodet om. Den europæiske digitale ID-tegnebog bør gøre selektiv videregivelse af attributter til modtagerparter teknisk mulig. Sådanne selektivt videregivne attributter, herunder når de oprindeligt var dele af flere særskilte elektroniske attesteringer, kan efterfølgende kombineres og fremlægges for modtagerparter. Denne funktion bør blive et grundlæggende element i udformningen og derved styrke bekvemmeligheden og beskyttelsen af personoplysninger, herunder dataminimering.
- (30) Attributter, der leveres af kvalificerede tillidstjenesteudbydere som led i kvalificerede attesteringer af attributter, bør kontrolleres mod de autentiske kilder enten direkte af den kvalificerede tillidstjenesteudbyder eller ved hjælp af udpegede mellemmand, der er anerkendt på nationalt plan i overensstemmelse med national ret eller EU-retten, 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 ved hjælp af autentiske kilder. Passende mekanismer kan omfatte anvendelse af specifikke mellemmand eller tekniske løsninger i overensstemmelse med national ret, der giver adgang til autentiske kilder. Sikring af, at der findes en mekanisme, der gør det muligt at kontrollere attributter mod autentiske kilder, bør gøre det lettere for kvalificerede tillidstjenesteudbydere af kvalificeret elektronisk attestering af attributter at overholde deres forpligtelser som fastsat i denne forordning. Bilag VI indeholder en liste over kategorier af attributter, for hvilke medlemsstaterne bør sikre, at der træffes foranstaltninger, så kvalificerede udbydere af elektroniske attesteringer af attributter på brugerens anmodning elektronisk kan kontrollere deres ægthed mod den relevante autentiske kilde. Medlemsstaterne bør være enige om de specifikke attributter, der falder ind under disse kategorier.

- (31) 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 forordningen om bekæmpelse af hvidvaskning af penge [henvisning tilføjes efter vedtagelsen af forslaget], eller egnethedskrav, der følger af lovgivning om investorbekyttelse, eller for at støtte opfyldelsen af krav om stærk kundeautentifikation til onlineidentifikation med henblik på kontologin og iværksættelse af transaktioner inden for betalingstjenester.
- (31a) For at sikre ensartet certificeringspraksis i hele EU 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 medlemsstaterne i at tillade offentlige eller private organer, der har certificerede kvalificerede elektroniske signaturgenereringssystemer, midlertidigt at forlænge gyldigheden af certificeringen, når en fornyet certificering af det samme system ikke har kunnet ske inden for den lovbestemte tidsramme af andre årsager end et brud eller en sikkerhedshændelse, og uden at dette berører den gældende certificeringspraksis.

(32) Webstedsautentifikations tjenester giver brugere en høj grad af sikkerhed for, at der bag et websted står en ægte og legitim enhed, uanset hvilken platform der anvendes til at vise det. Disse tjenester bidrager til at opbygge tillid og tryghed til at drive forretning online og nedbringe tilfælde af onlinesvindel. Websteders brug af webstedsautentifikations tjenester bør være frivillig. For at webstedsautentifikation kan blive et middel til at fremme tilliden ved at give brugerne en bedre oplevelse og stimulere vækst på det indre marked, bør der imidlertid ved denne forordning fastsættes minimumsforpligtelser for udbydere af webstedsautentifikations tjenester og deres tjenester med hensyn til sikkerhed og ansvar. Med henblik herpå bør webbrowsereudbydere sørge for støtte af og interoperabilitet med kvalificerede certifikater for webstedsautentifikation i henhold til forordning (EU) nr. 910/2014. De bør anerkende kvalificerede certifikater for webstedsautentifikation og gøre det muligt at vise de certificerede identitetsdata for slutbrugeren i browsermiljøet på grundlag af de specifikationer, der er fastsat i overensstemmelse med nærværende forordning. Anerkendelsen af et kvalificeret certifikat for webstedsautentifikation som et kvalificeret certifikat udstedt af en kvalificeret tillidstjenesteudbyder bør sikre, at de identitetsdata, der indgår i certifikatet, kan autentificeres og kontrolleres i overensstemmelse med nærværende forordning. Dette bør ikke berøre muligheden for, at udbydere af webbrowsere kan afhjælpe større uoverensstemmelser i forbindelse med brud på sikkerheden og tab af integritet i individuelle certifikater og dermed bidrage til slutbrugernes onlinesikkerhed. For yderligere at beskytte borgerne og fremme brugen af certifikaterne bør offentlige myndigheder i medlemsstaterne overveje at indføre kvalificerede certifikater for webstedsautentifikation for deres websteder.

(33) Mange medlemsstater har indført nationale krav til tjenester, der leverer sikker og pålidelig digital arkivering, for at gøre det muligt at bevare elektroniske data og tilknyttede tillidstjenester i lang tid. For at sikre retssikkerhed, tillid og harmonisering på tværs af medlemsstaterne bør der etableres en retlig ramme for kvalificerede elektroniske arkiveringstjenester, der er inspireret af rammen for de andre tillidstjenester, der er fastsat i denne forordning. Denne ramme 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 både elektronisk fødte dokumenter og papirdokumenter, der er blevet scannet og digitaliseret. Når det kræves, bør det i henhold til disse bestemmelser være muligt at overføre de bevarede elektroniske data til forskellige medier eller formater med henblik på at forlænge deres holdbarhed og læsbarhed ud over den teknologiske gyldighedsperiode, samtidig med at tab og ændringer minimeres i videst muligt omfang. Når elektroniske data, der indgives til den digitale arkivtjeneste, indeholder en eller flere kvalificerede elektroniske signaturer eller kvalificerede elektroniske segl, bør tjenesten anvende procedurer og teknologier, der kan forlænge deres pålidelighed for den periode, hvor sådanne data opbevares, eventuelt ved hjælp af andre kvalificerede elektroniske tillidstjenester, der er oprettet ved denne forordning. Der bør anvendes kvalificerede elektroniske tillidstjenester til at frembringe opbevaringsdokumentation, hvor der anvendes elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler. I det omfang elektroniske arkiveringstjenester ikke er harmoniseret ved denne forordning, kan medlemsstaterne i overensstemmelse med EU-retten opretholde eller indføre nationale bestemmelser vedrørende disse tjenester såsom specifikke bestemmelser, der tillader visse undtagelser for tjenester, der er integreret i en organisation og udelukkende anvendes til denne organisations "interne arkiver". I denne forordning bør der ikke skelnes mellem elektronisk fødte dokumenter og fysiske dokumenter, der er blevet digitaliseret.

- (33a) Nationale arkiver og hukommelsesinstitutioner har i deres egenskab af organisationer, der har til opgave at bevare den dokumenterede arv i offentlighedens interesse, normalt bemyndigelse til at udføre deres aktiviteter i henhold til national ret og leverer ikke nødvendigvis tillidstjenester som omhandlet i denne forordning. For så vidt disse institutioner ikke leverer sådanne tjenester, berører denne forordning ikke deres drift.
- (34) Elektroniske hovedbøger er en sekvens af elektroniske dataposter, der sikrer deres integritet og nøjagtigheden af deres kronologiske rækkefølge. Formålet med elektroniske hovedbøger er at fastlægge en kronologisk rækkefølge af dataposter for at forhindre, at digitale aktiver kopieres og sælges til flere modtagere. Elektroniske hovedbøger kan f.eks. anvendes til digitale registreringer af ejerskab inden for global handel, forsyningskædefinansiering, digitalisering af intellektuelle ejendomsrettigheder eller af råvarer såsom elektricitet. Sammen med andre teknologier kan 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 eller registrering af ejerskab til fast ejendom i decentraler matrikelregistre. Kvalificerede elektroniske hovedbøger skaber en retlig formodning for den entydige og nøjagtige kronologiske rækkefølge og integritet af dataposterne i hovedbogen. De specifikke attributter ved elektroniske hovedbøger, dvs. den sekventielle kronologiske rækkefølge af dataposter, adskiller elektroniske hovedbøger fra andre tillidstjenester såsom elektroniske tidsstempler og elektroniske registrerede leveringstjenester. Hverken tidsstempling af digitale dokumenter eller overførsel heraf ved hjælp af elektroniske registrerede leveringstjenester kan nemlig uden yderligere tekniske eller organisatoriske foranstaltninger 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 (centraliseret eller distribueret).

(35) For at forhindre fragmentering på det indre marked bør der oprettes en paneuropæisk retlig ramme, der muliggør grænseoverskridende anerkendelse af tillidstjenester med hensyn til registrering af data i kvalificerede elektroniske hovedbøger. Tillidstjenesteudbydere af elektroniske hovedbøger bør have bemyndigelse til at få fastslået den sekventielle registrering af data i hovedbogen. Denne forordning gælder uanset eventuelle retlige forpligtelser, som brugere af elektroniske hovedbøger måtte skulle opfylde i henhold til EU-retten og national ret. F.eks. bør brugstilfælde, der involverer behandling af personoplysninger, være i overensstemmelse med forordning (EU) 2016/679. Brugstilfælde, der involverer kryptoaktiver, bør være forenelige med alle gældende finansielle regler, herunder f.eks. direktivet om markeder for finansielle instrumenter<sup>11</sup>, betalingstjenestedirektivet<sup>12</sup> og direktivet om elektroniske penge<sup>13</sup>, samt eventuel fremtidig lovgivning om markeder for kryptoaktiver og med regler om bekæmpelse af hvidvask af penge, som kan indgå i forordningen om pengeoverførsler<sup>14</sup>, og kan kræve, at udbydere af kryptoaktivtjenester kontrollerer identiteten af brugere af elektroniske hovedbøger for at overholde internationale standarder for bekæmpelse af hvidvask af penge.

---

<sup>11</sup> Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF (EUT L 173 af 12.6.2014, s. 349).

<sup>12</sup> Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

<sup>13</sup> Europa-Parlamentets og Rådets direktiv 2009/110/EF af 16. september 2009 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, ændring af direktiv 2005/60/EF og 2006/48/EF og ophævelse af direktiv 2000/46/EF (EUT L 267 af 10.10.2009, s. 7).

<sup>14</sup> Se Kommissionens [forslag af 20.7.2021 om omarbejdning af](#) Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler (COM(2021) 422 final).

- (36) For at undgå fragmentering og hindringer som følge af divergerende standarder og tekniske restriktioner og for at sikre en koordineret proces, hvorved det undgås at bringe gennemførelsen af den kommende europæiske ramme for digital identitet i fare, er der behov for en procedure for et tæt og struktureret samarbejde mellem Kommissionen, medlemsstaterne og den private sektor. For at nå dette mål bør medlemsstaterne samarbejde inden for de rammer, der er fastsat i Kommissionens henstilling XXX/XXXX [værktøjskasse for en koordineret tilgang til en ramme for en europæisk digital identitet]<sup>15</sup>, om at udarbejde en værktøjskasse for en europæisk ramme for digital identitet. Værktøjsskassen bør indeholde en omfattende teknisk arkitektur og referenceramme, et sæt fælles standarder og tekniske referencer og et sæt retningslinjer og beskrivelser af bedste praksis, der som minimum dækker alle aspekter af funktionaliteten og interoperabiliteten af europæiske digitale ID-tegnebøger, herunder e-signaturer, og den kvalificerede tillidstjeneste til attestering af attributter som fastsat i denne forordning. I den forbindelse bør medlemsstaterne også nå til enighed om fælles elementer i en forretningsmodel og en gebyrstruktur for europæiske digitale ID-tegnebøger for at lette udbredelsen, navnlig blandt små og mellemstore virksomheder, i en grænseoverskridende sammenhæng. Værktøjskassens indhold bør udvikles parallelt med og afspejle resultatet af drøftelserne af og processen for vedtagelsen af den europæiske ramme for digital identitet.
- (36a) 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 overbevisning, at ikkekvalificerede tillidstjenester, der tilbydes af denne udbyder, er kvalificerede.

