EUROPEISKA UNIONEN

EUROPAPARLAMENTET **RÅDET**

Bryssel den 13 mars 2024
(OR. en)

2021/0136 (COD) **PE-CONS 68/23**

TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237

LAGSTIFTNINGSAKTER OCH ANDRA INSTRUMENT

Ärende:	EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet

EUROPAPARLAMENTETS OCH RÅDETS
FÖRORDNING (EU) 2024/…

av den …

om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

med beaktande av Regionkommitténs yttrande[2],

i enlighet med det ordinarie lagstiftningsförfarandet[3], och

---

1 EUT C 105, 4.3.2022, s. 81.
2 EUT C 61, 4.2.2022, s. 42.
3 Europaparlamentets ståndpunkt av den 29 februari 2024 (ännu inte offentliggjord i EUT) och rådets beslut av den ...

av följande skäl:

(1) I kommissionens meddelande av den 19 februari 2020, *Att forma EU:s digitala framtid*, tillkännages att Europaparlamentets och rådets förordning (EU) nr 910/2014[4] ska revideras i syfte att förbättra dess effektivitet, utvidga dess förmåner till den privata sektorn och främja betrodda digitala identiteter för alla européer.

(2) I sina slutsatser av den 1–2 oktober 2020 uppmanade Europeiska rådet kommissionen att föreslå en utveckling av ett unionsomfattande ramverk för säker offentlig elektronisk identifiering, inklusive interoperabla elektroniska underskrifter, så att människor kan ha kontroll över sin identitet och sina uppgifter på nätet och få tillgång till offentliga, privata och gränsöverskridande digitala tjänster.

(3) I policyprogrammet för det digitala decenniet, inrättat genom Europaparlamentets och rådets beslut (EU) 2022/2481[5], fastställs syftena och de digitala målen för ett unionsramverk som, senast 2030, är avsett att leda till en omfattande utbyggnad av en betrodd, frivillig och användarkontrollerad digital identitet som erkänns i hela unionen och som innebär att varje användare kan kontrollera sina uppgifter vid onlineinteraktioner.

---

4 Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

5 Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030 (EUT L 323, 19.12.2022, s. 4).

(4) I den europeiska förklaringen om digitala rättigheter och principer för det digitala decenniet, som kungjordes av Europaparlamentet, rådet och kommissionen[6] (*förklaringen*), understryks allas rätt att ha tillgång till digitala tekniker, produkter och tjänster som är säkra och trygga och utformade på ett sätt som skyddar den personliga integriteten. Detta inbegriper att säkerställa att alla människor i unionen erbjuds en tillgänglig, säker och tillförlitlig digital identitet som ger tillgång till ett brett utbud av nättjänster och offlinetjänster och som är skyddad mot cybersäkerhetsrisker och it-brottslighet, däribland personuppgiftsincidenter och stöld eller manipulation av identiteten. I förklaringen anges även att alla har rätt till skydd av sina personuppgifter. Denna rätt innefattar kontrollen över hur uppgifterna används och vem som får ta del av dem.

(5) Unionsmedborgarna och invånare i unionen bör ha en rätt till en digital identitet som står under deras egen kontroll och som innebär att de kan utöva sina rättigheter i den digitala miljön och delta i den digitala ekonomin. För att nå detta syfte bör ett europeiskt ramverk för digital identitet inrättas som ger unionsmedborgare och invånare i unionen tillgång till offentliga och privata nättjänster och offlinetjänster i hela unionen.

(6) Ett harmoniserat ramverk för digital identitet bör bidra till att skapa en digitalt mer integrerad union genom att minska de digitala hindren mellan medlemsstaterna och ge unionsmedborgarna och invånare i unionen möjlighet att dra nytta av digitaliseringens fördelar och samtidigt öka öppenheten och skyddet av deras rättigheter.

---

[6] EUT C 23, 23.1.2023, s. 1.

(7) En mer harmoniserad strategi för elektronisk identifiering bör minska de risker och kostnader som den nuvarande fragmenteringen har lett till på grund av användningen av olika nationella lösningar eller, i vissa medlemsstater, frånvaron av sådana lösningar för elektronisk identifiering. En sådan strategi bör stärka den inre marknaden genom att göra det möjligt för unionsmedborgare, invånare i unionen enligt definitionen i nationell rätt och företag att identifiera sig och att autentisera sin identitet online och offline på ett säkert, tillförlitligt, användarvänligt, enkelt, tillgängligt och harmoniserat sätt i hela unionen. Den europeiska digitala identitetsplånboken bör förse fysiska och juridiska personer i hela unionen med harmoniserade medel för elektronisk identifiering som möjliggör autentisering och utbyte av data som är kopplade till deras identitet. Alla bör ha möjlighet att komma åt offentliga och privata tjänster på ett säkert sätt genom ett förbättrat ekosystem för betrodda tjänster och med verifierade identitetsbevis och elektroniska attributsintyg, till exempel akademiska kvalifikationer, inbegripet universitetsexamina eller andra utbildnings- eller yrkeskvalifikationer. Det europeiska ramverket för digital identitet är avsett att åstadkomma en övergång från användningen av endast nationella lösningar för elektronisk identifiering till tillhandahållande av elektroniska attributsintyg som är giltiga och rättsligt erkända i hela unionen. Tillhandahållare av elektroniska attributsintyg bör omfattas av en tydlig och enhetlig uppsättning av regler, medan offentliga förvaltningar bör kunna förlita sig på elektroniska dokument i ett visst format.

(8) Flera medlemsstater har infört och använder medel för elektronisk identifiering som godtas av tjänsteleverantörer i unionen. Dessutom gjordes investeringar i både nationella och gränsöverskridande lösningar på grundval av förordning (EU) nr 910/2014, inbegripet interoperabilitet i anmälda system för elektronisk identifiering enligt den förordningen. För att säkerställa komplementaritet och ett snabbt ibruktagande av europeiska digitala identitetsplånböcker av nuvarande användare av anmälda medel för elektronisk identifiering och för att minimera konsekvenserna för befintliga tjänsteleverantörer, förväntas de europeiska digitala identitetsplånböckerna dra nytta av att bygga vidare på erfarenheterna av befintliga medel för elektronisk identifiering och av infrastrukturen för anmälda system för elektronisk identifiering på unionsnivå och nationell nivå.

(9) Europaparlamentets och rådets förordning (EU) 2016/679[7] och, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG[8] är tillämpliga på all behandling av personuppgifter i enlighet med förordning (EU) nr 910/2014. Lösningarna inom det interoperabilitetsramverk som föreskrivs i den här förordningen är också förenliga med dessa regler. Unionsrätten om dataskydd innehåller dataskyddsprinciper, såsom uppgiftsminimering och principen om ändamålsbegränsning, och skyldigheter, såsom inbyggt dataskydd och dataskydd som standard.

---

7 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

8 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

(10) För att förbättra unionsföretagens konkurrenskraft bör tillhandahållare av både nättjänster och offlinetjänster kunna förlita sig på lösningar för elektronisk identifiering som erkänns i hela unionen, oavsett vilken medlemsstat dessa lösningar tillhandahålls i, och därmed dra nytta av en harmoniserad unionsstrategi för tillförlitlighet, säkerhet och interoperabilitet. Både användare och tjänsteleverantörer bör kunna gynnas av att samma rättsliga värde ges till elektroniska attributsintyg i hela unionen. Ett harmoniserat ramverk för digital identitet är avsett att skapa ekonomiskt värde genom att underlätta tillgången till varor och tjänster, genom att avsevärt minska driftskostnaderna för elektroniska identifierings- och autentiseringsförfaranden, t.ex. vid anslutning av nya kunder, genom att minska risken för it-brottslighet, såsom identitetsstöld, datastöld och nätbedrägeri, och på så sätt främja effektivitetsvinster och en säker digital omställning bland unionens mikroföretag och små och medelstora företag.

(11) Europeiska digitala identitetsplånböcker bör underlätta tillämpningen av engångsprincipen och på så sätt minska den administrativa bördan och stödja gränsöverskridande rörlighet för unionsmedborgare och invånare i unionen och företag i unionen samt främja utvecklingen av interoperabla e-förvaltningstjänster i hela unionen.

(12) Förordning (EU) 2016/679, Europaparlamentets och rådets förordning (EU) 2018/1725[9] och direktiv 2002/58/EG är tillämpliga på behandlingen av personuppgifter i samband med genomförandet av denna förordning. Därför bör specifika skyddsåtgärder fastställas i denna förordning för att förhindra att tillhandahållare av medel för elektronisk identifiering och elektroniska attributsintyg kombinerar personuppgifter som erhållits vid tillhandahållande av andra tjänster med personuppgifter som behandlas för att tillhandahålla de tjänster som omfattas av tillämpningsområdet för denna förordning. Personuppgifter som rör tillhandahållandet av de europeiska digitala identitetsplånböckerna bör hållas logiskt avskilda från andra data som innehas av tillhandahållaren av den europeiska digitala identitetsplånboken. Denna förordning bör inte hindra tillhandahållare av europeiska digitala identitetsplånböcker från att tillämpa ytterligare tekniska åtgärder som bidrar till skyddet av personuppgifter, såsom fysisk åtskillnad mellan personuppgifter som rör tillhandahållandet av europeiska digitala identitetsplånböcker och andra uppgifter som innehas av tillhandahållaren. Utan att det påverkar tillämpningen av förordning (EU) 2016/679 specificeras i denna förordning ytterligare tillämpningen av principerna om ändamålsbegränsning, uppgiftsminimering, inbyggt dataskydd och dataskydd som standard.

---

[9] Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

(13) De europeiska digitala identitetsplånböckerna bör ha en funktion i form av en gemensam instrumentpanel som är inbäddad i dess utformning för att säkerställa att användarna har en högre grad av öppenhet, integritet och kontroll när det gäller deras data. Den funktionen bör ha ett enkelt, användarvänligt gränssnitt med en översikt över alla förlitande parter med vilka användaren delar data, inklusive attribut, och vilken typ av uppgifter som delats med varje förlitande part. Den bör göra det möjligt för användare att spåra alla transaktioner som utförs genom den europeiska digitala identitetsplånboken med åtminstone följande uppgifter: tidpunkt och datum för transaktionen, identifiering av motparten, begärda personuppgifter och delade uppgifter. Denna information bör lagras även om transaktionen inte fullföljs. Det bör inte vara möjligt att bestrida äktheten hos den information som ingår i transaktionshistoriken. En sådan funktion bör vara aktiv som utgångspunkt. Den bör göra det möjligt för användare att enkelt begära att en förlitande part omedelbart raderar personuppgifter enligt artikel 17 i förordning (EU) 2016/679 och att enkelt rapportera den förlitande parten till den behöriga nationella dataskyddsmyndigheten om en påstått olaglig eller misstänkt begäran om personuppgifter tagits emot, direkt via den europeiska digitala identitetsplånboken.

(14) Medlemsstaterna bör integrera olika integritetsbevarande tekniker, såsom nollkunskapsbevis, i den europeiska digitala identitetsplånboken. Dessa kryptografiska metoder bör göra det möjligt för en förlitande part att validera om ett visst påstående baserat på personens identifieringsuppgifter och attributsintyg är sant, utan att några uppgifter med anknytning till detta påstående förmedlas, och därigenom bevara användarens integritet.

(15) Denna förordning fastställer harmoniserade villkor för inrättandet av ett ramverk för europeiska digitala identitetsplånböcker som ska tillhandahållas av medlemsstaterna. Alla unionsmedborgare och invånare i unionen enligt definitionen i nationell rätt bör på ett säkert sätt kunna begära, välja, kombinera, lagra, radera, dela och visa identitetsuppgifter och begära att deras personuppgifter raderas på ett användarvänligt och bekvämt sätt under användarens egen kontroll, samtidigt som selektivt utlämnande av personuppgifter möjliggörs. Denna förordning återspeglar gemensamma europeiska värden och respekterar grundläggande rättigheter, rättsliga garantier och ansvarsskyldighet, och skyddar därmed demokratiska samhällen, unionsmedborgare och invånare i unionen. De tekniker som används för att uppnå dessa mål bör utformas för att uppnå högsta möjliga nivå av säkerhet, integritet, användarvänlighet, tillgänglighet, användbarhet och sömlös interoperabilitet. Medlemsstaterna bör säkerställa lika tillgång till elektronisk identifiering för alla sina medborgare och invånare. Medlemsstaterna bör inte, vare sig direkt eller indirekt, begränsa tillgången till offentliga eller privata tjänster för fysiska eller juridiska personer som väljer att inte använda en europeisk digital identitetsplånbok och bör göra lämpliga alternativa lösningar tillgängliga.

(16) Medlemsstaterna bör förlita sig på de möjligheter som denna förordning erbjuder för att på eget ansvar tillhandahålla europeiska digitala identitetsplånböcker för användning av fysiska och juridiska personer som är bosatta på deras territorium. För att ge medlemsstaterna flexibilitet och öka utnyttjandet den senaste tekniken bör denna förordning möjliggöra tillhandahållande av europeiska digitala identitetsplånböcker direkt av en medlemsstat, på uppdrag av en medlemsstat eller oberoende av en medlemsstat men med erkännande av den medlemsstaten.

(17) För registreringsändamål bör förlitande parter tillhandahålla den information som krävs för att möjliggöra elektronisk identifiering och autentisering av dem gentemot europeiska digitala identitetsplånböcker. När förlitande parter deklarerar sin avsedda användning av den europeiska digitala identitetsplånboken bör de tillhandahålla information om de uppgifter som de eventuellt kommer att begära för att tillhandahålla sina tjänster och om skälet till begäran. Registreringen av förlitande parter underlättar medlemsstaternas kontroller av lagenligheten hos de förlitande parternas verksamhet i enlighet med unionsrätten. Registreringsskyldigheten enligt denna förordning bör inte påverka de skyldigheter som fastställs i annan unionsrätt eller nationell rätt, såsom den information som ska lämnas till de registrerade i enlighet med förordning (EU) 2016/679. Förlitande parter bör följa de garantier som erbjuds genom artiklarna 35 och 36 i den förordningen, särskilt genom att utföra konsekvensbedömningar avseende dataskydd och genom att samråda med de behöriga dataskyddsmyndigheterna innan de behandlar uppgifter, om konsekvensbedömningar avseende dataskydd visar att behandlingen skulle leda till en hög risk. Sådana garantier bör utgöra ett stöd för förlitande parters lagliga behandling av personuppgifter, i synnerhet avseende särskilda kategorier av uppgifter, såsom hälsouppgifter. Registreringen av förlitande parter syftar till att öka öppenheten i och förtroendet för användningen av europeiska digitala identitetsplånböcker. Registreringen bör vara kostnadseffektiv och stå i proportion till de relaterade riskerna för att säkerställa att den sprids bland tjänsteleverantörerna. I detta sammanhang bör registreringen innebära att automatiserade förfaranden används, inbegripet att medlemsstaterna förlitar sig på och använder befintliga register, och den bör inte innefatta något förfarande för förhandsgodkännande. Registreringsprocessen bör möjliggöra en rad olika användningsfall som kan skilja sig åt i fråga om driftsätt – antingen online eller offline – eller i fråga om kravet på autentisering av enheter för interaktion med den europeiska digitala identitetsplånboken. Registreringen bör uteslutande gälla förlitande parter som tillhandahåller tjänster genom digital interaktion.

(18) Att skydda unionsmedborgare och invånare i unionen mot obehörig eller bedräglig användning av europeiska digitala identitetsplånböcker är av stor betydelse för att säkerställa förtroende för och en bred spridning av europeiska digitala identitetsplånböcker. Användarna bör förses med ett effektivt skydd mot sådant missbruk. I synnerhet när fakta som utgör grunden för bedräglig eller annan olaglig användning av en europeisk digital identitetsplånbok fastställs av en nationell rättslig myndighet i samband med ett annat förfarande, bör tillsynsorgan som ansvarar för utfärdare av europeiska digitala identitetsplånböcker efter anmälan vidta nödvändiga åtgärder för att säkerställa att registreringen av den förlitande parten och inkluderingen av förlitande parter i autentiseringsmekanismen återkallas eller tillfälligt upphävs till dess att den anmälande myndigheten bekräftar att de konstaterade oriktigheterna har åtgärdats.

(19) Alla europeiska digitala identitetsplånböcker bör göra det möjligt för användarna att identifiera och autentisera sig på elektronisk väg online och offline över gränserna för att få tillgång till ett stort utbud av offentliga och privata tjänster. Utan att det påverkar medlemsstaternas behörigheter när det gäller identifieringen av deras medborgare och invånare kan europeiska digitala identitetsplånböcker även användas för att tillgodose de institutionella behoven vid offentliga förvaltningar, internationella organisationer samt EU:s institutioner, organ och byråer. I många sektorer är det viktigt med autentisering offline, bland annat i hälso- och sjukvårdssektorn, där tjänsterna ofta tillhandahålls vid direkta kontakter, och e-recept bör kunna autentiseras med hjälp av QR-koder eller liknande tekniker. För att säkerställa en hög tillitsnivå vad gäller system för elektronisk identifiering bör de europeiska digitala identitetsplånböckerna utnyttja den potential som erbjuds via manipuleringssäkra lösningar såsom säkerhetsdetaljer för att uppfylla säkerhetskraven i denna förordning. Europeiska digitala identitetsplånböcker bör även göra det möjligt för användarna att skapa och använda kvalificerade elektroniska underskrifter och stämplar som godtas i hela unionen. När fysiska personer väl har börjat använda en europeisk digital identitetsplånbok bör de, som utgångspunkt och kostnadsfritt, kunna använda den för att underteckna med kvalificerade elektroniska underskrifter utan att behöva genomgå några ytterligare administrativa förfaranden. Användare bör kunna underteckna eller stämpla egna förklaringar eller attribut. För att ge personer och företag i hela unionen fördelar i form av enkel hantering och sänkta kostnader, däribland genom att tillåta behörigheter att företräda och elektroniska fullmakter, bör medlemsstaterna tillhandahålla europeiska digitala identitetsplånböcker på grundval av gemensamma standarder och tekniska specifikationer för att säkerställa sömlös interoperabilitet och på adekvat sätt höja it-säkerhetsnivån, stärka motståndskraften mot cyberattacker och på så vis avsevärt minska de potentiella riskerna med den pågående digitaliseringen för unionsmedborgare, invånare i unionen och företag.

Det är endast medlemsstaternas behöriga myndigheter som kan fastställa identiteter med en hög tillförlitlighetsnivå och därmed garantera att en person faktiskt är den person som han eller hon påstår sig vara. Därför måste tillhandahållandet av de europeiska digitala identitetsplånböckerna bygga på den juridiska identiteten för unionsmedborgare, invånare i unionen eller juridiska personer. Användning av den juridiska identiteten bör inte hindra användarna av de europeiska digitala identitetsplånböckerna från att få tillgång till tjänster under en pseudonym om det inte finns något rättsligt krav på juridisk identitet för autentisering. Tilliten till de europeiska digitala identitetsplånböckerna skulle förstärkas om utfärdande och förvaltande parter hade varit tvungna att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa den högsta säkerhetsnivå som står i rimlig proportion till riskerna för fysiska personers rättigheter och friheter i enlighet med förordning (EU) 2016/679.

(20) Användningen av en kvalificerad elektronisk underskrift bör vara kostnadsfri för alla fysiska personer för icke-yrkesmässiga ändamål. Det bör vara möjligt för medlemsstaterna att föreskriva åtgärder för att hindra att fysiska personer kostnadsfritt använder kvalificerade elektroniska underskrifter för yrkesmässiga ändamål och samtidigt säkerställa att alla sådana åtgärder står i proportion till identifierade risker och är motiverade.

(21) Det är fördelaktigt att underlätta spridningen och användningen av europeiska digitala identitetsplånböcker genom att på ett smidigt sätt integrera dem i ekosystemet av offentliga och privata digitala tjänster som redan införts på nationell, lokal eller regional nivå. För att uppnå detta mål bör medlemsstaterna kunna föreskriva rättsliga och organisatoriska åtgärder för att öka flexibiliteten för tillhandahållare av europeiska digitala identitetsplånböcker och medge ytterligare funktioner i de europeiska digitala identitetsplånböckerna utöver vad som fastställs i denna förordning, bland annat genom ökad interoperabilitet med befintliga nationella medel för elektronisk identifiering. Sådana ytterligare funktioner bör inte på något sätt inverka negativt på tillhandahållandet av de europeiska digitala identitetsplånböckernas centrala funktioner som föreskrivs i denna förordning och inte heller främja befintliga nationella lösningar framför europeiska digitala identitetsplånböcker. Eftersom sådana ytterligare funktioner går utöver denna förordning omfattas de inte av de bestämmelser om gränsöverskridande användning av europeiska digitala identitetsplånböcker som fastställs i denna förordning.

(22) Europeiska digitala identitetsplånböcker bör ha en funktion för att generera pseudonymer, som användarna väljer och hanterar, för autentisering vid åtkomst till nättjänster.

(23) För att uppnå en hög nivå av säkerhet och tillförlitlighet innehåller denna förordning krav för de europeiska digitala identitetsplånböckerna. Plånböckernas efterlevnad med dessa krav bör intygas av ackrediterade organ för bedömning av överensstämmelse som utses av medlemsstaterna.

(24) För att undvika skilda tillvägagångssätt och harmonisera genomförandet av de krav som fastställs i denna förordning bör kommissionen, med avseende på certifiering av europeiska digitala identitetsplånböcker, anta genomförandeakter i syfte att fastställa en förteckning över referensstandarder och, vid behov, specifikationer och förfaranden i syfte att formulera närmare tekniska specifikationer av dessa krav. I den mån intyg om överensstämmelse för de europeiska digitala identitetsplånböckerna med relevanta cybersäkerhetskrav inte omfattas av befintliga ordningar för cybersäkerhetscertifiering som avses i denna förordning, och när det gäller andra krav än cybersäkerhetskrav som är relevanta för europeiska digitala identitetsplånböcker, bör medlemsstaterna inrätta nationella certifieringssystem i enlighet med de harmoniserade krav som fastställs i och antas i enlighet med denna förordning. Medlemsstaterna bör överföra sina utkast till nationella certifieringssystem till den europeiska samarbetsgruppen för digital identitet, som bör kunna utfärda yttranden och rekommendationer.

(25) Certifiering av överensstämmelse med de cybersäkerhetskrav som fastställs i denna förordning bör, i förekommande fall, bygga på de relevanta europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881[10], som inrättar en frivillig europeisk ram för cybersäkerhetscertifiering av IKT-produkter, IKT-processer och IKT-tjänster.

[10] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

(26) För att kontinuerligt bedöma och minska säkerhetsrelaterade risker bör certifierade europeiska digitala identitetsplånböcker bli föremål för regelbundna sårbarhetsbedömningar som syftar till att upptäcka eventuella sårbarheter i den europeiska digitala identitetsplånbokens certifierade produkt-, process- och tjänsterelaterade komponenter.

(27) Genom att skydda användare och företag mot cybersäkerhetsrisker bidrar de väsentliga cybersäkerhetskrav som fastställs i denna förordning också till att förbättra skyddet av personuppgifter och individers integritet. När det gäller både standardiseringen och certifieringen av cybersäkerhetsaspekter bör synergier övervägas genom samarbete mellan kommissionen, europeiska standardiseringsorganisationer, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska dataskyddsstyrelsen, som inrättats genom förordning (EU) 2016/679, och de nationella tillsynsmyndigheterna med ansvar för dataskydd.

(28) Anslutning av unionsmedborgare och invånare i unionen till den europeiska digitala identitetsplånboken bör underlättas genom att man förlitar sig på medel för elektronisk identifiering som utfärdats med tillitsnivå hög. Medel för elektronisk identifiering som utfärdats med tillitsnivå väsentlig bör endast användas om harmoniserade tekniska specifikationer och förfaranden med hjälp av medel för elektronisk identifiering som utfärdats med tillitsnivå väsentlig i kombination med kompletterande medel för kontroll av identitet möjliggör uppfyllande av kraven i denna förordning vad gäller tillitsnivå hög. Sådana kompletterande medel bör vara tillförlitliga och lätta att använda och skulle kunna bygga på möjligheten att använda förfaranden för anslutning på distans, kvalificerade certifikat som stöds av kvalificerade elektroniska underskrifter, kvalificerade elektroniska attributsintyg eller en kombination av dessa. För att säkerställa tillräcklig spridning av de europeiska digitala identitetsplånböckerna bör harmoniserade tekniska specifikationer och förfaranden för anslutning av användare med hjälp av medel för elektronisk identifiering, inbegripet sådana som utfärdats med tillitsnivå väsentlig, fastställas i genomförandeakter.