---

<sup>15</sup> [Indsæt henvisning efter vedtagelsen.]

- (36b) Denne forordning bør sikre et harmoniseret niveau af kvalitet, pålidelighed og sikkerhed for kvalificerede tillidstjenester, uanset stedet, hvor aktiviteterne udføres. En kvalificeret tillidstjenesteudbyder bør derfor have mulighed for at outsource sine aktiviteter i forbindelse med levering af en kvalificeret tillidstjeneste uden for Unionen, hvis den stiller garantier, og sikre, at tilsynsaktiviteter og revisioner kan håndhæves, som om disse aktiviteter blev udført i Unionen. Når overholdelsen af forordningen ikke kan sikres fuldt ud, bør tilsynsorganerne kunne vedtage forholdsmæssige og begrundede foranstaltninger, herunder inddragelse af status som kvalificeret for den udbudte tillidstjeneste.
- (36c) For at sikre retssikkerhed for så vidt angår gyldigheden af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater, er det nødvendigt at specificere, hvilke elementer af en avanceret elektronisk signatur, der er baseret på kvalificerede certifikater, der bør vurderes af den modtagerpart, der foretager valideringen af den pågældende signatur.
- (36d) Tillidstjenesteudbydere bør anvende kryptografiske algoritmer, der afspejler nuværende bedste praksis og pålidelige implementeringer af disse algoritmer, for at sikre deres tillidstjenesters sikkerhed og pålidelighed.
- (36e) Denne forordning bør fastsætte en forpligtelse for kvalificerede tillidstjenesteudbydere til at kontrollere identiteten af en fysisk eller juridisk person, som det kvalificerede certifikat er udstedt til, på grundlag af forskellige harmoniserede metoder i hele EU. En sådan metode kan omfatte anvendelse af elektroniske identifikationsmidler, der opfylder kravene til sikringsniveau "betydelig" kombineret med yderligere harmoniserede procedurer på afstand, der sikrer identifikation af personen med en høj grad af tillid.



- (36f) Udstedere af europæiske digitale ID-tegnebøger og udstedere af anmeldte elektroniske identifikationsmidler, der handler i kommerciel eller professionel egenskab og anvender centrale platformstjenester, som udbydes af gatekeepere med henblik på eller i forbindelse med levering af varer og tjenesteydelser til slutbrugere, bør betragtes som erhvervsbrugere i overensstemmelse med artikel 2, nr. 21), i forordning (EU) 2022/1925. Det bør derfor kræves af gatekeeperne, at de gratis sikrer effektiv interoperabilitet med og adgang med henblik på interoperabilitet til det samme styresystem, den samme hardware eller de samme softwarefunktioner, som er tilgængelige eller anvendes i forbindelse med, at de udbyder deres egne supplerende og understøttende tjenester og hardware. Dette bør gøre det muligt for udstedere af europæiske digitale ID-tegnebøger og udstedere af anmeldte elektroniske identifikationsmidler at sammenkoble via grænseflader eller lignende løsninger til de respektive funktioner lige så effektivt som gatekeeperens egne tjenester eller hardware.
- (36g) For at holde denne forordning i overensstemmelse med den nuværende udvikling og følge 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, der er opstået på det indre marked.
- (37) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1525<sup>16</sup>.
- (38) Forordning (EU) nr. 910/2014 bør derfor ændres i overensstemmelse hermed –

---

<sup>16</sup> 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).

VEDTAGET DENNE FORORDNING:

*Artikel 1*

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

1) Artikel 1 affattes således:

"Denne forordning har til formål at sikre et velfungerende indre marked og et tilstrækkeligt sikkerhedsniveau for elektroniske identifikationsmidler og tillidstjenester. Med henblik herpå omfatter denne forordning:

- aa) fastsættelse af betingelser for, hvordan medlemsstaterne leverer og anerkender elektroniske identifikationsmidler for fysiske og juridiske personer, der er omfattet af en anmeldt elektronisk identifikationsordning i en anden medlemsstat
- ab) fastsættelse af betingelser for, hvordan medlemsstaterne leverer og anerkender europæiske digitale ID-tegnebøger
- 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 validering af elektroniske signaturer, elektroniske segl og deres certifikater, elektronisk validering af certifikater for webstedsautentifikation, elektronisk bevaring af elektroniske signaturer, elektroniske segl og deres certifikater, elektronisk arkivering, elektronisk attestering af attributter, forvaltning af kvalificerede elektroniske systemer til signatur- og sejlgenerering på afstand 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 blevet anmeldt af en medlemsstat, europæiske digitale ID-tegnebøger, der er leveret af en medlemsstat, samt tillidstjenesteudbydere, der er hjemmehørende i Unionen."

b) Stk. 3 affattes således:

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

3) I artikel 3 foretages følgende ændringer:

X) Nr. 1) affattes således:

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

a) Nr. 2) affattes således:

"2) "elektronisk identifikationsmiddel": en materiel og/eller immateriel enhed, herunder europæiske digitale ID-tegnebøger, der indeholder personidentifikationsdata, og som bruges til autentifikation i forbindelse med en onlinetjeneste eller, hvis det er relevant, en offlinetjeneste".

aa) Nr. 3) affattes således:

"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 en fysisk person, der repræsenterer en fysisk eller juridisk person".

b) Nr. 4) affattes således:

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

ba) Nr. 5) affattes således:

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".

bb) Følgende indsættes som nr. 5a):

"5a) "bruger": en fysisk eller juridisk person eller en fysisk person, der repræsenterer en fysisk eller juridisk person, som anvender tillidstjenester eller elektroniske identifikationsmidler, der leveres i henhold til denne forordning".

c) Nr. 14) affattes således:

"14) "certifikat for elektronisk signatur": en elektronisk attestering, som knytter elektroniske signaturvalideringsdata til en fysisk person og som minimum bekræfter denne persons navn eller pseudonym".

d) Nr. 16) affattes således:

"16) "tillidstjeneste": en elektronisk tjeneste, der normalt udføres mod betaling, og som består af:

- a) udstedelse af certifikater for elektroniske signaturer, certifikater for elektroniske segl, certifikater for webstedsautentifikation eller certifikater for levering af andre tillidstjenester
- aa) validering af certifikater for elektroniske signaturer, certifikater for elektroniske segl, certifikater for webstedsautentifikation eller certifikater for levering af andre tillidstjenester
- b) generering af elektroniske signaturer eller elektroniske segl
- c) validering af elektroniske signaturer eller elektroniske segl
- d) bevaring af elektroniske signaturer, elektroniske segl, certifikater for elektroniske signaturer eller certifikater for elektroniske segl
- e) forvaltning af kvalificerede elektroniske systemer til signaturgenerering på afstand eller af kvalificerede elektroniske systemer til sejlgenerering på afstand
- f) udstedelse af elektroniske attesteringer af attributter

- fa) validering af elektronisk attestering af attributter
- g) generering af elektroniske tidsstempler
- ga) validering af elektroniske tidsstempler
- gb) udførelse af elektroniske registrerede leveringstjenester
- gc) validering af data fremsendt via elektroniske registrerede leveringstjenester og tilhørende dokumentation
- h) elektronisk arkivering af elektroniske data eller
- i) registrering af elektroniske data i en elektronisk hovedbog".

da) Nr. 18) affattes således:

"18) "overensstemmelsesvurderingsorgan": et organ 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 til at udføre certificering af europæiske digitale ID-tegnebøger eller elektroniske identifikationsmidler".

e) Nr. 21) affattes således:

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

f) Som nr. 23a) og 23b) indsættes:

"23a) "kvalificeret elektronisk system til signaturgenerering 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 system til seglgenerering på afstand": et kvalificeret elektronisk seglgenereringssystem, der i overensstemmelse med artikel 39a forvaltes af en kvalificeret tillidstjenesteudbyder på vegne af en forseglende part".

g) Nr. 29) affattes således:

"29) "certifikat for elektronisk segl": en elektronisk attestering, som knytter elektroniske seglvalideringsdata til en fysisk person og bekræfter denne persons navn".

h) Nr. 41) affattes således:

"41) "validering": en fremgangsmåde til at kontrollere og bekræfte gyldigheden af data i elektronisk form i henhold til kravene i denne forordning".

i) Som nr. 42) til 55c) tilføjes:

"42) "europæisk digital ID-tegnebog": et elektronisk identifikationsmiddel, der gør det muligt for brugeren at lagre og hente identitetsdata, herunder personidentifikationsdata, elektroniske attesteringer af attributter knyttet til deres identitet, stille disse til rådighed for modtagerparter efter anmodning og anvende dem online og, hvis det er relevant, offline til autentifikation i forbindelse med en tjeneste i overensstemmelse med artikel 6a, og at underskrive ved hjælp af kvalificerede elektroniske signaturer og at 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
- 45a) "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 45da, og som opfylder de krav, der er fastsat i bilag VII
- 46) "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, 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
- 47) "elektronisk arkivering": en tjeneste, der sikrer modtagelse, lagring, hentning og sletning af elektroniske data med henblik på at garantere deres holdbarhed og læsbarhed samt at bevare deres integritet, fortrolighed og oprindelsesbevis i hele opbevaringsperioden



- 48) "kvalificeret elektronisk arkiveringstjeneste": en elektronisk arkiveringstjeneste, der opfylder de krav, der er fastsat i artikel 45ga
- 49) "EU-tillidsmærke for europæiske digitale ID-tegnebøger": en kontrollerbar simpel, genkendelig og tydelig angivelse af, at en europæisk digital ID-tegnebog er leveret i overensstemmelse med denne forordning
- 50) "stærk brugerautentifikation": en autentifikation baseret på anvendelse af mindst to autentifikationsfaktorer fra forskellige kategorier af enten viden (noget, som kun brugeren ved), besiddelse (noget, som kun brugeren besidder) eller iboende egenskab (noget, som brugeren er), og som er uafhængige, idet brud på et af dem ikke svækker de andres pålidelighed, og som desuden er udformet på en måde, der beskytter fortroligheden af autentifikationsdataene
- 53) "elektronisk hovedbog": en sekvens af elektroniske dataposter, der sikrer deres integritet og nøjagtigheden af deres kronologiske rækkefølge
- 53a) "kvalificeret elektronisk hovedbog": en elektronisk hovedbog, der opfylder de krav, der er fastsat i artikel 45i
- 54) "personoplysninger": personoplysninger som defineret i artikel 4, nr. 1), i forordning (EU) 2016/679
- 55) "matchning af registreringer": en proces, hvorved personidentifikationsdata, personidentifikationsmidler, kvalificeret elektronisk attestering af attributter eller attesteringer af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, sammenholdes med eller knyttes til en eksisterende konto, der tilhører den samme person

- 55a) "entydig og vedvarende identifikator": en identifikator, der kan bestå af enten et eller flere nationale eller sektorspecifikke identifikationsdata, og som er knyttet til en enkelt bruger inden for et givet system og vedvarende over tid
- 55b) "datapost": elektroniske data, der er registreret med tilhørende metadata (eller attributter) til støtte for behandlingen af dataene
- 55c) "offlineanvendelse af europæiske digitale ID-tegnebøger": interaktion mellem en bruger og en modtagerpart på et fysisk sted, hvor det ikke er påkrævet, at tegnebogen kan få adgang til fjernsystemer via elektroniske kommunikationsnet med henblik på interaktionen."

#### *"Artikel 5*

#### Pseudonymer i elektroniske transaktioner

Uden at den retsvirkning, der tillægges pseudonymer i henhold til national ret dermed foregribes, forbydes anvendelsen af pseudonymer i elektroniske transaktioner ikke."

- 5) I kapitel II indsættes følgende som overskrift før artikel 6a:

#### "AFDELING I

Europæisk digital ID-tegnebog".

7) Som artikel 6a, 6b, 6c og 6d indsættes:

*"Artikel 6a*

Europæiske digitale ID-tegnebøger

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, sikrer hver medlemsstat, at der leveres en europæisk digital ID-tegnebog senest 24 måneder efter ikrafttrædelsen af de gennemførelsesretsakter, der er omhandlet i stk. 11 og artikel 6c, stk. 4.
2. Europæiske digitale ID-tegnebøger leveres:
  - a) af en medlemsstat
  - b) i henhold til et mandat fra en medlemsstat eller
  - c) uafhængigt af en medlemsstat, men med anerkendelse fra en medlemsstat.
3. Europæiske digitale ID-tegnebøger er elektroniske identifikationsmidler, der gør det muligt for brugeren på en måde, der er gennemsigtig og sporbar for brugeren:
  - a) på sikker vis at anmode om, udvælge, kombinere, lagre og slette elektronisk attestering af attributter og personidentifikationsdata og fremlægge dette for modtagerparter, herunder til autentifikation online og, hvis det er relevant, offline med henblik på at benytte offentlige og private tjenester, samtidig med at det sikres, at selektiv videregivelse af data er mulig
  - b) at underskrive ved hjælp af kvalificerede elektroniske signaturer og at forsegle ved hjælp af kvalificerede elektroniske segl.

4. Europæiske digitale ID-tegnebøger skal navnlig:
- a) have et fælles sæt brugergrænseflader:
    - 1) til udstedelse af personidentifikationsdata, kvalificerede og ikkekvalificerede elektroniske attesteringer af attributter eller kvalificerede og ikkekvalificerede certifikater til europæiske digitale ID-tegnebøger
    - 2) således at modtagerparter kan anmode om personidentifikationsdata og elektroniske attesteringer af attributter
    - 3) til forelæggelse for modtagerparter af personidentifikationsdata eller elektronisk attestering af attributter online og, hvis det er relevant, også offline
    - 4) således at brugeren kan interagere med den europæiske digitale ID-tegnebog og fremvise et "EU-tillidsmærke for europæiske digitale ID-tegnebøger"
  - b) ikke give tillidstjenesteudbydere af elektroniske attesteringer af attributter oplysninger om anvendelsen af sådanne attributter efter deres udstedelse
  - ba) sikre, at modtagerparternes identitet kan valideres ved at indføre autentifikationsmekanismer i overensstemmelse med artikel 6b
  - c) opfylde de krav, der er fastsat i artikel 8, med hensyn til sikringsniveauet "høj", der finder tilsvarende anvendelse på forvaltning og anvendelse af personidentifikationsdata gennem tegnebogen, herunder elektronisk identifikation og autentifikation
  - e) sikre, at de personidentifikationsdata, der er omhandlet i artikel 12, stk. 4, litra d), entydigt og vedvarende repræsenterer den fysiske eller juridiske person eller den fysiske person, der repræsenterer den fysiske eller juridiske person, som er knyttet til tegnebogen.

- 4a. Medlemsstaterne indfører procedurer, der gør det muligt for brugeren at indberette eventuelt tab eller misbrug af sin tegnebog og anmode om tilbagekaldelse.
5. Medlemsstaterne indfører valideringsmekanismer for europæiske digitale ID-tegnebøger med henblik på at:
- a) sikre, at tegnebøgernes autenticitet og gyldighed kan kontrolleres
  - d) give brugeren mulighed for at autentificere modtagerparter i overensstemmelse med artikel 6b.
6. De europæiske digitale ID-tegnebøger udstedes i henhold til en anmeldt elektronisk identifikationsordning med sikringsniveauet "høj".
- 6a. Det er gratis for fysiske personer at udstede europæiske digitale ID-tegnebøger, at anvende dem til autentifikation og at tilbagekalde dem.
- 6b. Uden at det berører artikel 6db, kan medlemsstaterne i overensstemmelse med national ret indføre yderligere funktionaliteter i de europæiske digitale ID-tegnebøger, herunder interoperabilitet med eksisterende nationale eID-midler.
7. Brugere har fuld kontrol over anvendelsen af den europæiske digitale ID-tegnebog og dataene i deres europæiske digitale ID-tegnebog. Udstederen af den europæiske digitale ID-tegnebog indsamler ikke oplysninger om anvendelsen af tegnebogen, som ikke er nødvendige for leveringen af tegnebogstjenester, og kombinerer heller ikke personidentifikationsdata og andre personoplysninger, der er lagret, eller som vedrører anvendelsen af den europæiske digitale ID-tegnebog, med personoplysninger fra andre tjenester, som udbydes af udstederen, eller fra tredjepartstjenester, som ikke er nødvendige for leveringen af tegnebogstjenester, medmindre brugeren udtrykkeligt har anmodet herom. Personoplysninger vedrørende levering af europæiske digitale ID-tegnebøger opbevares logisk adskilt fra alle andre data, der opbevares af udstederen af europæiske digitale ID-tegnebøger. Hvis den europæiske digitale ID-tegnebog er leveret af en privat part i overensstemmelse med stk. 2, litra b) og c), finder bestemmelserne i artikel 45f, stk. 4, tilsvarende anvendelse.

- 7a. Medlemsstaterne meddeler hurtigst muligt Kommissionen oplysninger om:
- a) det organ, der er ansvarligt for at oprette og ajourføre listen over anmeldte modtagerparter, der benytter de europæiske digitale ID-tegnebøger i overensstemmelse med artikel 6b, stk. 2
  - b) de organer, der er ansvarlige for leveringen af europæiske digitale ID-tegnebøger i overensstemmelse med artikel 6a, stk. 1
  - c) de organer, der er ansvarlige for at sikre, at personidentifikationsdataene har tilknytning til tegnebogen, jf. artikel 6a, stk. 4, litra e).

Meddelelsen skal også indeholde oplysninger om den mekanisme, der gør det muligt at validere de personidentifikationsdata, der er omhandlet i artikel 12, stk. 4, og modtagerparternes identitet.

Kommissionen stiller de oplysninger, der er omhandlet i dette stykke, til rådighed for offentligheden via en sikker kommunikationsforbindelse og i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

- 8. Artikel 11 finder tilsvarende anvendelse på europæiske digitale ID-tegnebøger.
- 9. Artikel 24, stk. 2, litra b), e), g) og h), finder tilsvarende anvendelse på udstederen af europæiske digitale ID-tegnebøger.
- 10. De europæiske digitale ID-tegnebøger gøres tilgængelige for personer med handicap i overensstemmelse med tilgængelighedskravene i direktiv 2019/882.

11. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen tekniske og operationelle specifikationer og referencestandarder for de i stk. 3, 4, 5 og 7a omhandlede krav ved hjælp af en gennemførelsesretsakt om gennemførelsen af europæiske digitale ID-tegnebøger. Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.
- 11a. Kommissionen fastsætter tekniske og operationelle specifikationer og referencestandarder med henblik på at lette brugernes onboarding af den europæiske digitale ID-tegnebog ved hjælp af enten elektroniske identifikationsmidler, der opfylder niveauet "høj", eller elektroniske identifikationsmidler, der opfylder niveauet "betydelig", sammenholdt med yderligere onboardingprocedurer på afstand, som tilsammen opfylder kravene til sikringsniveauet "høj". Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

#### *Artikel 6b*

##### Modtagerparter i forbindelse med europæiske digitale ID-tegnebøger

1. Hvis modtagerparter, der leverer private eller offentlige tjenester, har til hensigt at benytte europæiske digitale ID-tegnebøger, der er leveret i overensstemmelse med denne forordning, meddeler de dette til den medlemsstat, hvori modtagerparterne er etableret.
- 1a. Anmeldelsesproceduren skal være omkostningseffektiv og stå i et rimeligt forhold til risikoen og sikre, at modtagerparter som minimum giver de oplysninger, der er nødvendige for autentifikation til europæiske digitale ID-tegnebøger. Dette bør som minimum omfatte den medlemsstat, hvor de er etableret, samt modtagerpartens navn og, hvis det er relevant, registreringsnummer, som det fremgår af det officielle register.

- 1b. Anmeldelseskravet berører ikke andre anmeldelses- og registreringskrav i overensstemmelse med EU-retten eller national ret såsom dem, der gælder for særlige kategorier af personoplysninger, som kan kræve yderligere godkendelseskrav.
- 1c. Medlemsstaterne kan fritage modtagerparter fra anmeldelseskravet, hvis EU-retten eller national ret ikke fastsætter specifikke anmeldelses- eller registreringskrav for at få adgang til oplysninger, der leveres ved hjælp af den europæiske digitale ID-tegnebog. De fritagne modtagerparter behøver ikke autentifikation til den europæiske digitale ID-tegnebog.
- 1d. Modtagerparter, der er blevet anmeldt i henhold til denne artikel, underretter straks medlemsstaten om enhver efterfølgende ændring af de oprindeligt meddelte oplysninger.
2. Modtagerparterne sikrer gennemførelsen af de autentifikationsmekanismer, der er omhandlet i artikel 6a, stk. 4, litra ba).
3. Modtagerparterne er ansvarlige for at gennemføre proceduren for autentifikation af personer og validering af elektroniske attesteringer af attributter, der hidrører fra europæiske digitale ID-tegnebøger, som er indhentet via den fælles brugergrænseflade i henhold til artikel 6a, stk. 4, litra a), nr. 2).
4. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen tekniske og operationelle specifikationer for de i stk. 1, 1a og 1d omhandlede krav ved hjælp af en gennemførelsesretsakt om gennemførelsen af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11. Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.