(29) Syftet med denna förordning är att förse användaren med en helt mobil, säker och användarvänlig europeisk digital identitetsplånbok. Som en övergångsåtgärd till dess att certifierade manipuleringssäkra lösningar, såsom säkerhetskomponenter i användarnas enheter, finns tillgängliga bör de europeiska digitala identitetsplånböckerna kunna förlita sig på certifierade externa säkerhetskomponenter för skyddet av kryptografiskt material och andra känsliga uppgifter eller på anmälda medel för elektronisk identifiering med tillitsnivå hög för att påvisa överensstämmelse med de relevanta kraven i denna förordning vad gäller den europeiska digitala identitetsplånbokens tillitsnivå. Denna förordning bör inte påverka nationella villkor avseende utfärdande och användning av certifierade externa säkerhetskomponenter om denna övergångsåtgärd är beroende av dessa.

(30) De europeiska digitala identitetsplånböckerna bör garantera högsta möjliga dataskydds- och säkerhetsnivå för elektronisk identifiering och autentisering som underlättar tillgången till offentliga och privata tjänster, oavsett om uppgifterna lagras lokalt eller genom molnbaserade lösningar, där vederbörlig hänsyn tas till de olika risknivåerna.

(31) De europeiska digitala identitetsplånböckerna bör ha inbyggd säkerhet och innefatta avancerade säkerhetsfunktioner för att skydda mot identitetsstöld och annan datastöld, tillgänglighetsförlust och alla andra cyberhot. Säkerheten bör innefatta toppmoderna krypterings- och lagringsmetoder som är tillgängliga och dekrypterbara endast för användaren, och som förlitar sig på totalsträckskrypterad kommunikation med andra europeiska digitala identitetsplånböcker och förlitande parter. Dessutom bör de europeiska digitala identitetsplånböckerna kräva en säker, uttrycklig och aktiv bekräftelse av användaren för de operationer som utförs via de europeiska digitala identitetsplånböckerna.

(32) Kostnadsfri användning av europeiska digitala identitetsplånböcker bör inte leda till behandling av data utöver data som är nödvändig för tillhandahållandet av tjänster relaterade till europeiska digitala identitetsplånböcker. Denna förordning bör inte tillåta behandling av personuppgifter som lagras i eller härrör från användningen av den europeiska digitala identitetsplånboken av tillhandahållaren av den europeiska digitala identitetsplånboken för andra ändamål än tillhandahållandet av tjänster relaterade till europeiska digitala identitetsplånböcker. För att säkerställa integritet bör tillhandahållare av europeiska digitala identitetsplånböcker säkerställa icke-observerbarhet genom att inte samla in uppgifter och inte ha insyn i de transaktioner som utförs av användarna av den europeiska digitala identitetsplånboken. Denna icke-observerbarhet innebär att tillhandahållarna inte kan se detaljerade uppgifter om användarens transaktioner. I specifika fall, baserat på användarens uttryckliga föregående samtycke i vart och ett av dessa specifika fall, och i full överensstämmelse med förordning (EU) 2016/679, skulle tillhandahållare av europeiska digitala identitetsplånböcker emellertid kunna beviljas tillgång till den information som krävs för tillhandahållandet av en viss tjänst som gäller europeiska digitala identitetsplånböcker.

(33) Transparensen i europeiska digitala identitetsplånböcker och tillhandahållarnas ansvarsskyldighet är viktiga faktorer för att skapa social tillit och få till stånd acceptans för ramverket. De europeiska digitala identitetsplånböckernas funktionssätt bör därför vara transparent och i synnerhet medge kontrollerbar behandling av personuppgifter. För att uppnå detta bör medlemsstaterna lämna ut källkoden för programvarukomponenter i användartillämpningen av europeiska digitala identitetsplånböcker, inbegripet dem som rör behandling av personuppgifter och uppgifter om juridiska personer. Offentliggörandet av denna källkod under en licens med öppen källkod bör göra det möjligt för samhället, inbegripet användare och utvecklare, att förstå hur koden fungerar samt revidera och granska koden. Detta skulle öka användarnas förtroende för ekosystemet och bidra till de europeiska digitala identitetsplånböckernas säkerhet genom att göra det möjligt för vem som helst att rapportera sårbarheter och fel i koden. På det hela taget bör detta ge leverantörerna incitament att leverera och upprätthålla en mycket säker produkt. I vissa fall kan dock offentliggörandet av källkoden för bibliotek, kommunikationskanaler eller andra element som inte finns på användarenheten begränsas av medlemsstaterna, av vederbörligen motiverade skäl, särskilt med hänsyn till den allmänna säkerheten.

(34) Att använda europeiska digitala identitetsplånböcker liksom att upphöra att använda dem bör vara användarens exklusiva rättighet och val. Medlemsstaterna bör utarbeta enkla och säkra förfaranden så att användarna kan begära att giltigheten för europeiska digitala identitetsplånböcker omedelbart återkallas, även i händelse av förlust eller stöld. Vid användarens död eller när en juridisk persons verksamhet upphör bör en mekanism inrättas som gör det möjligt för den myndighet som ansvarar för att reglera arvet efter den fysiska personen eller tillgångarna hos den juridiska personen att begära att europeiska digitala identitetsplånböcker omedelbart återkallas.

(35) För att främja spridningen av europeiska digitala identitetsplånböcker och en bredare användning av digitala identiteter bör medlemsstaterna inte bara främja fördelarna med de relevanta tjänsterna, utan bör även, i samarbete med den privata sektorn, forskare och den akademiska världen, utveckla utbildningsprogram som syftar till att stärka de digitala färdigheterna hos sina medborgare och invånare, särskilt för utsatta grupper, såsom personer med funktionsnedsättning och äldre personer. Medlemsstaterna bör också öka medvetenheten om fördelarna och riskerna med europeiska digitala identitetsplånböcker genom informationskampanjer.

(36) För att säkerställa att det europeiska ramverket för digital identitet är öppet för innovation och teknisk utveckling och att det är framtidssäkrat uppmuntras medlemsstaterna att gemensamt inrätta testmiljöer där innovativa lösningar kan testas i en kontrollerad och säker miljö i syfte att förbättra lösningarnas funktion, personuppgiftsskydd, säkerhet och interoperabilitet och lägga grunden för framtida uppdateringar av tekniska referenser och rättsliga krav. Denna miljö bör även uppmuntra deltagande av små och medelstora företag, uppstartsföretag och enskilda innovatörer och forskare samt berörda parter från branschen. Sådana initiativ bör bidra till och stärka regelefterlevnaden och den tekniska robustheten hos de europeiska digitala identitetsplånböcker som ska tillhandahållas unionsmedborgare och invånare i unionen, och därigenom förhindra att det utvecklas lösningar som inte är förenliga med unionsrätten om dataskydd eller som är sårbara vad gäller säkerheten.

(37) Genom Europaparlamentets och rådets förordning (EU) 2019/1157[11] kommer säkerheten för identitetskort att utökas med ytterligare säkerhetsdetaljer i augusti 2021. Medlemsstaterna bör överväga om det är möjligt att anmäla dem inom ramen för systemen för elektronisk identifiering för att utöka den gränsöverskridande tillgången till medel för elektronisk identifiering.

(38) Anmälningen av system för elektronisk identifiering bör förenklas och påskyndas för att främja tillgången till bekväma, tillförlitliga, säkra och innovativa lösningar för autentisering och identifiering och, i förekommande fall, uppmuntra privata leverantörer av lösningar för identifiering att erbjuda system för elektronisk identifiering till medlemsstaternas myndigheter för anmälning som nationella system för elektronisk identifiering enligt förordning (EU) nr 910/2014.

(39) En effektivisering av de nuvarande förfarandena för anmälan och sakkunnigbedömning kommer att förhindra skilda synsätt på bedömningen av olika anmälda system för elektronisk identifiering och bygga upp förtroendet mellan medlemsstaterna. Nya, förenklade mekanismer är avsedda att främja medlemsstaternas samarbete i frågor som rör säkerheten och interoperabiliteten med avseende på deras anmälda system för elektronisk identifiering.

(40) Medlemsstaterna bör kunna utnyttja nya, flexibla verktyg för att säkerställa att kraven i denna förordning och i de relevanta genomförandeakter som antas enligt denna uppfylls. Denna förordning bör ge medlemsstaterna möjlighet att använda rapporter och bedömningar, som utförts av ackrediterade organ för bedömning av överensstämmelse, såsom föreskrivs i samband med de certifieringsordningar som ska inrättas på unionsnivå enligt förordning (EU) 2019/881, som stöd i deras arbete med att anpassa systemen, eller delar av dessa, till förordning (EU) nr 910/2014.

---

[11] Europaparlamentets och rådets förordning (EU) 2019/1157 av den 20 juni 2019 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet (EUT L 188, 12.7.2019, s. 67).

(41) Offentliga tjänsteleverantörer använder de uppgifter för personidentifiering som finns tillgängliga genom systemen för elektronisk identifiering enligt förordning (EU) nr 910/2014 för att matcha den elektroniska identiteten hos användare från andra medlemsstater med de uppgifter för personidentifiering som tillhandahålls dessa användare i den medlemsstat som utför den gränsöverskridande identitetsmatchningsprocessen. För att säkerställa korrekt identitetsmatchning när medlemsstaterna agerar som förlitande parter krävs det dock i många fall, trots användningen av den minimiuppsättning uppgifter som tillhandahålls inom ramen för de anmälda systemen för elektronisk identifiering, ytterligare information om användaren och specifika kompletterande unika identifieringsförfaranden som genomförs på nationell nivå. För att ytterligare stödja användbarheten hos medel för elektronisk identifiering, tillhandahålla bättre offentliga nättjänster och öka rättssäkerheten när det gäller användarnas elektroniska identitet bör förordning (EU) nr 910/2014 kräva att medlemsstaterna vidtar specifika åtgärder online för att säkerställa otvetydig identitetsmatchning när användare avser att få åtkomst till gränsöverskridande offentliga nättjänster.

(42) Vid utvecklingen av europeiska digitala identitetsplånböcker är det mycket viktigt att ta hänsyn till användarnas behov. Meningsfulla användningsfall och nättjänster som förlitar sig på europeiska digitala identitetsplånböcker bör vara tillgängliga. För användarnas bekvämlighet och för att säkerställa gränsöverskridande tillgång till sådana tjänster är det viktigt att vidta åtgärder för att underlätta en liknande strategi för utformning, utveckling och genomförande av nättjänster i alla medlemsstater. Icke-bindande riktlinjer för hur nättjänster som förlitar sig på europeiska digitala identitetsplånböcker ska utformas, utvecklas och genomföras har potential att bli ett användbart verktyg för att uppnå detta mål. Sådana riktlinjer bör utarbetas med beaktande av unionens interoperabilitetsramverk. Medlemsstaterna bör ha en ledande roll när det gäller att anta dessa riktlinjer.

(43) I enlighet med Europaparlamentets och rådets direktiv (EU) 2019/882[12] bör personer med funktionsnedsättning kunna använda europeiska digitala identitetsplånböcker, betrodda tjänster och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster på samma villkor som andra användare.

(44) För att säkerställa en effektiv efterlevnad av denna förordning bör det fastställas en miniminivå för de maximala administrativa sanktionsavgifterna för både kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster. Medlemsstaterna bör föreskriva effektiva, proportionella och avskräckande sanktioner. Vid fastställandet av sanktionerna bör vederbörlig hänsyn tas till de berörda enheternas storlek, deras affärsmodeller och överträdelsernas allvar.