## Artikel 6c

### Certificering af europæiske digitale ID-tegnebøger

1. Europæiske digitale ID-tegnebøgers overensstemmelse med kravene i artikel 6a, stk. 3, 4 og 5, med kravet om logisk adskillelse i artikel 6a, stk. 7, og, hvor det er relevant, med kravene i artikel 6a, stk. 11a, certificeres af overensstemmelsesvurderingsorganer, der er akkrediteret i overensstemmelse med artikel 60 i forordningen om cybersikkerhed og i overensstemmelse med de ordninger, specifikationer, standarder og procedurer, som der henvises til i stk. 4, litra a), aa) og aaa), og som er udpeget af medlemsstaterne. Certificeringen må ikke overstige fem år på betingelse af en regelmæssig sårbarhedsvurdering hvert andet år. Hvis der konstateres sårbarheder, og disse ikke udbedres inden for tre måneder, annulleres certificeringen.
2. For så vidt angår opfyldelse af databeskyttelseskravene i artikel 6a, stk. 7, kan certificeringen i stk. 1 suppleres med en certificering i henhold til artikel 42 i forordning (EU) 2016/679.
3. Overensstemmelsen af de europæiske digitale ID-tegnebøger eller dele heraf med de cybersikkerhedsrelevante krav i artikel 6a, stk. 3, 4, 5, 7 og, hvor det er relevant, stk. 11a, certificeres af de overensstemmelsesvurderingsorganer, der er omhandlet i stk. 1, inden for rammerne af de relevante cybersikkerhedscertificeringsordninger i henhold til forordning (EU) 2019/881, som der henvises til i stk. 4, litra a), og stk. 4, litra aa).
- 3a. Certificerede europæiske digitale ID-tegnebøger er ikke omfattet af kravene i artikel 7 og 9.

4. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter:
- a) en liste over cybersikkerhedscertificeringsordninger i henhold til forordning (EU) 2019/881, der kræves for certificering af de i stk. 3 omhandlede europæiske digitale ID-tegnebøger
  - aa) specifikationer, procedurer og referencestandarder for deres anvendelse i henhold til de relevante cybersikkerhedscertificeringsordninger, der er anført i overensstemmelse med litra a)
  - aaa) en liste over specifikationer, procedurer og referencestandarder, der fastlægger fælles certificeringskrav, som ikke er omfattet af relevante cybersikkerhedscertificeringsordninger i henhold til forordning (EU) 2019/881 med henblik på certificering, jf. stk. 1, med henblik på at påvise, at en europæisk digital ID-tegnebog opfylder kravene i stk. 1
- b) tekniske, proceduremæssige, organisatoriske og operationelle specifikationer for udpegelse af overensstemmelsesvurderingsorganer, jf. stk. 1, og, for så vidt angår de certificeringskrav, der er fastsat i henhold til litra aaa), for overvågning og revision af de certificeringsordninger og dertil knyttede evalueringsmetoder, som disse organer anvender, og de certifikater og certificeringsrapporter, de udsteder.
5. Medlemsstaterne meddeler Kommissionen navn og adresse på de i stk. 1 omhandlede offentlige eller private organer. Kommissionen stiller disse oplysninger til rådighed for medlemsstaterne.
6. De gennemførelsesretsakter, der er omhandlet i stk. 4, vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

## *Artikel 6d*

### Offentliggørelse af en liste over certificerede europæiske digitale ID-tegnebøger

1. Medlemsstaterne anmelder uden unødigt ophold de europæiske digitale ID-tegnebøger, der er leveret i henhold til artikel 6a og certificeret af de organer, der er omhandlet i artikel 6c, stk. 1, til Kommissionen. Medlemsstaterne underretter også uden unødigt ophold Kommissionen, hvis certificeringen er blevet annulleret.
2. På grundlag af de modtagne oplysninger opstiller, offentliggør og ajourfører Kommissionen en maskinlæsbar liste over certificerede europæiske digitale ID-tegnebøger.
3. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen formater og procedurer, der finder anvendelse med henblik på stk. 1 og 2, ved hjælp af en gennemførelsesretsakt om gennemførelse af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11. Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

## *Artikel 6da*

### Sikkerhedsbrud i europæiske digitale ID-tegnebøger

1. Hvis europæiske digitale ID-tegnebøger, der er leveret i henhold til artikel 6a, eller de valideringsmekanismer, der er omhandlet i artikel 6a, stk. 5, litra a), d) og e), er udsat for sikkerhedsbrud eller er delvist kompromitteret på en måde, som har indvirkning på deres pålidelighed eller andre europæiske digitale ID-tegnebøgers pålidelighed, suspenderer udstederen af de pågældende tegnebøger uden unødigt ophold udstedelsen og anvendelsen af den europæiske digitale ID-tegnebog. Den medlemsstat, hvor de pågældende tegnebøger blev leveret, underretter uden unødigt ophold medlemsstaterne og Kommissionen herom. Udstederen af de pågældende tegnebøger eller medlemsstaten underretter modtagerparterne og brugerne herom.

2. Når sikkerhedsbruddet eller kompromitteringen, jf. stk. 1, er afhjulpet, genoptager udstederen af tegnebogen udstedelsen og anvendelsen af den europæiske digitale ID-tegnebog. Den medlemsstat, hvor de pågældende tegnebøger blev leveret, underretter uden unødigt ophold medlemsstaterne og Kommissionen herom. Udstederen af de pågældende tegnebøger eller medlemsstaten underretter uden unødigt ophold modtagerparterne og brugerne herom.
3. Hvis sikkerhedsbruddet eller kompromitteringen, jf. stk. 1, ikke er afhjulpet senest tre måneder efter suspensionen, trækker den pågældende medlemsstat den pågældende europæiske digitale ID-tegnebog tilbage og underretter de øvrige medlemsstater og Kommissionen herom. Hvis det er begrundet i sikkerhedsbruddets alvorlighed, trækkes den pågældende europæiske digitale ID-tegnebog tilbage uden unødigt ophold.
4. Kommissionen offentliggør uden unødigt ophold de tilsvarende ændringer af den i artikel 6d omhandlede liste i Den Europæiske Unions Tidende.
5. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen de i stk. 1, 2 og 3 omhandlede foranstaltninger yderligere ved hjælp af en gennemførelsesretsakt om gennemførelse af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11. Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

## Artikel 6db

### Grænseoverskridende benyttelse af europæiske digitale ID-tegnebøger

1. Hvis medlemsstaterne kræver elektronisk identifikation ved hjælp af et elektronisk identifikationsmiddel og autentifikation for adgang til en onlinetjeneste, der udbydes af en offentlig myndighed, accepterer de også europæiske digitale ID-tegnebøger, der er leveret i overensstemmelse med denne forordning med henblik på autentifikation af brugeren.
2. Hvis private modtagerparter, der udbyder tjenester, med undtagelse af mikrovirksomheder og små virksomheder som defineret i Kommissionens henstilling 2003/361/EF, i henhold til national ret eller EU-retten er forpligtede til at anvende stærk brugerautentifikation til onlineidentifikation, eller hvis stærk brugerautentifikation 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, accepterer de private modtagerparter også, at der senest 12 måneder efter datoen for levering af europæiske digitale ID-tegnebøger i henhold til artikel 6a, stk. 1, og udelukkende efter brugerens frivillige anmodning anvendes europæiske digitale ID-tegnebøger, der er leveret i overensstemmelse med denne forordning, for så vidt angår de minimumsdata, der er nødvendige for den specifikke onlinetjeneste, for hvilken der anmodes om autentifikation af brugeren.
3. Hvis meget store onlineplatforme som defineret i artikel 25, stk. 1, i forordning [henvisning: forordningen om digitale tjenester] kræver, at brugerne autentificeres for at få adgang til onlinetjenester, accepterer de også, at der anvendes europæiske digitale ID-tegnebøger, der er leveret i overensstemmelse med denne forordning med henblik på autentifikation af brugeren, 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 tilskynder Kommissionen til og fremmer udviklingen af adfærdskodekser med henblik på at bidrage til en bred tilgængelighed og anvendelighed af europæiske digitale ID-tegnebøger inden for denne forordnings anvendelsesområde. Adfærdskodekserne skal fremme accepten af elektroniske identifikationsmidler, herunder europæiske digitale ID-tegnebøger, inden for denne forordnings anvendelsesområde, navnlig hos tjenesteudbydere, der benytter tredjeparters elektroniske identifikationstjenester til brugerautentifikation. Kommissionen fremmer udviklingen af sådanne adfærdskodekser i tæt samarbejde med alle relevante interessenter og tilskynder tjenesteudbydere til at færdiggøre udarbejdelsen af adfærdskodekser senest 12 måneder efter vedtagelsen af denne forordning og gennemføre dem effektivt senest 18 måneder efter vedtagelsen af denne forordning.
5. Kommissionen foretager senest 24 måneder efter indførelsen af de europæiske digitale ID-tegnebøger en vurdering på grundlag af dokumentation, der viser efterspørgslen efter og tilgængeligheden og anvendeligheden af europæiske digitale ID-tegnebøger, af, hvorvidt yderligere private udbydere af onlinetjenester skal pålægges at acceptere anvendelse af europæiske digitale ID-tegnebøger udelukkende efter frivillig anmodning fra brugeren. Vurderingskriterierne omfatter omfanget af brugerbasen, tjenesteudbydernes tilstedeværelse på tværs af grænserne, den teknologiske udvikling; udviklingen i forbrugsmønstre og forbrugerefterspørgslen."

8) Som overskrift indsættes før artikel 7:

"AFDELING II

ELEKTRONISKE IDENTIFIKATIONSORDNINGER".

9) Indledningen til artikel 7 affattes således:

"I henhold til artikel 9, stk. 1, skal medlemsstater, der endnu ikke har gjort det, senest 24 måneder efter ikrafttrædelsen af de i artikel 6a, stk. 11, og artikel 6c, stk. 4, omhandlede gennemførelsesretsakter anmelde mindst én elektronisk identifikationsordning, herunder mindst ét identifikationsmiddel med sikringsniveauet "høj". En elektronisk identifikationsordning kan anmeldes i henhold til artikel 9, stk. 1, hvis alle nedenstående betingelser er opfyldt:".

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

"2. Kommissionen offentliggør i Den Europæiske Unions Tidende en liste over de elektroniske identifikationsordninger, der er anmeldt i henhold til stk. 1 i nærværende artikel, med grundlæggende oplysninger om ordningerne.

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

12) Som artikel 11a indsættes:

*"Artikel 11a*

Matchning af registreringer

1. Når anmeldte elektroniske identifikationsmidler eller europæiske digitale ID-tegnebøger anvendes til autentifikation, sikrer medlemsstaterne, når de fungerer som modtagerparter, matchning af registreringer.

2. Med henblik på levering af europæiske digitale ID-tegnebøger medtager medlemsstaterne i det minimumssæt af personidentifikationsdata, der er omhandlet i artikel 12, stk. 4, litra d), mindst én entydig og vedvarende identifikator i overensstemmelse med EU-retten og national ret med henblik på at identificere brugeren efter anmodning i de tilfælde, hvor brugeridentifikation er krævet ved lov.
- 2a. Medlemsstaterne indfører tekniske og organisatoriske foranstaltninger for at sikre et højt beskyttelsesniveau for personoplysninger, der anvendes til matchning af registreringer, og for at forhindre profilering af brugere.
- 2aa. Medlemsstaterne kan i overensstemmelse med national ret fastsætte, at brugeren af europæiske digitale ID-tegnebøger skal kunne anmode om, at en entydig og vedvarende identifikator, der indgår i minimumssættet af personidentifikationsdata og er knyttet til tegnebogen i overensstemmelse med artikel 6a, stk. 4, litra e), erstattes af en anden entydig og vedvarende identifikator udstedt af medlemsstaten.
3. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen de i stk. 1 omhandlede foranstaltninger yderligere ved hjælp af en gennemførelsesretsakt. Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.
- 3a. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen de i stk. 2 og 2aa omhandlede foranstaltninger yderligere ved hjælp af en gennemførelsesretsakt. Gennemførelsesretsakten vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."