(45) Medlemsstaterna bör fastställa regler om sanktioner för överträdelser såsom direkta eller indirekta metoder som leder till förväxling mellan icke-kvalificerade och kvalificerade betrodda tjänster eller till att icke-kvalificerade tillhandahållare av betrodda tjänster missbrukar EU-förtroendemärket. EU-förtroendemärket bör inte användas på villkor som direkt eller indirekt leder till uppfattningen att icke-kvalificerade betrodda tjänster som tillhandahålls av dessa tillhandahållare är kvalificerade.

(46) Denna förordning bör inte gälla frågor som avser ingående av och giltigheten hos avtal eller andra rättsliga förpliktelser om unionsrätten eller nationell rätt föreskriver vissa formkrav. Den bör inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister.

---

[12] Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

(47) Tillhandahållandet och användningen av betrodda tjänster och de fördelar detta innebär vad gäller bekvämlighet och rättssäkerhet i samband med gränsöverskridande transaktioner, i synnerhet när kvalificerade betrodda tjänster används, blir allt viktigare för internationell handel och internationellt samarbete. Unionens internationella partner håller på att inrätta tillitsramverk som har inspirerats av förordning (EU) nr 910/2014. För att underlätta erkännandet av kvalificerade betrodda tjänster och deras tillhandahållare kan kommissionen anta genomförandeakter för att fastställa de villkor enligt vilka tillitsramverk i tredjeländer skulle kunna anses vara likvärdiga med tillitsramverket för kvalificerade betrodda tjänster och tillhandahållare av sådana tjänster i denna förordning. En sådan strategi bör komplettera möjligheten till ett ömsesidigt erkännande av betrodda tjänster och tillhandahållare av sådana tjänster som är etablerade i unionen och i tredjeländer i enlighet med artikel 218 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). Vid fastställandet av de villkor som måste uppfyllas av tillitsramverk i tredjeländer för att anses vara likvärdiga med tillitsramverket för kvalificerade betrodda tjänster och tillhandahållare av sådana tjänster enligt förordning (EU) nr 910/2014, bör även efterlevnaden av de relevanta bestämmelserna i Europaparlamentets och rådets direktiv (EU) 2022/2555[13] och förordning (EU) 2016/679 säkerställas, liksom användningen av förteckningar över betrodda tjänsteleverantörer som avgörande komponenter för att bygga upp förtroende.

[13] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).

(48) Denna förordning bör främja valfrihet och möjligheten att byta mellan europeiska digitala identitetsplånböcker om en medlemsstat har godkänt mer än en lösning för europeiska digitala identitetsplånböcker på sitt territorium. För att undvika inlåsningseffekter i sådana situationer bör tillhandahållarna av europeiska digitala identitetsplånböcker där detta är tekniskt genomförbart säkerställa effektiv portabilitet för uppgifter på begäran av användare av europeiska digitala identitetsplånböcker, och de bör inte tillåtas använda avtalsenliga, ekonomiska eller tekniska spärrar för att förhindra eller försvåra ett effektivt byte mellan olika europeiska digitala identitetsplånböcker.

(49) För att säkerställa att de europeiska digitala identitetsplånböckerna fungerar korrekt behöver tillhandahållare av europeiska digitala identitetsplånböcker effektiv interoperabilitet och rättvisa, rimliga och icke-diskriminerande villkor för att de europeiska digitala identitetsplånböckerna ska få tillgång till specifika maskinvaru- och programvarufunktioner hos mobila enheter. Dessa komponenter skulle särskilt kunna omfatta NFC-antenner och säkerhetskomponenter, inbegripet universella smartkort, inbäddade säkerhetskomponenter, microSD-kort och Bluetooth Low Energy. Tillgången till komponenterna skulle kunna kontrolleras av mobilnätsoperatörer och tillverkare av utrustning. Därför bör tillverkare av originalutrustning för mobila enheter eller tillhandahållare av elektroniska kommunikationstjänster inte neka tillgång till sådana komponenter när de behövs för att tillhandahålla tjänster relaterade till de europeiska digitala identitetsplånböckerna. Dessutom bör de företag som betecknas som grindvakter för centrala plattformstjänster enligt kommissionens förteckning i Europaparlamentets och rådets förordning (EU) 2022/1925[14] fortsätta att omfattas av de särskilda bestämmelserna i den förordningen, på grundval av artikel 6.7 i den förordningen.

---

[14] Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1).

(50) För att anpassa de skyldigheter avseende cybersäkerhet som införts för tillhandahållare av betrodda tjänster, och för att dessa tillhandahållare och deras respektive behöriga myndigheter ska kunna gynnas av den rättsliga ram som inrättas genom direktiv (EU) 2022/2555, ska betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder i enlighet med det direktivet, däribland åtgärder mot systembrister, mänskliga fel, olagliga handlingar eller naturfenomen, för att hantera säkerhetsriskerna i de nätverk och informationssystem som dessa tillhandahållare använder för att tillhandahålla sina tjänster, liksom för att anmäla allvarliga incidenter och cyberhot i enlighet med det direktivet. När det gäller rapporteringen av incidenter bör tillhandahållare av betrodda tjänster anmäla varje incident som har en betydande inverkan på tillhandahållandet av deras tjänster, däribland sådana som orsakas av stöld eller förlust av anordningar, skador på nätverkskablar eller incidenter i samband med identifieringen av personer. Kraven och rapporteringsskyldigheterna för hanteringen av riskerna för cybersäkerheten enligt direktiv (EU) 2022/2555 bör ses som komplement till de krav som införs för tillhandahållare av betrodda tjänster enligt denna förordning. I tillämpliga fall bör nationella förfaranden eller riktlinjer som fastställts med avseende på genomförandet av säkerhets- och rapporteringskraven och övervakningen av efterlevnaden av sådana krav enligt förordning (EU) nr 910/2014 fortsätta att tillämpas av de behöriga myndigheter som utses enligt direktiv (EU) 2022/2555. Denna förordning påverkar inte skyldigheten att anmäla personuppgiftsincidenter enligt förordning (EU) 2016/679.

(51) Vederbörlig hänsyn bör tas för att säkerställa ett effektivt samarbete mellan de tillsynsorgan som utses i enlighet med artikel 46b i förordning (EU) nr 910/2014 och de behöriga myndigheter som utses eller fastställs i enlighet med artikel 8.1 i direktiv (EU) 2022/2555. Om ett sådant tillsynsorgan skiljer sig från en sådan behörig myndighet bör de bedriva ett nära och effektivt samarbete genom att utbyta relevant information för att säkerställa en effektiv tillsyn och att tillhandahållarna av betrodda tjänster uppfyller kraven i förordning (EU) nr 910/2014 och direktiv (EU) 2022/2555. I synnerhet bör de tillsynsorganen som utses i enlighet med förordning (EU) nr 910/2014 ha rätt att begära att behöriga myndigheter som utses eller fastställs i enlighet med direktiv (EU) 2022/2555 tillhandahåller all relevant information som behövs för att bevilja status som kvalificerad och för att utföra tillsynsåtgärder för att kontrollera att tillhandahållarna av betrodda tjänster uppfyller de relevanta kraven i direktiv (EU) 2022/2555 eller kräva att de åtgärdar bristerna.

(52) Det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. En sådan ram kan även skapa nya marknadsmöjligheter för tillhandahållare av betrodda tjänster i unionen att erbjuda nya unionsomfattande elektroniska tjänster för rekommenderade leveranser. För att säkerställa att data som skickas med hjälp av en kvalificerad elektronisk tjänst för rekommenderade leveranser levereras till rätt adressat bör kvalificerade elektroniska tjänster för rekommenderade leveranser med komplett säkerhet säkerställa identifieringen av adressaten, medan en hög tillförlitlighetsnivå skulle räcka när det gäller identifiering av avsändaren. Tillhandahållare av kvalificerade elektroniska tjänster för rekommenderade leveranser bör av medlemsstaterna uppmuntras att göra sina tjänster interoperabla med sådana kvalificerade elektroniska tjänster för rekommenderade leveranser som tillhandahålls av andra kvalificerade tillhandahållare av betrodda tjänster i syfte att enkelt överföra elektroniska rekommenderade uppgifter mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster och främja god sed på den inre marknaden.

(53) I de flesta fall kan unionsmedborgare och invånare i unionen inte utbyta digital information över gränserna om sin identitet, t.ex. adress, ålder och yrkeskvalifikationer, körkort och andra tillstånd eller betalningsuppgifter, på ett säkert sätt och med en hög nivå av dataskydd.

(54) Det bör vara möjligt att utfärda och hantera tillförlitliga elektroniska attribut och bidra till att minska den administrativa bördan genom att ge unionsmedborgare och invånare i unionen möjlighet att använda dem i privata och offentliga transaktioner. Unionsmedborgare och invånare i unionen bör till exempel kunna bevisa innehav av ett giltigt körkort som har utfärdats av en myndighet i en medlemsstat och som kan verifieras och godtas av de berörda myndigheterna i andra medlemsstater. De bör även kunna förlita sig på sina uppgifter om social trygghet eller framtida digitala resehandlingar i ett gränsöverskridande sammanhang.

(55) Alla tillhandahållare av tjänster som utfärdar attesterade attribut i elektroniskt format, såsom examensbevis, licenser, personbevis eller befogenheter och uppdrag att företräda fysiska eller juridiska personer eller agera på deras vägnar bör anses vara en tillhandahållare av betrodda elektroniska attributsintyg. Ett elektroniskt attributsintyg bör inte förvägras rättslig verkan på grund av att det har elektronisk form eller inte uppfyller kraven för ett kvalificerat elektroniskt attributsintyg. Allmänna krav bör fastställas för att säkerställa att kvalificerade elektroniska attributsintyg har samma rättsliga verkan som lagligen utfärdade intyg i pappersform. Sådana krav bör emellertid gälla utan att det påverkar tillämpningen av unionsrätt eller nationell rätt som omfattar ytterligare sektorsspecifika krav med underliggande rättsliga verkningar vad gäller formen och, i synnerhet, det gränsöverskridande erkännandet av kvalificerade elektroniska attributsintyg i tillämpliga fall.

(56) En bred tillgång till och användbarhet för europeiska digitala identitetsplånböcker bör leda till att de godtas i större utsträckning och öka förtroendet för dem både hos privatpersoner och hos privata tillhandahållare av tjänster. Privata förlitande parter som tillhandahåller tjänster till exempel inom områdena transport, energi, bankväsende och finansiella tjänster, social trygghet, hälso- och sjukvård, dricksvatten, posttjänster, digital infrastruktur, telekommunikation eller utbildning bör därför godta att de europeiska digitala identitetsplånböckerna används i samband med tillhandahållandet av tjänster där en säker autentisering för onlineidentifiering krävs enligt unionsrätten eller nationell rätt eller genom avtalsenliga skyldigheter. Varje begäran som den förlitande parten framställer om information från användaren av en europeisk digital identitetsplånbok bör vara nödvändig för och stå i proportion till den avsedda användningen i ett givet fall, bör vara förenlig med principen om uppgiftsminimering och bör säkerställa transparens när det gäller vilka uppgifter som delas och för vilka ändamål. För att underlätta användningen och godtagandet av europeiska digitala identitetsplånböcker bör allmänt accepterade branschstandarder och specifikationer beaktas när plånböckerna införs.

(57) Om mycket stora onlineplattformar, enligt artikel 33.1 i Europaparlamentets och rådets förordning (EU) 2022/2065[15], kräver att användarna är autentiserade för att få tillgång till nättjänster bör dessa plattformar vara skyldiga att godta användning av europeiska digitala identitetsplånböcker på användarens frivilliga begäran. Användarna bör inte vara tvungna att använda en europeisk digital identitetsplånbok för att få tillgång till privata tjänster, och deras tillgång till tjänster bör inte begränsas eller hindras på grund av att de inte använder en europeisk digital identitetsplånbok. Om användarna emellertid vill göra det, bör stora onlineplattformar godta dem i detta syfte, med iakttagande av principen om uppgiftsminimering och användarnas rätt att använda pseudonymer som de fritt väljer. Med tanke på de mycket stora onlineplattformarnas räckvidd, i synnerhet när det gäller antalet mottagare av tjänsten och antalet ekonomiska transaktioner, är skyldigheten att godta europeiska digitala identitetsplånböcker nödvändig för att öka användarnas skydd mot bedrägerier och säkerställa en hög nivå av dataskydd.

(58) Uppförandekoder på unionsnivå bör utarbetas för att bidra till allmän tillgång till och användbarhet hos medel för elektronisk identifiering, däribland de europeiska digitala identitetsplånböckerna, inom denna förordnings tillämpningsområde. Uppförandekoderna bör underlätta ett brett erkännande av medel för elektronisk identifiering, däribland europeiska digitala identitetsplånböcker, bland de tjänsteleverantörer som inte klassificeras som mycket stora plattformar och som förlitar sig på tredje parts tjänster för elektronisk identifiering för användarautentisering.

---

[15] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

(59) Selektivt utlämnande är ett begrepp som ger dataägaren rätt att endast lämna ut vissa delar av en större datamängd, så att den mottagande enheten endast kan inhämta information som är nödvändig för tillhandahållandet av en tjänst som begärs av en användare. De europeiska digitala identitetsplånböckerna bör ha tekniska egenskaper som möjliggör ett selektivt utlämnande av attribut till förlitande parter. Det bör vara tekniskt möjligt för användaren att selektivt utelämna attribut, inbegripet från flera olika elektroniska intyg, och att kombinera och presentera dem sömlöst för förlitande parter. Denna funktion bör vara en grundläggande inbyggd funktion i europeiska digitala identitetsplånböcker som förstärker bekvämligheten och skyddet av personuppgifter, inbegripet uppgiftsminimering.

(60) Såvida inte särskilda bestämmelser i unionsrätten eller nationell rätt kräver att användarna ska identifiera sig bör åtkomst till tjänster med hjälp av en pseudonym inte förbjudas.

(61) Attribut som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som en del av kvalificerade attributsintyg bör verifieras mot autentiska källor, antingen direkt av den kvalificerade tillhandahållaren av betrodda tjänster eller genom särskilt utsedda mellanhänder som erkänns på nationell nivå i enlighet med unionsrätten eller nationell rätt för ett säkert utbyte av intygade attribut mellan tillhandahållare av identitetslösningar eller attributsintyg och förlitande parter. Medlemsstaterna bör inrätta lämpliga mekanismer på nationell nivå för att säkerställa att sådana kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade elektroniska attributsintyg kan kontrollera, på grundval av samtycke från den person till vilken intyget utfärdas, äktheten hos de attribut som bygger på autentiska källor. Lämpliga mekanismer bör kunna innefatta användningen av särskilda mellanhänder eller tekniska lösningar som i enlighet med nationell rätt ger tillgång till de autentiska källorna. Säkerställandet av tillgång till en mekanism som möjliggör kontroll av attribut mot autentiska källor avser att underlätta för kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade elektroniska attributsintyg att uppfylla sina skyldigheter enligt förordning (EU) nr 910/2014. En ny bilaga till den förordningen bör innehålla en förteckning över kategorier av attribut avseende vilka medlemsstaterna ska säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade tillhandahållare av elektroniska attributsintyg att på användarens begäran på elektronisk väg kontrollera deras äkthet gentemot den relevanta autentiska källan.

(62) Säker elektronisk identifiering och tillhandahållande av attributsintyg bör erbjuda ytterligare flexibilitet och lösningar inom sektorn för finansiella tjänster för att göra det möjligt att identifiera kunder och utbyta särskilda attribut som behövs för att, till exempel, uppfylla kraven på kundkontroll enligt en framtida förordning om inrättande av myndigheten för bekämpning av penningtvätt och lämplighetskraven i lagstiftningen om investerarskydd, eller för att bidra till efterlevnaden av kraven på stark kundautentisering för onlineidentifiering vid kontoinloggning och inledande av transaktioner inom betaltjänstområdet.

(63) Den rättsliga verkan av en elektronisk underskrift ska inte bestridas på den grunden att den är i elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk underskrift. Det är dock i nationell rätt som den rättsliga verkan av elektroniska underskrifter ska fastställas, med undantag för de krav som föreskrivs i denna förordning, enligt vilka den rättsliga verkan av en kvalificerad elektronisk underskrift ska anses vara likvärdig med en handskriven underskrift. Vid fastställandet av elektroniska underskrifters rättsliga verkan bör medlemsstaterna beakta principen om proportionalitet mellan det rättsliga värdet av en handling som ska undertecknas och den säkerhetsnivå och kostnad som en elektronisk underskrift kräver. För att öka tillgängligheten till och användningen av elektroniska underskrifter uppmuntras medlemsstaterna att överväga användningen av avancerade elektroniska underskrifter för de dagliga transaktioner för vilka de tillhandahåller en tillräcklig nivå av säkerhet och tillförlitlighet.

(64) För att säkerställa enhetliga certifieringsmetoder i hela unionen bör kommissionen utfärda riktlinjer för certifiering och omcertifiering av kvalificerade anordningar för skapande av elektroniska underskrifter och kvalificerade anordningar för skapande av elektroniska stämplar, inbegripet vad gäller deras giltighet och tidsbegränsningar. Denna förordning hindrar inte de offentliga eller privata organ som har certifierade kvalificerade anordningar för skapande av elektroniska underskrifter från att omcertifiera sådana anordningar för en kort certifieringsperiod, baserat på resultaten av den föregående certifieringsprocessen, om en sådan omcertifiering inte kan utföras inom den rättsligt fastställda tidsramen av ett annat skäl än en överträdelse eller en säkerhetsincident, utan att det påverkar skyldigheten att utföra en sårbarhetsbedömning och utan att det påverkar tillämplig certifieringspraxis.

(65) Utfärdandet av certifikat för autentisering av webbplatser är avsett att ge användarna tillit, med en hög tillförlitlighetsnivå när det gäller identiteten hos den enhet som står bakom webbplatsen, oavsett vilken plattform som används för att visa identiteten. Dessa certifikat bör bidra till att bygga upp förtroendet för näthandeln, eftersom användarna kan förväntas hysa tillit till en webbplats som har autentiserats. Användningen av sådana certifikat bör vara frivillig. För att autentiseringen av webbplatser ska kunna bli ett sätt att stärka förtroendet, ge användaren en bättre upplevelse och främja tillväxten på den inre marknaden fastställs i denna förordning ett tillitsramverk som innefattar minimiskyldigheter vad gäller säkerhet och skadeståndsansvar för tillhandahållare av kvalificerade certifikat för autentisering av webbplatser och krav i fråga om utfärdandet av dessa certifikat. Nationella förteckningar över betrodda tjänsteleverantörer bör bekräfta att tjänster för autentisering av webbplatser och deras tillhandahållare av betrodda tjänster har status som kvalificerade, inbegripet att de fullt ut följer kraven i denna förordning när det gäller utfärdande av kvalificerade certifikat för autentisering av webbplatser. Erkännandet av kvalificerade certifikat för autentisering av webbplatser innebär att tillhandahållare av webbläsare inte bör neka äktheten hos kvalificerade certifikat för autentisering av webbplatser vars enda i syfte är att intyga kopplingen mellan webbplatsens domännamn och den fysiska eller juridiska person till vilken certifikatet är utfärdat eller bekräfta den personens identitet. Tillhandahållare av webbläsare bör visa de certifierade identitetsuppgifterna och de andra intygade attributen för slutanvändaren på ett användarvänligt sätt i webbläsarmiljön genom valfria tekniska medel. För detta ändamål bör tillhandahållare av webbläsare säkerställa stöd och interoperabilitet med kvalificerade certifikat för autentisering av webbplatser som utfärdats i fullständig överensstämmelse med denna förordning.

Den skyldighet som innebär erkännande av och kompatibilitet med samt stöd för kvalificerade certifikat för autentisering av webbplatser påverkar inte friheten för tillhandahållare av webbläsare att säkerställa webbsäkerhet, domänautentisering och kryptering av webbtrafik på ett sätt och med hjälp av den teknik som de anser lämpligast. För att bidra till slutanvändarnas onlinesäkerhet bör tillhandahållare av webbläsare i undantagsfall kunna vidta säkerhetsåtgärder som är både nödvändiga och proportionella som en reaktion på välgrundade farhågor om säkerhetsincidenter eller integritetsförluster hos ett identifierat certifikat eller en identifierad uppsättning certifikat. Om tillhandahållare av webbläsare vidtar sådana säkerhetsåtgärder bör de, utan onödigt dröjsmål, underrätta kommissionen, det nationella tillsynsorganet om vilken enhet certifikatet utfärdades till och vilken kvalificerad tillhandahållare av betrodda tjänster som utfärdade certifikatet eller uppsättningen certifikat, om alla farhågor med avseende på en sådan säkerhetsincident eller integritetsförlust samt om vilka åtgärder som vidtagits avseende det enskilda certifikatet eller uppsättningen certifikat. Dessa åtgärder bör inte påverka den skyldighet som tillhandahållare av webbläsare har att erkänna kvalificerade certifikat för autentisering av webbplatser i enlighet med de nationella förteckningarna över betrodda tjänsteleverantörer. För att ytterligare skydda unionsmedborgare och invånare i unionen och främja användningen av kvalificerade certifikat för autentisering av webbplatser bör medlemsstaternas offentliga myndigheter överväga att införa kvalificerade certifikat för autentisering av webbplatser på sina egna webbplatser. De åtgärder som föreskrivs i denna förordning som syftar till att skapa ökad samstämmighet mellan medlemsstaternas skilda tillvägagångssätt och praxis när det gäller tillsynsförfaranden är avsedda att bidra till större förtroende och tillit för säkerhet, kvalitet och tillgänglighet avseende kvalificerade certifikat för autentisering av webbplatser.

(66) Många medlemsstater har infört nationella krav för tjänster som tillhandahåller säker och tillförlitlig elektronisk arkivering för att möjliggöra långsiktig lagring av elektroniska uppgifter och elektroniska dokument och tillhörande betrodda tjänster. För att säkerställa rättssäkerhet, förtroende och harmonisering mellan medlemsstaterna bör en rättslig ram för kvalificerade elektroniska arkiveringstjänster inrättas, och den bör inspireras av ramen för de andra betrodda tjänster som föreskrivs i denna förordning. Den rättsliga ramen för kvalificerade elektroniska arkiveringstjänster bör erbjuda tillhandahållare och användare av betrodda tjänster en effektiv verktygslåda som omfattar funktionskrav för den elektroniska arkiveringstjänsten samt tydlig rättslig verkan när en kvalificerad elektronisk arkiveringstjänst används. Bestämmelserna bör vara tillämpliga på elektroniska uppgifter och elektroniska dokument skapade i elektronisk form liksom på pappersdokument som har skannats och digitaliserats. När så krävs bör bestämmelserna tillåta att bevarade elektroniska uppgifter och elektroniska dokument överförs till olika medier eller format i syfte att förlänga deras hållbarhet och läsbarhet bortom den tekniska giltighetstiden, samtidigt som förluster och ändringar förhindras i möjligaste mån. När elektroniska data och elektroniska dokument som lämnas till den elektroniska arkiveringstjänsten innehåller en eller flera kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar bör tjänsten använda förfaranden och teknik som kan förlänga deras tillförlitlighet under bevarandeperioden för sådana uppgifter, eventuellt genom användning av andra kvalificerade betrodda tjänster som inrättas genom denna förordning. För att skapa bevarandebevis när elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar används bör kvalificerade betrodda tjänster användas. I den mån som elektroniska arkiveringstjänster inte harmoniseras genom denna förordning bör medlemsstaterna kunna behålla eller införa nationella bestämmelser, i enlighet med unionsrätten, som rör dessa tjänster, såsom särskilda bestämmelser för tjänster som är integrerade i en organisation och som endast används för den organisationens interna arkiv. Denna förordning bör inte göra skillnad på elektroniska uppgifter och elektroniska dokument skapade i elektronisk form och fysiska dokument som har digitaliserats.

(67) Nationella arkivs och minnesinstitutioners verksamhet regleras, i egenskap av organisationer som arbetar med att bevara det dokumenterade arvet i allmänhetens intresse, vanligtvis i nationell rätt och tillhandahåller inte nödvändigtvis betrodda tjänster i den mening som avses i denna förordning. I den mån sådana institutioner inte tillhandahåller sådana betrodda tjänster ska denna förordning inte påverka deras verksamhet.