13) I artikel 12 foretages følgende ændringer:

#### Samarbejde og interoperabilitet

a) Stk. 3, litra d), udgår

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

"d) en henvisning til et minimumssæt af personidentifikationsdata, der er nødvendige for entydigt og vedvarende at repræsentere en fysisk eller juridisk person, eller en fysisk person, der repræsenterer fysiske eller juridiske personer".

ba) I stk. 5 indsættes følgende som litra c):

"c) en lignende tilgang til onlinetjenester, der accepterer brugen af europæiske digitale ID-tegnebøger, der leveres i overensstemmelse med denne forordning."

c) Stk. 6, litra a), affattes således:

"a) udvekslingen af oplysninger, erfaring og god praksis med hensyn til elektroniske identifikationsordninger og navnlig tekniske krav til interoperabilitet, matchning af registreringer og sikringsniveauer".

ca) I stk. 6 indsættes som litra e):

"e) udveksling af oplysninger, erfaringer og god praksis og udstedelse af retningslinjer for, hvordan onlinetjenester kan udformes, udvikles og gennemføres med henblik på at benytte de europæiske digitale tegnebøger."

14) Følgende indsættes som artikel 12a og 12b:

*"Artikel 12a*

Certificering af elektroniske identifikationsordninger

1. Elektroniske identifikationsordningers overensstemmelse med de krav, der er fastsat i denne forordning, certificeres for at påvise, at sådanne ordninger eller dele heraf opfylder kravene i artikel 8, stk. 2, vedrørende sikringsniveauerne for elektroniske identifikationsordninger inden for rammerne af en relevant cybersikkerhedscertificeringsordning i henhold til forordning (EU) 2019/881 eller dele heraf, for så vidt cybersikkerhedsattesten eller dele heraf omfatter de krav, der er fastsat i artikel 8, stk. 2, vedrørende sikringsniveauerne for elektroniske identifikationsordninger. Certificeringen må ikke overstige fem år på betingelse af en regelmæssig sårbarhedsvurdering hvert andet år. Hvis der konstateres sårbarheder, og disse ikke udbedres inden for tre måneder, annulleres certificeringen.

Certificeringen foretages af akkrediterede offentlige eller private overensstemmelsesvurderingsorganer, der er udpeget af medlemsstaterne, og i overensstemmelse med forordning (EF) nr. 765/2008.

2. Fagfællebedømmelsen (peerreview) af elektroniske identifikationsordninger, jf. artikel 12, stk. 6, litra c), finder ikke anvendelse på elektroniske identifikationsordninger eller dele af sådanne ordninger, der er certificeret i overensstemmelse med stk. 1.
- 2a. Uanset denne artikels stk. 2 kan medlemsstaterne anmode en anmeldende medlemsstat om yderligere oplysninger om elektroniske identifikationsordninger eller dele heraf, der er certificeret i henhold til denne artikels stk. 2.
3. Medlemsstaterne meddeler Kommissionen navn og adresse på de i stk. 1 omhandlede offentlige eller private organer. Kommissionen stiller disse oplysninger til rådighed for medlemsstaterne.

## Artikel 12b

### Adgang til hardware og softwarefunktioner

Udstedere af europæiske digitale ID-tegnebøger 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 forordning (EU) 2022/1925 med henblik på eller i forbindelse med levering af europæiske digitale ID-tegnebogstjenester og elektroniske identifikationsmidler til slutbrugere, er erhvervsbrugere i overensstemmelse med artikel 2, nr. 21), i forordning (EU) 2022/1925."

### 17) Artikel 13, stk. 1, affattes således:

"1. Uanset denne artikels stk. 2 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.

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 opstod uden forsæt eller uagtsomhed fra den pågældende kvalificerede tillidstjenesteudbyders side."

18) Artikel 14 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 de tillidstjenester, der har oprindelse i tredjelandet, eller den internationale organisation anerkendes i henhold til en gennemførelsesafgørelse eller en aftale, som er indgået mellem Unionen og tredjelandet eller en international organisation i overensstemmelse med traktatens artikel 218.
2. De i stk. 1 omhandlede gennemførelsesafgørelser og aftaler skal sikre, at tillidstjenesteudbydere i tredjelandet eller de internationale organisationer og de tillidstjenester, de udbyder, opfylder de krav, der gælder for kvalificerede tillidstjenesteudbydere, som er hjemmehørende i Unionen, og de kvalificerede tillidstjenester, de udbyder. Tredjelande og internationale organisationer opretter, ajourfører og offentliggør navnlig en positivliste over anerkendte tillidstjenesteudbydere.  
  
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.
3. De i stk. 1 omhandlede gennemførelsesafgørelser vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

19) Artikel 15 affattes således:

*"Artikel 15*

Tilgængelighed for personer med handicap

Leveringen af tillidstjenester og slutbrugerprodukter, der anvendes til levering af disse tjenester, gøres tilgængelig for personer med handicap i overensstemmelse med tilgængelighedskravene i direktiv 2019/882 om tilgængelighedskrav til produkter og tjenesteydelser."

20) I artikel 17 foretages følgende ændringer:

a) I stk. 4 foretages følgende ændringer:

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

"c) at underrette de i henhold til direktiv (EU) XXXX/XXXX [NIS 2] udpegede relevante nationale kompetente myndigheder i de berørte medlemsstater om alle væsentlige sikkerhedsbrud eller tab af integritet, som tilsynsorganet får kendskab til i forbindelse med udførelsen af sine opgaver. Hvis det væsentlige brud på sikkerheden eller det væsentlige tab af integritet vedrører andre medlemsstater, underretter tilsynsorganet den i henhold til direktiv (EU) XXXX/XXXX (NIS 2) udpegede kvikskranke i den berørte medlemsstat og de tilsynsorganer, der er udpeget i henhold til denne forordnings artikel 17, i de øvrige berørte medlemsstater. Det underrettede tilsynsorgan skal også informere offentligheden eller kræve, at tillidstjenesteudbyderen gør det, hvis det fastslår, at det er i offentlighedens interesse, at et brud på sikkerheden eller tab af integritet offentliggøres."

2) Litra f) affattes således:

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

b) Stk. 6 affattes således:

"6. Senest den 31. marts hvert år forelægger tilsynsorganerne Kommissionen en rapport om det foregående kalenderårs primære tilsynsvirksomhed."

c) Stk. 8 affattes således:

"8. Senest 12 måneder efter denne forordnings ikrafttræden vedtager Kommissionen retningslinjer for tilsynsorganernes udførelse af de i stk. 4 omhandlede opgaver og fastlægger ved hjælp af gennemførelsesretsakter vedtaget efter undersøgelsesproceduren i artikel 48, stk. 2, formater og procedurer for den i stk. 6 omhandlede rapport."

21) I artikel 18 foretages følgende ændringer:

a) Overskriften til artikel 18 affattes således:

"Gensidig bistand og samarbejde".

b) Stk. 1 affattes således:

"1. Tilsynsorganerne samarbejder med henblik på at udveksle god praksis og oplysninger vedrørende levering af tillidstjenester."

c) Som stk. 4 og 5 tilføjes:

- "4. Tilsynsorganer og nationale kompetente myndigheder i henhold til Europa-Parlamentets og Rådets direktiv (EU) XXXX/XXXX [NIS 2] samarbejder og bistår hinanden for at sikre, at tillidstjenesteudbydere opfylder de krav, der er fastsat i denne forordning og i direktiv (EU) XXXX/XXXX [NIS 2]. Tilsynsorganer anmoder de i henhold til direktiv XXXX/XXXX [NIS 2] nationale kompetente myndigheder om at gennemføre tilsynsforanstaltninger for at kontrollere, at tillidstjenesteudbydere overholder kravene i direktiv XXXX/XXXX (NIS 2), kræve, at tillidstjenesteudbydere udbedrer enhver manglende overholdelse af disse krav, levere rettidige resultater for alle tilsynsaktiviteter vedrørende tillidstjenesteudbydere og underrette tilsynsorganerne om relevante hændelser, der er anmeldt i overensstemmelse med direktiv XXXX/XXXX [NIS 2].
5. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter de proceduremæssige ordninger for fremme af samarbejdet mellem de i stk. 1 omhandlede tilsynsmyndigheder. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

21a) Som artikel 19a indsættes:

"Krav til ikkekvalificerede tillidstjenesteudbydere

1. En ikkekvalificeret tillidstjenesteudbyder, der udbyder ikkekvalificerede tillidstjenester, skal:
  - a) indføre en passende politik og træffe tilsvarende foranstaltninger til at styre juridiske, erhvervsmæssige, operationelle og andre direkte eller indirekte risici i forbindelse med leveringen af den ikkekvalificerede tillidstjeneste. Uanset bestemmelserne i artikel 18 i direktiv EU XXXX/XXX [NIS 2] omfatter disse foranstaltninger som minimum følgende:
    - i) foranstaltninger vedrørende registrerings- og onboardingprocedurer for en tjeneste
    - ii) foranstaltninger vedrørende proceduremæssig eller administrativ kontrol
    - iii) foranstaltninger vedrørende forvaltning og gennemførelse af tjenester
  - b) hurtigst muligt og under alle omstændigheder senest 24 timer efter at være blevet opmærksomme på forholdet underrette tilsynsorganet, de identificerbare berørte personer, offentligheden, hvis det er i offentlighedens interesse, og, hvis det er relevant, andre relevante kompetente organer om eventuelle sikkerhedsbrud eller forstyrrelser i leveringen af tjenesten eller gennemførelsen af de foranstaltninger, der er omhandlet i litra a), nr. i), ii) og iii), som har en betydelig indvirkning på den tillidstjeneste, der udbydes, eller på de personoplysninger, der opbevares deri.
2. Senest 12 måneder efter denne forordnings ikrafttræden præciserer Kommissionen ved hjælp af gennemførelsesretsakter de tekniske kendetegn ved de foranstaltninger, der er omhandlet i stk. 1, litra a). Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2."



22) 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 18 i direktiv Directive (EU) XXXX/XXXX [NIS 2]. Kvalificerede tillidstjenesteudbydere forelægger den resulterende overensstemmelsesvurderingsrapport for tilsynsorganet senest tre arbejdsdage efter modtagelsen heraf."

aa) Følgende stykke indsættes:

"1a. Medlemsstaterne kan fastsætte, at kvalificerede tillidstjenesteudbydere på forhånd skal underrette tilsynsorganet om planlagte kontroller og efter anmodning give tilsynsorganet mulighed for at deltage som observatør."

b) I stk. 2 affattes sidste punktum således:

"Ved mistanke om overtrædelse af reglerne om beskyttelse af personoplysninger underretter tilsynsorganet uden unødigt ophold de kompetente tilsynsmyndigheder i henhold til forordning (EU) 2016/679 om resultaterne af kontrolundersøgelserne."

c) Stk. 3 og 4 erstattes af:

"3. Hvis den kvalificerede tillidstjenesteudbyder ikke opfylder 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, hvis det er relevant, inden for den frist, der er fastsat af tilsynsorganet, kan tilsynsorganet under hensyntagen til navnlig omfanget, varigheden og konsekvenserne af manglen tilbagetrække den pågældende tjenesteudbyders eller den berørte tjenestes status som kvalificeret.