(68) Elektroniska liggare är en sekvens av elektroniska dataloggar som bör säkerställa dataintegriteten och riktigheten i deras kronologiska ordning. Elektroniska liggare bör upprätta en kronologisk sekvens av dataloggar. Tillsammans med annan teknik bör de bidra till lösningar för effektivare och omdanande offentliga tjänster såsom elektronisk röstning, gränsöverskridande samarbete mellan tullmyndigheter, gränsöverskridande samarbete mellan akademiska institutioner och registrering av äganderätt till fastigheter i decentraliserade fastighetsregister. Kvalificerade elektroniska liggare bör skapa en legal presumtion för den unika och korrekta sekventiella kronologiska ordningsföljden och integriteten hos dataloggarna i liggaren. På grund av sina specifika egenskaper, såsom den sekventiella kronologiska ordningsföljden för dataloggar, bör elektroniska liggare skiljas från andra betrodda tjänster såsom elektroniska tidsstämplingar och elektroniska tjänster för rekommenderade leveranser. För att säkerställa rättssäkerhet och främja innovation bör en unionsomfattande rättslig ram inrättas som föreskriver ett gränsöverskridande erkännande av betrodda tjänster för registrering av uppgifter i elektroniska liggare. Detta bör i tillräcklig utsträckning kunna förhindra att samma digitala tillgång kopieras och säljs mer än en gång till olika parter. Processen för att skapa och uppdatera en elektronisk liggare beror på vilken typ av liggare som används, nämligen om den är centraliserad eller distribuerad. Denna förordning bör säkerställa teknikneutralitet, dvs. varken gynna eller diskriminera någon teknik som används för att genomföra den nya betrodda tjänsten för elektroniska liggare. Dessutom bör hållbarhetsindikatorer för eventuella negativa effekter på klimatet eller andra miljörelaterade negativa effekter beaktas av kommissionen, med hjälp av lämpliga metoder, när den utarbetar de genomförandeakter där kraven för kvalificerade elektroniska liggare specificeras.

(69) Rollen för tillhandahållare av betrodda tjänster för elektroniska liggare bör vara att säkerställa den sekventiella registreringen av uppgifter i liggaren. Denna förordning påverkar inte eventuella rättsliga skyldigheter som användare av elektroniska liggare har enligt unionsrätten eller nationell rätt. Till exempel bör användningsfall som inbegriper behandlingen av personuppgifter uppfylla kraven i förordning (EU) 2016/679 och användningsfall som rör finansiella tjänster bör uppfylla kraven i relevant unionsrätt om finansiella tjänster.

(70) För att undvika fragmentering och hinder på den inre marknaden på grund av varierande standarder och tekniska begränsningar, och för att säkerställa en samordnad process för att undvika att genomförandet av det europeiska ramverket för digital identitet påverkas, krävs det ett förfarande för ett nära och strukturerat samarbete mellan kommissionen, medlemsstaterna, civilsamhället, den akademiska världen och den privata sektorn. För att uppnå detta mål bör medlemsstaterna och kommissionen samarbeta inom den ram som fastställs i kommissionens rekommendation (EU) 2021/946[16] för att utarbeta en unionsgemensam verktygslåda för det europeiska ramverket för digital identitet. I detta sammanhang bör medlemsstaterna enas om en övergripande teknisk arkitektur och referensram, ett antal gemensamma standarder och tekniska referenser inbegripet erkända befintliga standarder samt en uppsättning riktlinjer och beskrivningar av bästa praxis som åtminstone omfattar all funktionalitet och interoperabilitet hos europeiska digitala identitetsplånböcker, inklusive elektroniska underskrifter, och hos tillhandahållaren av kvalificerade betrodda tjänster för elektroniska attributsintyg som fastställs i denna förordning. I detta sammanhang bör medlemsstaterna även komma överens om gemensamma inslag i en affärsmodell och en avgiftsstruktur för europeiska digitala identitetsplånböcker för att underlätta användningen, i synnerhet för små och medelstora företag i gränsöverskridande sammanhang. Innehållet i verktygslådan bör utvecklas parallellt med och återspegla resultatet av diskussionen och processen för antagandet av det europeiska ramverket för digital identitet.

---

[16] Kommissionens rekommendation (EU) 2021/946 av den 3 juni 2021 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet (EUT L 210, 14.6.2021, s. 51).

(71) Denna förordning föreskriver en harmoniserad nivå av kvalitet, tillförlitlighet och säkerhet när det gäller kvalificerade betrodda tjänster, oavsett var verksamheten bedrivs. En kvalificerad tillhandahållare av betrodda tjänster bör därför ha rätt att lägga ut sin verksamhet vad gäller tillhandahållandet av en kvalificerad betrodd tjänst på entreprenad i ett tredje land, om det tredje landet tillhandahåller tillräckliga garantier och säkerställer att tillsynsverksamhet och revisioner kan verkställas som om de hade bedrivits i unionen. Om efterlevnaden av denna förordning inte kan garanteras fullt ut bör tillsynsorganen kunna vidta proportionella och motiverade åtgärder, inbegripet återkallande av den tillhandahållna betrodda tjänstens status som kvalificerad.

(72) För att säkerställa rättssäkerhet vad gäller giltigheten för avancerade elektroniska underskrifter baserade på kvalificerade certifikat är det viktigt att bedömningen av den förlitande part som utför valideringen av den avancerade elektroniska underskriften baserad på kvalificerade certifikat specificeras.

(73) Tillhandahållare av betrodda tjänster bör använda krypteringsmetoder som återspeglar rådande bästa praxis och tillförlitliga tillämpningar av dessa algoritmer för att säkerställa säkerheten och tillförlitligheten hos sina betrodda tjänster.

(74) I denna förordning fastställs en skyldighet för kvalificerade tillhandahållare av betrodda tjänster att kontrollera identiteten på en fysisk eller juridisk person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska attributsintyget utfärdas på grundval av olika harmoniserade metoder i hela unionen. För att säkerställa att kvalificerade certifikat och kvalificerade elektroniska attributsintyg utfärdas till den person som de tillhör och att de intygar den korrekta och unika uppsättning uppgifter som representerar den personens identitet, bör kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat eller utfärdar kvalificerade elektroniska attributsintyg, vid tidpunkten för utfärdandet av dessa certifikat och intyg med full säkerhet säkerställa identifieringen av den personen. Utöver den obligatoriska kontrollen av personens identitet, i tillämpliga fall för utfärdande av kvalificerade certifikat och vid utfärdande av ett kvalificerat elektroniskt attributsintyg, bör kvalificerade tillhandahållare av betrodda tjänster med full säkerhet säkerställa att de intygade attributen för den person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska attributsintyget utfärdas är korrekta och riktiga. Dessa krav på resultat och full säkerhet vid kontrollen av de intygade uppgifterna bör stödjas på lämpligt sätt, bland annat genom användning av en eller, när så krävs, en kombination av specifika metoder som föreskrivs i denna förordning. Det bör vara möjligt att kombinera dessa metoder för att ge en lämplig grund för kontroll av identiteten på den person till vilken det kvalificerade certifikatet eller ett kvalificerat elektroniskt attributsintyg utfärdas. En sådan kombination bör kunna innefatta användning av medel för elektronisk identifiering som uppfyller kraven på tillitsnivå väsentlig i kombination med andra metoder för identitetskontroll som skulle göra det möjligt att uppfylla de harmoniserade kraven i denna förordning vad gäller tillitsnivå hög som en del av ytterligare harmoniserade distansförfaranden och säkerställa identifiering med en hög tillförlitlighetsnivå. Dessa metoder bör inbegripa möjligheten för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar ett kvalificerat elektroniskt attributsintyg att kontrollera de attribut som ska intygas på elektronisk väg på användarens begäran, i enlighet med unionsrätten eller nationell rätt, inbegripet mot autentiska källor.

(75) För att hålla denna förordning i linje med den globala utvecklingen och för att följa praxis på den inre marknaden bör de delegerade akter och genomförandeakter som antas av kommissionen ses över och vid behov uppdateras regelbundet. Vid bedömningen av behovet av dessa uppdateringar bör hänsyn tas till ny teknik och nya metoder, standarder eller tekniska specifikationer.

(76) Eftersom målen för denna förordning, nämligen utvecklingen av det unionsomfattande europeiska ramverket för digital identitet och av ett ramverk för betrodda tjänster, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av deras omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå dessa mål.

(77) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725.

(78) Förordning (EU) nr 910/2014 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av förordning (EU) nr 910/2014

Förordning (EU) nr 910/2014 ska ändras på följande sätt:

1. Artikel 1 ska ersättas med följande:

”*Artikel 1*

Innehåll

Denna förordning syftar till att säkerställa en väl fungerande inre marknad och tillhandahålla en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster som används i hela unionen i syfte att möjliggöra och underlätta fysiska och juridiska personers utövande av rätten att delta i det digitala samhället på ett säkert sätt och att ha tillgång till offentliga och privata nättjänster i hela unionen. För dessa ändamål fastställs i denna förordning

a) de villkor enligt vilka medlemsstaterna ska erkänna fysiska och juridiska personers medel för elektronisk identifiering som omfattas av en annan medlemsstats anmälda system för elektronisk identifiering och tillhandahålla och erkänna europeiska digitala identitetsplånböcker,

b) regler för betrodda tjänster, i synnerhet för elektroniska transaktioner,

c) en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser, certifikattjänster för autentisering av webbplatser, elektronisk arkivering och elektroniska attributsintyg, anordningar för skapande av elektroniska underskrifter, anordningar för skapande av elektroniska stämplar samt elektroniska liggare.”

2. Artikel 2 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Denna förordning är tillämplig på system för elektronisk identifiering som har anmälts av en medlemsstat, på europeiska digitala identitetsplånböcker som tillhandahålls av en medlemsstat och på tillhandahållare av betrodda tjänster som är etablerade inom unionen.”

b) Punkt 3 ska ersättas med följande:

”3. Denna förordning påverkar inte unionsrätt eller nationell rätt som avser ingående av avtal och avtalens giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende form, eller sektorsspecifika krav avseende form.

4. Denna förordning påverkar inte tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679*.

---

* Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).”

3. Artikel 3 ska ändras på följande sätt:

a) Leden 1–5 ska ersättas med följande:

”1. *elektronisk identifiering*: en process inom vilken uppgifter för personidentifiering i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person, används.

2. *medel för elektronisk identifiering*: en materiell och/eller immateriell enhet som innehåller uppgifter för personidentifiering och som används för autentisering för en nättjänst eller, i tillämpliga fall, för en offlinetjänst.

3. *uppgifter för personidentifiering*: en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller på en fysisk person som företräder en annan fysisk person eller en juridisk person.

4. *system för elektronisk identifiering*: ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person.

5. *autentisering*: en elektronisk process som gör det möjligt att bekräfta en fysisk eller juridisk persons elektroniska identifiering eller att bekräfta ursprunget för och integriteten hos uppgifter i elektronisk form.”

b) Följande led ska införas:

”5a. *användar*e: en fysisk eller juridisk person, eller en fysisk person som företräder en annan fysisk person eller en juridisk person, som använder betrodda tjänster eller medel för elektronisk identifiering som tillhandahålls i enlighet med denna förordning.”

c) Led 6 ska ersättas med följande:

”6. *förlitande part*: en fysisk eller juridisk person som förlitar sig på elektronisk identifiering, europeiska digitala identitetsplånböcker eller andra medel för elektronisk identifiering eller på en betrodd tjänst.”

d) Led 16 ska ersättas med följande:

”16. *betrodd tjänst*: en elektronisk tjänst som vanligen tillhandahålls mot ersättning och som består av något av följande:

a) Utfärdande av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplar, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster.

b) Validering av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplar, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster.

c) Skapande av elektroniska underskrifter eller elektroniska stämplar.

d) Validering av elektroniska underskrifter eller elektroniska stämplar.

e) Bevarande av elektroniska underskrifter, elektroniska stämplar, certifikat för elektroniska underskrifter eller certifikat för elektroniska stämplar.

f) Förvaltning av anordningar för skapande av elektroniska underskrifter på distans eller anordningar för skapande av elektroniska stämplar på distans.

g) Utfärdande av elektroniska attributsintyg.

h) Validering av elektroniska attributsintyg.

i) Skapande av elektroniska tidsstämplingar.

j) Validering av elektroniska tidsstämplingar.

k) Tillhandahållande av elektroniska tjänster för rekommenderade leveranser.

l) Validering av data som överförs via elektroniska tjänster för rekommenderade leveranser och tillhörande bevis.

m) Elektronisk arkivering av elektroniska uppgifter och elektroniska dokument.

n) Registrering av elektroniska uppgifter i en elektronisk liggare.”

e) Led 18 ska ersättas med följande:

”18. *organ för bedömning av överensstämmelse*: ett organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat som behörigt att utföra bedömning av överensstämmelse av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller, eller som behörigt att utföra certifiering av europeiska digitala identitetsplånböcker eller medel för elektronisk identifiering.”

f) Led 21 ska ersättas med följande:

”21. *produkt*: maskinvara eller programvara, eller relevanta komponenter i maskinvara eller programvara, som är avsedda att användas för tillhandahållande av elektronisk identifiering och betrodda tjänster.”

g) Följande led ska läggas till:

”23a. *kvalificerad anordning för skapande av elektroniska underskrifter på distans*: en kvalificerad anordning för skapande av elektroniska underskrifter som förvaltas av en kvalificerad tillhandahållare av betrodda tjänster i enlighet med artikel 29a för undertecknarens räkning.

23b. *kvalificerad anordning för skapande av elektroniska stämplar på distans*: en kvalificerad anordning för skapande av elektroniska stämplar som förvaltas av en kvalificerad tillhandahållare av betrodda tjänster i enlighet med artikel 39a för stämpelskaparens räkning. ”

h) Led 38 ska ersättas med följande:

”38. *certifikat för autentisering av webbplatser*: ett elektroniskt intyg som gör det möjligt att autentisera en webbplats och kopplar webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.”

i) Led 41 ska ersättas med följande:

”41. *validering*: en process genom vilken det kontrolleras och bekräftas att data i elektronisk form är giltiga i enlighet med denna förordning.”

j) Följande led ska läggas till:

”42. *europeisk digital identitetsplånbok*: ett medel för elektronisk identifiering som gör det möjligt för användaren att på ett säkert sätt lagra, hantera och validera personidentitetsuppgifter och elektroniska attributsintyg i syfte att tillhandahålla dem till förlitande parter och andra användare av europeiska digitala identitetsplånböcker, och att underteckna med kvalificerade elektroniska underskrifter eller att stämpla med kvalificerade elektroniska stämplar.

43. *attribut*: en egenskap, en kvalitet, en rättighet eller ett tillstånd för en fysisk eller juridisk person eller ett föremål.

44. *elektroniskt attributsintyg*: ett intyg i elektronisk form som möjliggör autentisering av attribut.

45. *kvalificerat elektroniskt attributsintyg*: ett elektroniskt attributsintyg som är utfärdat av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga V.

46. *elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa*: ett elektroniskt attributsintyg utfärdat av ett offentligt organ som ansvarar för en autentisk källa eller av ett offentligt organ som utsetts av medlemsstaten för att utfärda sådana attributsintyg på uppdrag av de offentliga organ som ansvarar för autentiska källor i enlighet med artikel 45f och med bilaga VII.

47. *autentisk källa*: samlingsplats eller system, som innehas under ansvar av ett offentligt organ eller en privat enhet, som innehåller och tillhandahåller attribut om en fysisk eller juridisk person eller ett föremål och som anses vara en primärkälla för den informationen eller erkänns som autentisk i enlighet med unionsrätten eller nationell rätt, inbegripet administrativa förfaranden.

48. *elektronisk arkivering*: en tjänst som säkerställer mottagande, lagring, hämtning och radering av elektroniska uppgifter och elektroniska dokument i syfte att säkerställa deras hållbarhet och läsbarhet samt att bevara deras integritet, konfidentialitet och ursprungsbevis under hela bevarandeperioden.

49. *kvalificerad elektronisk arkiveringstjänst*: en elektronisk arkiveringstjänst som tillhandahålls av en kvalificerad tillhandahållare av betrodda tjänster och som uppfyller de krav som fastställs i artikel 45j.

50. *EU:s förtroendemärke för digitala identitetsplånböcker*: en kontrollerbar enkel och igenkännlig angivelse, visad på ett tydligt sätt, som meddelar att en europeisk digital identitetsplånbok har tillhandahållits i enlighet med denna förordning.

51. *stark användarautentisering*: en autentisering som är baserad på användningen av åtminstone två autentiseringsfaktorer från olika kategorier av antingen kunskap (något som endast användaren känner till), besittning (något som endast användaren besitter) eller unik egenskap (något som användaren är) som är oberoende av varandra på ett sådant sätt att en incident avseende en av faktorerna inte äventyrar tillförlitligheten hos de andra, och som är utformad för att skydda konfidentialiteten för autentiseringsdata.

52. *elektronisk liggare*: en sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i dessa loggars kronologiska ordning.

53. *kvalificerad elektronisk liggare*: en elektronisk liggare som tillhandahålls av en kvalificerad tillhandahållare av betrodda tjänster och som uppfyller de krav som fastställs i artikel 45l.

54. *personuppgifter*: varje upplysning enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

55. *identitetsmatchning*: en process där uppgifter för personidentifiering eller medel för elektronisk identifiering matchas mot eller kopplas till ett befintligt konto som tillhör samma person.

56. *datalogg*: elektroniska uppgifter som registrerats med tillhörande metadata som stöder behandlingen av dessa data.

57. *offlineläge*: i fråga om användningen av europeiska digitala identitetsplånböcker, en interaktion mellan en användare och en tredje part på en fysisk plats med beröringsfri teknik, där det inte krävs att den europeiska digitala identitetsplånboken har åtkomst till system på distans via elektroniska kommunikationsnätverk för att genomföra interaktionen.”

4. Artikel 5 ska ersättas med följande:

”*Artikel 5*
Pseudonymer vid elektroniska transaktioner

Utan att det påverkar tillämpningen av särskilda bestämmelser i unionsrätten eller nationell rätt som kräver att användarna ska identifiera sig, eller pseudonymers rättsverkan enligt nationell rätt, ska användning av pseudonymer valda av användaren inte vara förbjuden.”

5. I kapitel II ska följande avsnitt införas:

”AVSNITT 1
EUROPEISK DIGITAL IDENTITETSPLÅNBOK

Artikel 5a
Europeiska digitala identitetsplånböcker

1. För att säkerställa att alla fysiska och juridiska personer i unionen har säker, tillitsbaserad och sömlös gränsöverskridande tillgång till offentliga och privata tjänster, samtidigt som de har full kontroll över sina uppgifter, ska varje medlemsstat tillhandahålla åtminstone en europeisk digital identitetsplånbok inom 24 månader från det att de genomförandeakter som avses i punkt 23 i denna artikel och i artikel 5c.6 träder i kraft.

2. Europeiska digitala identitetsplånböcker ska tillhandahållas på ett eller flera av följande sätt:

   a) Direkt av en medlemsstat.

   b) På uppdrag av en medlemsstat.

   c) Oberoende av en medlemsstat men med den medlemsstatens erkännande.

3. Källkoden för programvarukomponenterna i europeiska digitala identitetsplånböcker ska vara licensierad med öppen källkod. Medlemsstaterna får föreskriva att källkoden för andra specifika komponenter än de som installeras på användarenheter inte ska lämnas ut om det föreligger vederbörligen motiverade skäl.

4. Europeiska digitala identitetsplånböcker ska göra det möjligt för användaren att, på ett sätt som är användarvänligt, transparent och spårbart för användaren,

a) på ett säkert sätt kunna begära, erhålla, välja, kombinera, lagra, radera, dela och visa, under användarens egen kontroll, uppgifter för personidentifiering och, i tillämpliga fall, i kombination med elektroniska attributsintyg, autentisera gentemot förlitande parter online och, i lämpliga fall, i offlineläge, i syfte att få tillgång till offentliga och privata tjänster, samtidigt som det säkerställs att selektivt utlämnande av data är möjligt,

b) generera pseudonymer och lagra dem i krypterad form lokalt i den europeiska digitala identitetsplånboken,

c) på ett säkert sätt autentisera en annan persons europeiska digitala identitetsplånbok och ta emot och dela uppgifter för personidentifierings och elektroniska attributsintyg på ett säkert sätt mellan de två europeiska digitala identitetsplånböckerna,

d) få tillgång till en logg över alla transaktioner som utförs genom den europeiska digitala identitetsplånboken via en gemensam instrumentpanel som gör det möjligt för användaren att

i) se en uppdaterad förteckning över förlitande parter med vilka användaren har upprättat en förbindelse och, i tillämpliga fall, alla utbytta uppgifter,

ii) på ett enkelt sätt begära att en förlitande part raderar personuppgifter enligt artikel 17 i förordning (EU) 2016/679,

iii) på ett enkelt sätt rapportera en förlitande part till den behöriga nationella dataskyddsmyndigheten, om en påstått olaglig eller misstänkt begäran om uppgifter tas emot,

e) underteckna med kvalificerade elektroniska underskrifter eller stämpla med kvalificerade elektroniska stämplar,

f) i den mån det är tekniskt möjligt ladda ned användarens uppgifter, elektroniska attributsintyg och konfigurationer,

g) utöva användarens rättigheter till dataportabilitet.

5. Europeiska digitala identitetsplånböcker ska i synnerhet

a) stödja gemensamma protokoll och gränssnitt

i) för utfärdande av uppgifter för personidentifiering, kvalificerade och icke-kvalificerade elektroniska attributsintyg eller kvalificerade och icke-kvalificerade certifikat till den europeiska digitala identitetsplånboken,

ii) för att förlitande parter ska kunna begära och validera uppgifter för personidentifiering och elektroniska attributsintyg,

iii) för delning och visning av uppgifter för personidentifiering, elektroniska attributsintyg eller selektivt utlämnade relaterade uppgifter för förlitande parter online och, när så är lämpligt, i offlineläge,

iv) för att användaren ska kunna tillåta interaktion med den europeiska digitala identitetsplånboken och visa upp EU:s förtroendemärke för digitala identitetsplånböcker,

v) för säker anslutning av användaren genom användning av ett medel för elektronisk identifiering i enlighet med artikel 5a.24,

vi) för interaktion mellan två personers europeiska digitala identitetsplånböcker i syfte att ta emot, validera och dela uppgifter för personidentifiering och elektroniska attributsintyg på ett säkert sätt,

vii) för autentisering och identifiering av förlitande parter genom att autentiseringsmekanismer genomförs i enlighet med artikel 5b,

viii) för att förlitande parter ska kunna kontrollera europeiska digitala identitetsplånböckers äkthet och giltighet,

ix) för att begära att en förlitande part raderar personuppgifter enligt artikel 17 i förordning (EU) 2016/679,

x) för rapportering av en förlitande part till den behöriga nationella dataskyddsmyndigheten i fall då en påstått olaglig eller misstänkt begäran om data tas emot,

xi) för skapande av kvalificerade elektroniska underskrifter eller elektroniska stämplar genom anordningar för skapande av kvalificerade elektroniska underskrifter eller elektroniska stämplar,

b) inte ge någon information till tillhandahållare av betrodda tjänster som tillhandahåller elektroniska attributsintyg om användningen av dessa elektroniska intyg,

c) säkerställa att förlitande parter kan autentiseras och identifieras genom att autentiseringsmekanismer genomförs i enlighet med artikel 5b,

d) uppfylla de krav som fastställs i artikel 8 vad gäller tillitsnivå hög, särskilt när den tillämpas på kraven för styrkande och kontroll av identitet, och förvaltning och autentisering av medel för elektronisk identifiering,

e) införa, i fråga om elektroniska attributsintyg med inbyggda policyer för utlämnande, en lämplig mekanism för att informera användaren om att den förlitande parten eller den användare av den europeiska digitala identitetsplånboken som begär det elektroniska attributsintyget har tillstånd att få tillgång till intyget,

f) säkerställa att de uppgifter för personidentifiering som är tillgängliga från det system för elektronisk identifiering under vilket den europeiska digitala identitetsplånboken tillhandahålls, på ett unikt sätt avser den fysiska personen, den juridiska personen eller den fysiska person som företräder den fysiska eller juridiska personen, och är kopplade till den europeiska digitala identitetsplånboken,

g) ge alla fysiska personer möjlighet att som utgångspunkt och kostnadsfritt underteckna med kvalificerade elektroniska underskrifter.