3a. Hvis tilsynsorganet af de kompetente nationale myndigheder i henhold til direktiv (EU) XXXX/XXXX [NIS 2] underrettes om, at den kvalificerede tillidstjenesteudbyder ikke opfylder de krav, der er fastsat i artikel 18 i direktiv (EU) XXXX/XXXX [NIS 2], kan tilsynsorganet under hensyntagen til navnlig omfanget, varigheden og konsekvenserne af manglen tilbagetrække den pågældende tjenesteudbyders eller den berørte tjenestes status som kvalificeret.

3b. Hvis tilsynsorganet af tilsynsmyndighederne i henhold til forordning (EU) 2016/679 underrettes om, at den kvalificerede tillidstjenesteudbyder ikke opfylder de krav, der er fastsat i forordning (EU) 2016/679, kan tilsynsorganet under hensyntagen til navnlig omfanget, varigheden og konsekvenserne af manglen tilbagetrække den pågældende tjenesteudbyders eller den 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 i artikel 22, stk. 3, omhandlede organ med henblik på ajourføring af positivlisterne, jf. artikel 22, stk. 1, og den kompetente nationale myndighed, jf. direktiv XXXX [NIS 2].
4. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder med henblik på følgende:
- a) akkreditering af overensstemmelsesvurderingsorganerne og for overensstemmelsesvurderingsrapporten, jf. stk. 1
  - b) revisionskrav, i henhold til hvilke overensstemmelsesvurderingsorganerne foretager overensstemmelsesvurderinger af kvalificerede tillidstjenesteudbydere, jf. stk. 1
  - c) overensstemmelsesvurderingsordninger for overensstemmelsesvurderingsorganernes overensstemmelsesvurdering af de kvalificerede tillidstjenesteudbydere og for udarbejdelse af rapporten, jf. stk. 1.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

23) I artikel 21 foretages følgende ændringer:

"1. Ønsker en tillidstjenesteudbyder at udbyde kvalificerede tillidstjenester, skal tjenesteudbyderen anmelde sin hensigt til tilsynsorganet og indsende en overensstemmelsesvurderingsrapport udstedt af et overensstemmelsesvurderingsorgan, der bekræfter, at kravene i denne forordning og i artikel 18 i direktiv (EU) XXXX/XXXX [NIS 2] er opfyldt."

a) Stk. 2 affattes således:

"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 disses kvalificerede tillidstjenester.

For at kontrollere, at tillidstjenesteudbyderen opfylder de krav, der er fastsat i artikel 18 i direktiv XXXX [NIS 2], anmoder tilsynsorganet de kompetente myndigheder, der er omhandlet i direktiv XXXX [NIS 2], om at gennemføre tilsynsforanstaltninger med dette formål og fremlægge oplysninger om resultatet uden unødigt ophold og senest to måneder efter modtagelsen af denne anmodning fra de kompetente myndigheder, der er omhandlet i direktiv XXXX [NIS 2]. Er kontrollen ikke afsluttet inden to måneder efter anmeldelsen, underretter de kompetente myndigheder, der er omhandlet i direktiv XXXX [NIS 2], 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, jf. stk. 1 i nærværende artikel, det i artikel 22, stk. 3, omhandlede organ med henblik på ajourføring af positivlisterne, jf. artikel 22, stk. 1.

Er kontrollen ikke afsluttet senest tre måneder efter anmeldelsen, underretter tilsynsorganet tillidstjenesteudbyderen herom og forklarer årsagerne til forsinkelsen samt oplyser, hvornår kontrollen afsluttes."

b) Stk. 4 affattes således:

"4. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter formater og procedurer for anmeldelse og kontrol med henblik på stk. 1 og 2. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

25) I artikel 24 foretages følgende ændringer:

a) Stk. 1 affattes således:

"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.

De i første afsnit omhandlede oplysninger kontrolleres af den kvalificerede tillidstjenesteudbyder enten direkte eller via en tredjemand på enhver af følgende måder:

- a) ved hjælp af den europæiske digitale ID-tegnebog eller et anmeldt elektronisk identifikationsmiddel, der opfylder de krav, der er fastsat i artikel 8 med hensyn til sikringsniveauet "høj"
- b) ved hjælp af kvalificerede elektroniske attesteringer af attributter eller et certifikat for en kvalificeret elektronisk signatur eller for et kvalificeret elektronisk segl, der er udstedt i overensstemmelse med 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 procedurer og i overensstemmelse med national ret."

b) Som stk. 1a indsættes:

"1a. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske minimumsspecifikationer, -standarder og -procedurer med hensyn til kontrol af identitet og attributter i overensstemmelse med stk. 1, litra c). Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

c) I stk. 2 foretages følgende ændringer:

0) Litra a) affattes således:

"a) informere tilsynsorganet mindst en måned, før der gennemføres ændringer i udbuddet af dennes kvalificerede tillidstjenester eller mindst tre måneder, hvis det er hensigten at ophøre med denne virksomhed. Tilsynsorganet kan anmode om yderligere oplysninger eller resultatet af en overensstemmelsesvurdering, inden det giver tilladelse 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".

1) 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 algoritmer, nøglelængder og hashfunktioner i de systemer, produkter og processer, der understøttes af dem".

2) Som litra fa) og fb) indsættes:

- "fa) indføre en passende politik og træffe tilsvarende foranstaltninger til at styre juridiske, erhvervsmæssige, operationelle og andre direkte eller indirekte risici i forbindelse med leveringen af den kvalificerede tillidstjeneste. Uanset bestemmelserne i artikel 18 i direktiv EU XXXX/XXX [NIS 2] omfatter disse foranstaltninger som minimum følgende:
- i) foranstaltninger vedrørende registrerings- og onboardingprocedurer for en tjeneste
  - ii) foranstaltninger vedrørende proceduremæssig eller administrativ kontrol
  - iii) foranstaltninger vedrørende forvaltning og gennemførelse af tjenester



fb) hurtigst muligt og under alle omstændigheder senest 24 timer efter hændelsen underrette tilsynsorganet, de identificerbare berørte personer, 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) og iii), som har en betydelig indvirkning på den tillidstjeneste, der udbydes, eller på de personoplysninger, der opbevares heri".

3) Litra g) og h) 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 tillidstjenesteudbyders aktiviteter er ophørt, registrere og til rådighed stille alle relevante oplysninger om de data, den kvalificerede tillidstjenesteudbyder har udstedt og modtaget, for at kunne fremlægge bevis i retssager og for at garantere tjenestens kontinuitet. Denne registrering kan ske elektronisk".

4) Litra j) udgår.

d) Som stk. 4a indsættes:

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

e) Stk. 5 affattes således:

"5. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer, procedurer og referencenumre for standarder for de krav, der er omhandlet i stk. 2. Det formodes, at kravene i nærværende artikel overholdes, når disse tekniske specifikationer, procedurer og standarder er opfyldt. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

f) Som stk. 6 indsættes:

"6. Kommissionen tillægges beføjelser til at vedtage gennemførelsesretsakter, der præciserer de tekniske kendetegn ved de i stk. 2, litra fa), omhandlede foranstaltninger."

25a) I artikel 26 foretages følgende ændringer:

"2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for avancerede elektroniske signaturer. En avanceret elektronisk signatur, der opfylder disse specifikationer og standarder, formodes at overholde kravene til avancerede elektroniske signaturer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2."

25b) I artikel 27 foretages følgende ændringer:

Stk. 4 udgår.

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

"6. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for kvalificerede certifikater for elektroniske signaturer. Et kvalificeret certifikat for elektronisk signatur, der opfylder disse specifikationer og standarder, formodes at overholde kravene i bilag I. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

27) I artikel 29 tilføjes som stk. 1a:

"1a. Generering og forvaltning af elektroniske signaturgenereringsdata på underskriverens vegne eller kopiering af sådanne signaturgenereringsdata til backupformål må kun foretages af en kvalificeret tillidstjenesteudbyder, der leverer en kvalificeret tillidstjeneste til forvaltning af et kvalificeret elektronisk system til signaturgenerering på afstand."

28) Som artikel 29a indsættes:

*"Artikel 29a*

Krav til kvalificerede tjenester til forvaltning af kvalificerede elektroniske systemer til signaturgenerering på afstand

1. Forvaltning af kvalificerede elektroniske systemer til signaturgenerering 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), kun kan kopiere de elektroniske signaturgenereringsdata til backupformål, forudsat at følgende krav er opfyldt:
    - i. der opretholdes samme niveau af sikkerhed for 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 system til signaturgenerering på afstand, der er udstedt i henhold til artikel 30.
2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder med henblik på stk. 1."

29) I artikel 30 indsættes som stk. 3a:

"3a. Gyldigheden af den i stk. 1 omhandlede certificering må ikke overstige fem år på betingelse af en regelmæssig sårbarhedsvurdering hvert andet år. Hvis der konstateres sårbarheder, og disse ikke udbedres, annulleres certificeringen."

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

"3. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter formater og procedurer, der finder anvendelse med henblik på stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

31) I artikel 32 foretages følgende ændringer:

a) I stk. 1 tilføjes følgende afsnit:

"En validering af kvalificerede elektroniske signaturer, der opfylder de i stk. 3 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i første afsnit."

b) Stk. 3 affattes således:

"3. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter specifikationer og referencenumre for standarder for validering af kvalificerede elektroniske signaturer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

31a) Som artikel 32a indsættes:

"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 bekræfter gyldigheden af en avanceret elektronisk signatur, der er baseret på et kvalificeret certifikat, forudsat at:

- a) det certifikat, der støtter signaturen, på underskriftstidspunktet var et kvalificeret certifikat for elektronisk signatur, der var i overensstemmelse med 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, såfremt der på underskriftstidspunktet blev anvendt et pseudonym
- f) de underskrevne datas integritet ikke er bragt i fare
- g) kravene i artikel 26 var opfyldt på underskriftstidspunktet. En validering af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater, og som opfylder de i stk. 3 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i første afsnit.
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 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter specifikationer og referencenumre for standarder for validering af avancerede elektroniske signaturer, der er baseret på kvalificerede certifikater. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

31b) I artikel 33 foretages følgende ændringer:

- "1. En kvalificeret valideringstjeneste for kvalificerede elektroniske signaturer må kun stilles til rådighed af en kvalificeret tillidstjenesteudbyder, der".
- "2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for den i stk. 1 omhandlede kvalificerede valideringstjeneste. En valideringstjeneste for en kvalificeret elektronisk signatur, der opfylder disse specifikationer og standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

32) Artikel 34 affattes således:

*"Artikel 34*

Kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer

1. Kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer udbydes kun af kvalificerede tillidstjenesteudbydere, der anvender procedurer og teknologier, der gør det muligt at forlænge pålideligheden af den kvalificerede elektroniske signatur ud over den teknologiske gyldighedsperiode.
2. Ordninger for kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer, der opfylder de i stk. 3 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i stk. 1.
3. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for kvalificerede tjenester til bevaring af elektroniske signaturer. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

32a) I artikel 36 tilføjes som nyt stk. 2:

"2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for avancerede elektroniske segl.

Et avanceret elektronisk segl, der opfylder disse specifikationer og standarder, formodes at overholde kravene til avancerede elektroniske segl. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

33) I artikel 37 foretages følgende ændringer:

Stk. 4 udgår.

34) I artikel 38 foretages følgende ændringer:

a) Stk. 1 affattes således:

"1. Kvalificerede certifikater for elektronisk segl opfylder de krav, der er fastsat i bilag III. Et kvalificeret certifikat for elektronisk segl, der opfylder de i stk. 6 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i bilag III."

b) Stk. 6 affattes således:

"6. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for kvalificerede certifikater for elektroniske sejl. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."



35) Som artikel 39a indsættes:

*"Artikel 39a*

Krav til kvalificerede tjenester til forvaltning af kvalificerede elektroniske systemer til sejlgenerering på afstand

Artikel 29a finder tilsvarende anvendelse på kvalificerede tjenester til forvaltning af kvalificerede elektroniske systemer til sejlgenerering på afstand."

35a) Som artikel 40a indsættes:

*"Artikel 40a*

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

(1) Artikel 32a finder tilsvarende anvendelse på validering af avancerede elektroniske sejl, der er baseret på kvalificerede certifikater."

36) I artikel 42 foretages følgende ændringer:

a) Som stk. 1a indsættes:

"1a. Forbindelser af dato og tidspunkt med data og den nøjagtige tidskilde, der opfylder de i stk. 2 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i stk. 1."

b) Stk. 2 affattes således:

"2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for forbindelser af dato og tidspunkt med data og for nøjagtige tidskilder. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

36a) I artikel 43 tilføjes som nyt stk. 3:

"2a. En kvalificeret elektronisk registreret leveringstjeneste i en medlemsstat anerkendes som en kvalificeret elektronisk registreret leveringstjeneste i enhver anden medlemsstat."

37) I artikel 44 foretages følgende ændringer:

a) Som stk. 1a indsættes:

"1a. En dataafsendelses- og -modtagelsesproces, der opfylder de i stk. 2 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i stk. 1."

b) Stk. 2 affattes således:

"2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for dataafsendelses- og -modtagelsesprocesser. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

c) Som stk. 3 og 4 indsættes:

"3. Udbydere af kvalificerede elektroniske registrerede leveringstjenester kan nå til enighed om interoperabiliteten mellem de kvalificerede elektroniske registrerede leveringstjenester, som de udbyder. En sådan interoperabilitetsramme skal opfylde kravene i stk. 1. Opfyldelsen skal bekræftes af et overensstemmelsesvurderingsorgan.

4. Kommissionen kan ved hjælp af gennemførelsesretsakter fastsætte tekniske specifikationer og referencenumre for standarder for at lette overførslen af data mellem to eller flere kvalificerede tillidstjenesteudbydere. Standardernes tekniske specifikationer og indhold skal være omkostningseffektive og forholdsmæssige. Gennemførelsesretsakterne vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

38) Artikel 45 affattes således:

*"Artikel 45*

#### Krav til kvalificerede certifikater for webstedsautentifikation

1. Kvalificerede certifikater for webstedsautentifikation opfylder de krav, der er fastsat i bilag IV. Der foretages en evaluering af opfyldelsen af de krav, der er fastsat i bilag IV, i overensstemmelse med de specifikationer og standarder, der er omhandlet i stk. 4.
2. De i stk. 1 omhandlede kvalificerede certifikater for webstedsautentifikation anerkendes af webbrowsere. Med henblik herpå sikrer webbrowsere, at de identitetsdata, der opgives ved hjælp af enhver af metoderne, vises på en brugervenlig måde. Webbrowsere sikrer støtte af og interoperabilitet med kvalificerede certifikater for webstedsautentifikation som omhandlet i stk. 1 med undtagelse af virksomheder, der betragtes som mikrovirksomheder eller små virksomheder i overensstemmelse med Kommissionens henstilling 2003/361/EF i de første fem år, hvor de fungerer som udbydere af webbrowser-tjenester.
4. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter specifikationer og referencenumre for standarder for de i stk. 1 og 2 omhandlede kvalificerede certifikater for websideautentifikation. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

39) Efter artikel 45 indsættes som afdeling 9, 10 og 11:

"AFDELING 9

ELEKTRONISK ATTESTERING AF ATTRIBUTTER

*Artikel 45a*

Retsvirkninger af elektronisk attestering af attributter

1. Retsvirkning og anerkendelse som bevis i retssager af elektroniske attesteringer af attributter nægtes ikke 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 kvalificeret elektronisk attestering af attributter, der er udstedt i en medlemsstat, anerkendes som en kvalificeret elektronisk attestering af attributter i enhver anden medlemsstat.
4. En attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, 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 45b*

##### Elektronisk attestering af attributter i offentlige tjenester

Når 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 45c*

##### Krav til kvalificeret elektronisk attestering af attributter

1. Kvalificeret elektronisk attestering af attributter opfylder de krav, der er fastsat i bilag V.
  - 1a. Der foretages en evaluering af opfyldelsen af de krav, der er fastsat i bilag V, i overensstemmelse med de specifikationer og standarder, der er omhandlet i stk. 4.
2. Kvalificerede elektroniske attesteringer af attributter er ikke omfattet af ufravigelige krav ud over de krav, der er fastsat i bilag V.
3. 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.
4. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen tekniske specifikationer og referencenumre for standarder for kvalificerede elektroniske attesteringer af attributter ved hjælp af en gennemførelsesretsakt om gennemførelse af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11.

#### *Artikel 45d*

##### Kontrol af attributter mod autentiske kilder

1. Medlemsstaterne sikrer senest 24 måneder efter ikrafttrædelsen af de i artikel 6a, stk. 11, og artikel 6c, stk. 4, omhandlede gennemførelsesretsakter, at der i det mindste for de i bilag VI anførte attributter, når disse er afhængige af autentiske kilder i den offentlige sektor, træffes foranstaltninger til at gøre det muligt for kvalificerede udbydere af elektroniske attesteringer af attributter ved hjælp af elektroniske midler at kontrollere disse attributter efter anmodning fra brugeren og i overensstemmelse med national ret eller EU-retten.
2. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen under hensyntagen til relevante internationale standarder de tekniske minimumsspecifikationer, -standarder og -procedurer med henvisning til kataloget over attributter og ordninger for attesting af attributter og kontrolprocedurer for kvalificerede elektroniske attesteringer af attributter ved hjælp af en gennemførelsesretsakt om gennemførelse af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11.

#### *Artikel 45da*

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

1. En elektronisk attesting af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, skal opfylde følgende krav:
  - a) kravene i bilag VII

b) det kvalificerede certifikat, der støtter den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl fra den i artikel 3, nr. 45a), omhandlede offentlige myndighed, der er identificeret som udsteder, jf. bilag VII, litra b), skal indeholde 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 national ret eller EU-retten 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 nationale ret eller EU-ret.

2. Den medlemsstat, hvor de i artikel 3, nr. 45a), omhandlede offentlige myndigheder er etableret, sikrer, at de offentlige myndigheder, der udsteder elektroniske attesteringer af attributter, har samme pålidelighedsniveau som kvalificerede tillidstjenesteudbydere i overensstemmelse med artikel 24.

2a. Medlemsstaterne underretter Kommissionen om de i artikel 3, nr. 45a), 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. 45a), til rådighed for offentligheden via en sikker kommunikationsforbindelse og i en elektronisk underskrevet eller forsejlet form, der egner sig til automatiseret behandling.

3. 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. Efter tilbagekaldelsen kan den tilbagekaldte status for en elektronisk attestering ikke genetableres.

4. 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 være i overensstemmelse med kravene i denne artikels stk. 1, hvis den opfylder de i stk. 5 omhandlede standarder.

5. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen tekniske specifikationer og referencenumre for standarder for elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, ved hjælp af en gennemførelsesretsakt om gennemførelse af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11.

5a. Senest seks måneder efter denne forordnings ikrafttræden fastsætter Kommissionen formater, procedurer, specifikationer og standarder med henblik på stk. 2a ved hjælp af en gennemførelsesretsakt om gennemførelse af europæiske digitale ID-tegnebøger som omhandlet i artikel 6a, stk. 11.

6. De i artikel 3, nr. 45a), omhandlede offentlige myndigheder, der udsteder elektronisk attestering af attributter, stiller en grænseflade med europæiske digitale ID-tegnebøger, der er leveret i overensstemmelse med artikel 6a, til rådighed.



#### *Artikel 45e*

Udstedelse af elektroniske attesteringer af attributter til europæiske digitale ID-tegnebøger

Udbydere af kvalificerede elektroniske attesteringer af attributter stiller en grænseflade med europæiske digitale ID-tegnebøger, der er leveret i overensstemmelse med artikel 6a, til rådighed.

#### *Artikel 45f*

Supplerende regler for levering af tjenester til elektronisk attestering af attributter

1. Udbydere af kvalificerede og ikkekvalificerede tjenester til elektronisk attestering af attributter kombinerer ikke 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.
4. Udbydere af tjenester til elektronisk attestering af attributter gennemfører funktionel adskillelse med henblik på levering af sådanne tjenester.

## AFDELING 10

### ELEKTRONISKE ARKIVERINGSTJENESTER

#### *Artikel 45g*

##### Retsvirkning af en elektronisk arkiveringstjeneste

1. Elektroniske data, der er lagret ved hjælp af en elektronisk arkiveringstjeneste, må ikke nægtes retsvirkning og anerkendelse som bevismateriale under retssager alene af den grund, at de er i elektronisk form, eller at de ikke er lagret ved hjælp af en kvalificeret elektronisk arkiveringstjeneste.
2. Elektroniske data, der er lagret ved hjælp af en kvalificeret elektronisk arkiveringstjeneste, formodes af den kvalificerede tillidstjenesteudbyder at have deres integritet og oprindelse i hele opbevaringsperioden.
3. En kvalificeret elektronisk arkiveringstjeneste i en medlemsstat anerkendes som en kvalificeret elektronisk arkiveringstjeneste i enhver anden medlemsstat.

#### *Artikel 45ga*

##### 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 forlænge de elektroniske datas holdbarhed og læsbarhed ud over den teknologiske gyldighedsperiode og i det mindste i den lovbestemte eller kontraktlige opbevaringsperiode, samtidig med at deres integritet og oprindelse bevares.

- c) De sikrer, at de elektroniske data 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, der hentes fra et kvalificeret elektronisk arkiv, er omfattet af formodningen om dataenes integritet fra begyndelsen af opbevaringsperioden til det tidspunkt, hvor de hentes. Denne rapport leveres på en pålidelig og effektiv måde og er forsynet med den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl fra udbyderen af den kvalificerede elektroniske arkiveringstjeneste.
2. Senest 12 måneder efter denne forordnings ikrafttræden fastsætter Kommissionen ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for kvalificerede elektroniske arkiveringstjenester. En kvalificeret elektronisk arkiveringstjeneste, der opfylder disse specifikationer og standarder, formodes at overholde kravene til kvalificerede elektroniske arkiveringstjenester. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 48, stk. 2.

## AFDELING 11

### ELEKTRONISKE HOVEDBØGER

#### *Artikel 45h*

##### Retsvirkninger af elektroniske hovedbøger

1. Retsvirkning og anerkendelse som bevis i retssager af elektroniske hovedbøger nægtes ikke 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 deres integritet.
3. En kvalificeret elektronisk hovedbog i en medlemsstat anerkendes som en kvalificeret elektronisk hovedbog i enhver anden medlemsstat.

#### *Artikel 45i*

##### Krav til kvalificerede elektroniske hovedbøger

1. Kvalificerede elektroniske hovedbøger opfylder følgende krav:
  - a) De er oprettet af en eller flere kvalificerede tillidstjenesteudbydere.
  - b) De fastlægger oprindelsen af dataposter i hovedbogen.
  - c) De sikrer en entydig kronologisk rækkefølge af dataposter i hovedbogen.
  - d) De registrerer data på en sådan måde, at enhver efterfølgende ændring af dataene straks kan opdages, hvorved deres integritet løbende sikres.

2. En elektronisk hovedbog, der opfylder de i stk. 3 omhandlede specifikationer og standarder, formodes at overholde de krav, der er fastsat i stk. 1.
3. Kommissionen fastsætter ved hjælp af gennemførelsesretsakter tekniske specifikationer og referencenumre for standarder for oprettelse og drift af en kvalificeret elektronisk hovedbog. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2."

40) Som artikel 48a indsættes:

*"Artikel 48a*

#### Rapporteringskrav

1. Medlemsstaterne sikrer indsamling af statistikker vedrørende funktionen af europæiske digitale ID-tegnebøger, når de er leveret på deres område.
2. De statistikker, der indsamles i henhold til stk. 1, omfatter følgende:
  - a) antallet af fysiske og juridiske personer, der har en gyldig europæisk digital ID-tegnebog
  - b) typen og antallet af tjenester, der accepterer anvendelse af den europæiske digitale ID-tegnebog
  - c) sammenfattende rapport, herunder data om hændelser, som forhindrer anvendelse af den europæiske digitale ID-tegnebog.
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 henhold til stk. 2."

41) Artikel 49 affattes således:

*"Artikel 49*

Revision

1. Kommissionen reviderer anvendelsen af denne forordning og aflægger rapport til Europa-Parlamentet og Rådet senest 36 måneder efter forordningens ikrafttræden. Kommissionen evaluerer navnlig anvendelsesområdet for artikel 6 og 6db, og hvorvidt det er hensigtsmæssigt at ændre denne forordnings anvendelsesområde eller de specifikke bestemmelser heri, under hensyntagen til de erfaringer, der er gjort med anvendelsen af denne forordning, samt kundernes efterspørgsel og den teknologiske, markedsmæssige og retlige udvikling. Rapporten ledsages om nødvendigt af et forslag til ændring af denne forordning.
2. Evalueringsrapporten indeholder en vurdering af tilgængeligheden og anvendeligheden af europæiske digitale ID-tegnebøger, der er omfattet af denne forordnings anvendelsesområde, og hvorvidt alle private onlinetjenesteudbydere, der benytter tredjeparters elektroniske identifikationstjenester til autentifikation af brugere, skal pålægges at acceptere anvendelse af europæiske digitale ID-tegnebøger.
3. Kommissionen forelægger endvidere hvert fjerde år efter udarbejdelsen af den i stk. 1 omhandlede rapport Europa-Parlamentet og Rådet en rapport om de fremskridt, der er gjort med hensyn til opfyldelse af målene for denne forordning."

42) Artikel 51 affattes således:

*"Artikel 51*

Overgangsforanstaltninger

1. Sikre signaturgenereringssystemer, for hvilke det er fastslået, at de opfylder kravene i artikel 3, stk. 4, i direktiv 1999/93/EF, betragtes fortsat som kvalificerede elektroniske signaturgenereringssystemer i henhold til denne forordning i 36 måneder efter denne forordnings ikrafttræden.
2. Kvalificerede certifikater, der er udstedt til fysiske personer i henhold til direktiv 1999/93/EF, betragtes fortsat som kvalificerede certifikater for elektroniske signaturer i henhold til denne forordning i 24 måneder efter denne forordnings ikrafttræden.
  - 2a. Den forvaltning af kvalificerede elektroniske systemer til signatur- og seglgenerering på afstand, der foretages af andre kvalificerede tillidstjenesteudbydere end kvalificerede tillidstjenesteudbydere, der leverer kvalificerede tillidstjenester til forvaltning af kvalificerede elektroniske systemer til signatur- og seglgenerering på afstand, jf. artikel 29a og 39a, tages fortsat i betragtning, uden at det er nødvendigt at opnå status som kvalificeret med hensyn til levering af disse forvaltningstjenester i 24 måneder efter denne forordnings ikrafttræden.
  - 2b. Kvalificerede tillidstjenesteudbydere, der har fået deres status som kvalificeret i henhold til denne forordning inden den [datoen for ændringsforordningens ikrafttræden], forelægger ved hjælp af metoder til identitetskontrol med henblik på udstedelse af kvalificerede certifikater i overensstemmelse med artikel 24, stk. 1, så hurtigt som muligt og senest 30 måneder efter ændringsforordningens ikrafttræden tilsynsorganet en overensstemmelsesvurderingsrapport, der dokumenterer overensstemmelsen med artikel 24, stk. 1. Indtil forelæggelsen af en sådan overensstemmelsesvurderingsrapport og tilsynsorganets gennemførelse af sin vurdering kan den kvalificerede tillidstjenesteudbyder fortsat anvende de metoder til identitetskontrol, der er fastsat i artikel 24, stk. 1, i forordning (EU) nr. 910/2014."

- 43) Bilag I ændres som angivet i bilag I til denne forordning.
- 44) Bilag II affattes som angivet i bilag II til denne forordning.
- 45) Bilag III ændres som angivet i bilag III til denne forordning.
- 46) Bilag IV ændres som angivet i bilag IV til denne forordning.
- 47) Der tilføjes et nyt bilag V som angivet i bilag V til denne forordning.
- 48) Der tilføjes et nyt bilag VI til denne forordning.

#### *Artikel 52*

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 [...].

På Europa-Parlamentets vegne

På Rådets vegne

Formand

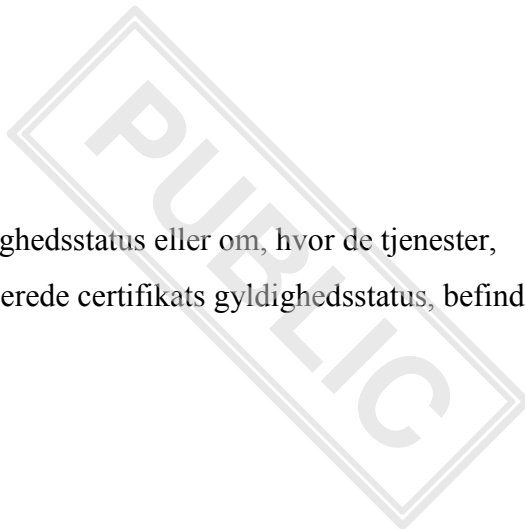
Formand



## BILAG I

I bilag I affattes litra i) således:

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



## BILAG II

### KRAV TIL KVALIFICEREDE ELEKTRONISKE SIGNATURGENERERINGSSYSTEMER

1. Kvalificerede elektroniske signaturgenereringssystemer sikrer ved hjælp af passende tekniske og proceduremæssige midler som minimum, at:
  - a) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, med rimelig sikkerhed forbliver fortrolige
  - b) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, i praksis kun kan forekomme en gang
  - c) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, med rimelig sikkerhed ikke kan udledes, og at den elektroniske signatur på pålidelig vis er beskyttet mod forfalskning under anvendelse af eksisterende teknologi
  - d) de elektroniske signaturgenereringsdata, der anvendes til elektronisk signaturgenerering, på pålidelig vis kan beskyttes af den retmæssige underskriver mod andres brug.
2. Kvalificerede elektroniske signaturgenereringssystemer hverken ændrer de data, som skal underskrives, eller hindrer, at disse data vises for underskriveren forud for signaturprocessen.

## BILAG III

I bilag III affattes litra i) således:

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

## BILAG IV

I bilag IV affattes litra j) således:

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

## BILAG V

### KRAV TIL KVALIFICERET ATTESTERING AF ATTRIBUTTER

Kvalificeret elektronisk attestering af attributter indeholder:

- e) 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
  
- f) 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
  - for en juridisk person: navn og, når det er relevant, registreringsnummer, som det fremgår af det officielle register
  - for en fysisk person: personens navn
  
- g) et sæt data, der entydigt repræsenterer den enhed, som de attesterede attributter henviser til; anvendes der pseudonym, er dette tydeligt angivet
  
- h) den attesterede attribut eller de attesterede attributter, herunder, hvis det er relevant, de oplysninger, der er nødvendige for at bestemme attributternes omfang
  
- i) oplysninger om attesteringens ikrafttrædelses- og udløbsdato

- j) attesteringens identifikationskode, som skal være entydig for den kvalificerede tillidstjenesteudbyder, og, hvis det er relevant, attesteringsordningen, som attesteringen er en del af
- k) den udstedende kvalificerede tillidstjenesteudbyders kvalificerede elektroniske signatur eller kvalificerede elektroniske segl
- l) oplysninger om, hvor certifikatet for den kvalificerede elektroniske signatur eller det kvalificerede elektroniske segl, der henvises til i litra g), er gratis tilgængeligt
- m) oplysninger om den kvalificerede attesteringens gyldighedsstatus eller om, hvor de tjenester, hvortil der kan rettes forespørgsel om den kvalificerede attesteringens gyldighedsstatus, befinder sig.

## BILAG VI

### MINIMUMSLISTE OVER ATTRIBUTTER

Medlemsstaterne sikrer, at der træffes foranstaltninger til at gøre det muligt for kvalificerede udbydere af elektroniske attesteringer af attributter ved hjælp af elektroniske midler efter anmodning fra brugeren at kontrollere autenticiteten af følgende attributter mod de relevante autentiske kilder på nationalt plan eller via udpegede mellemmand, der er anerkendte på nationalt plan, i overensstemmelse med national ret eller EU-retten og i tilfælde, hvor disse attributter er afhængige af autentiske kilder i den offentlige sektor, jf. artikel 45d:

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. offentlige tilladelser og licenser
10. finansielle data og virksomhedsoplysninger.

## 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 det officielle register
- c) et sæt data, der entydigt repræsenterer den enhed, som de attesterede attributter henviser til; anvendes der pseudonym, er dette tydeligt angivet
- 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, attesteringsordningen, som attesteringen 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 om attesteringens gyldighedsstatus, befinder sig.