Trots första stycket g får medlemsstaterna föreskriva proportionella åtgärder för att säkerställa att fysiska personers kostnadsfria användning av kvalificerade elektroniska underskrifter är begränsad till icke-yrkesmässiga ändamål.

6. Medlemsstaterna ska utan dröjsmål informera användare om eventuella säkerhetsincidenter som helt eller delvis kan ha äventyrat deras europeiska digitala identitetsplånbok eller dess innehåll, särskilt om deras europeiska digitala identitetsplånbok har upphävts tillfälligt eller återkallats enligt artikel 5e,

7. Utan att det påverkar tillämpningen av artikel 5f får medlemsstaterna, i enlighet med nationell rätt, föreskriva ytterligare funktioner för europeiska digitala identitetsplånböcker, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering. Dessa ytterligare funktioner ska överensstämma med den här artikeln.

8. Medlemsstaterna ska tillhandahålla valideringsmekanismer kostnadsfritt i syfte att

   a) säkerställa att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras,

   b) göra det möjligt för användare att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5b.

9. Medlemsstaterna ska säkerställa att den europeiska digitala identitetsplånbokens giltighet kan återkallas

   a) på användarens uttryckliga begäran,

   b) när den europeiska digitala identitetsplånbokens säkerhet har äventyrats,

   c) vid användarens död eller när den juridiska personen upphör med sin verksamhet.

10. Tillhandahållare av europeiska digitala identitetsplånböcker ska säkerställa att användarna enkelt kan begära tekniskt stöd och rapportera tekniska problem eller andra incidenter som har en negativ inverkan på användningen av europeiska digitala identitetsplånböcker.

11. Europeiska digitala identitetsplånböcker ska tillhandahållas enligt ett system för elektronisk identifiering med tillitsnivå hög.

12. Europeiska digitala identitetsplånböcker ska säkerställa inbyggd säkerhet.

13. Utfärdandet, användningen och återkallandet av europeiska digitala identitetsplånböcker ska vara utan kostnad för alla fysiska personer.

14. Användarna ska ha full kontroll över användningen av, och uppgifterna i, sin europeiska digitala identitetsplånbok. Tillhandahållaren av den europeiska digitala identitetsplånboken får varken samla in sådan information om användningen av den europeiska digitala identitetsplånboken som inte är nödvändig för tillhandahållandet av tjänster relaterade till den europeiska digitala identitetsplånboken eller kombinera uppgifter för personidentifiering eller några andra personuppgifter som lagras eller som rör användningen av den europeiska digitala identitetsplånboken med personuppgifter från andra tjänster som erbjuds av den tillhandahållaren eller från tredjepartstjänster och som inte krävs för tillhandahållandet av tjänster relaterade till den europeiska digitala identitetsplånboken, om inte användaren uttryckligen har begärt detta. Personuppgifter som rör tillhandahållandet av den europeiska digitala identitetsplånboken ska hållas logiskt avskilda från andra data som innehas av tillhandahållaren av europeiska digitala identitetsplånböcker. Om den europeiska digitala identitetsplånboken tillhandahålls av privata parter i enlighet med punkt 2 b och c i denna artikel, ska bestämmelserna i artikel 45h.3 gälla i tillämpliga delar.

15. Användningen av europeiska digitala identitetsplånböcker ska vara frivillig. Tillgången till offentliga och privata tjänster, tillträdet till arbetsmarknaden och näringsfriheten får inte på något sätt begränsas eller göras ofördelaktiga för fysiska eller juridiska personer som inte använder europeiska digitala identitetsplånböcker. Det ska alltjämt vara möjligt att få tillgång till offentliga och privata tjänster med hjälp av andra befintliga medel för identifiering och autentisering.

16. Det tekniska ramverket för den europeiska digitala identitetsplånboken ska

    a) inte tillåta tillhandahållare av elektroniska attributsintyg eller någon annan part att, efter utfärdandet av attributsintyget, erhålla data som gör det möjligt att spåra, länka, korrelera transaktioner eller användarbeteende eller på annat sätt få kännedom om transaktioner eller användarbeteende, såvida inte användaren uttryckligen har gett sitt tillstånd till detta,

    b) möjliggöra integritetsbevarande teknik som säkerställer att länkning är omöjlig, om attributsintyget inte kräver identifiering av användaren.

17. All behandling av personuppgifter som utförs av medlemsstaterna eller på deras vägnar av organ eller parter som ansvarar för tillhandahållandet av europeiska digitala identitetsplånböcker som medel för elektronisk identifiering ska utföras i enlighet med lämpliga och effektiva dataskyddsåtgärder. Behandlingens förenlighet med förordning (EU) 2016/679 ska visas. Medlemsstaterna får införa nationella bestämmelser för att ytterligare specificera tillämpningen av sådana åtgärder.

18. Medlemsstaterna ska utan onödigt dröjsmål informera kommissionen om

a) det organ som ansvarar för att upprätta och underhålla förteckningen över registrerade förlitande parter som förlitar sig på de europeiska digitala identitetsplånböckerna i enlighet med artikel 5b.5 och var den förteckningen finns tillgänglig,

b) de organ som ansvarar för tillhandahållandet av de europeiska digitala identitetsplånböckerna i enlighet med artikel 5a.1,

c) de organ som ansvarar för att säkerställa att uppgifterna för personidentifiering är kopplade till den europeiska digitala identitetsplånboken i enlighet med artikel 5a.5 f,

d) den mekanism som gör det möjligt att validera de uppgifter för personidentifiering som avses i artikel 5a.5 f och de förlitande parternas identitet,

e) mekanismen för validering av de europeiska digitala identitetsplånböckernas äkthet och giltighet.

Kommissionen ska göra den information som avses i första stycket tillgänglig för allmänheten genom en säker kanal i elektroniskt undertecknad eller stämplad form som lämpar sig för automatiserad behandling.

19. Utan att det påverkar tillämpningen av punkt 22 i denna artikel ska artikel 11 i tillämpliga delar gälla för den europeiska digitala identitetsplånboken.

20. Artikel 24.2 b och d–h ska gälla i tillämpliga delar för tillhandahållare av europeiska digitala identitetsplånböcker.

21. Europeiska digitala identitetsplånböcker ska göras tillgängliga för användning av personer med funktionsnedsättning, på samma villkor som andra användare, i enlighet med Europaparlamentets och rådets direktiv (EU) 2019/882*.

22. Vid tillhandahållandet av europeiska digitala identitetsplånböcker ska de europeiska digitala identitetsplånböckerna och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls inte omfattas av de krav som fastställs i artiklarna 7, 9, 10, 12 och 12a.

23. Senast … [sex månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som avses i punkterna 4, 5, 8 och 18 i denna artikel om genomförandet av den europeiska digitala identitetsplånboken. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

24. Kommissionen ska genom genomförandeakter upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för att främja anslutning av användare till den europeiska digitala identitetsplånboken, antingen genom medel för elektronisk identifiering som motsvarar tillitsnivå hög eller medel för elektronisk identifiering som motsvarar tillitsnivå väsentlig i kombination med ytterligare förfaranden för anslutning på distans som tillsammans uppfyller kraven för tillitsnivå hög. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5b

Europeiska digitala identitetsplånboken – förlitande parter

1. Om en förlitande part avser att förlita sig på europeiska digitala identitetsplånböcker för tillhandahållande av offentliga eller privata tjänster genom digital interaktion ska den förlitande parten registrera sig i den medlemsstat där den är etablerad.

2. Registreringsprocessen ska vara kostnadseffektiv och stå i proportion till riskerna. Den förlitande parten ska tillhandahålla åtminstone följande:

   a) Den information som krävs för autentisering till europeiska digitala identitetsplånböcker, som omfattar minst

      i) den medlemsstat där den förlitande parten är etablerad, och

      ii) den förlitande partens namn och, i tillämpliga fall, dess registreringsnummer i enlighet med vad som framgår i ett officiellt register, tillsammans med identifieringsuppgifter från det officiella registret.

b) Kontaktuppgifter till den förlitande parten.

c) Den avsedda användningen av europeiska digitala identitetsplånböcker, inbegripet angivande av de uppgifter som den förlitande parten ska begära från användare.

3. Förlitande parter får inte begära att användare tillhandahåller några andra uppgifter än dem som anges enligt punkt 2 c.

4. Punkterna 1 och 2 ska inte påverka tillämpningen av unionsrätt eller nationell rätt som är tillämplig på tillhandahållandet av särskilda tjänster.

5. Medlemsstaterna ska göra den information som avses i punkt 2 tillgänglig för allmänheten online i elektroniskt undertecknad eller stämplad form som lämpar sig för automatiserad behandling.

6. Förlitande parter som registrerat sig i enlighet med denna artikel ska utan dröjsmål informera medlemsstaterna om eventuella ändringar av den information som lämnats vid registreringen enligt punkt 2.

7. Medlemsstaterna ska tillhandahålla en gemensam mekanism för att möjliggöra identifiering och autentisering av förlitande parter, enligt vad som avses i artikel 5a.5 c.

8. Om förlitande parter avser att förlita sig på europeiska digitala identitetsplånböcker ska de identifiera sig för användaren.

9. Förlitande parter ska ansvara för genomförandet av förfarandet för autentisering och validering av uppgifter för personidentifiering och elektroniska attributsintyg som begärts från europeiska digitala identitetsplånböcker. Förlitande parter får inte neka användning av pseudonymer om identifiering av användaren inte krävs enligt unionsrätten eller nationell rätt.

10. Mellanhänder som agerar för förlitande parters räkning ska betraktas som förlitande parter och får inte lagra uppgifter om transaktionens innehåll.

11. Senast den … [sex månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen fastställa tekniska specifikationer och förfaranden för de krav som avses i punkterna 2, 5 och 6–9 i denna artikel genom genomförandeakter om det genomförande av europeiska digitala identitetsplånböcker som avses i artikel 5a.23. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5c

Certifiering av europeiska digitala identitetsplånböcker

1. Certifiering av att europeiska digitala identitetsplånböcker och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls överensstämmer med kraven i artikel 5a.4, 6a.5 och 6a.8, kravet på logiskt avskiljande i artikel 5a.14 och, i tillämpliga fall, de standarder och tekniska specifikationer som avses i artikel 5a.24 ska utföras av organ för bedömning av överensstämmelse som utsetts av medlemsstaterna.

2. Certifiering av att europeiska digitala identitetsplånböcker överensstämmer med de krav som avses i punkt 1 i denna artikel, eller delar av dem, som är relevanta för cybersäkerhet ska utföras i enlighet med europeiska cybersäkerhetscertifieringsordningar som antagits enligt Europaparlamentets och rådets förordning (EU) 2019/881[**] och som avses i de genomförandeakter som avses i punkt 6 i denna artikel.

3. För krav som avses i punkt 1 i denna artikel som inte är relevanta för cybersäkerhet och för krav som avses i punkt 1 i denna artikel som är relevanta för cybersäkerhet, i den mån som de ordningar för cybersäkerhetscertifiering som avses i punkt 2 i denna artikel inte, eller endast delvis, omfattar de cybersäkerhetskraven, ska medlemsstaterna även för de kraven inrätta nationella certifieringsordningar i enlighet med de krav som fastställs i de genomförandeakter som avses i punkt 6 i denna artikel. Medlemsstaterna ska översända sina utkast till nationella certifieringsordningar till den europeiska samarbetsgrupp för digital identitet som inrättats enligt artikel 46e.1 (*samarbetsgruppen*). Samarbetsgruppen får utfärda yttranden och rekommendationer.

4. Certifiering enligt punkt 1 ska vara giltig i upp till fem år, under förutsättning att en sårbarhetsbedömning utförs vartannat år. Om en sårbarhet identifieras och inte åtgärdas inom lämplig tid, ska certifieringen upphöra att gälla.

5. Överensstämmelse med kraven i artikel 5a i denna förordning avseende behandling av personuppgifter får certifieras enligt förordning (EU) 2016/679.

6. Senast den … [sex månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och vid behov fastställa specifikationer och förfaranden för certifiering av europeiska digitala identitetsplånböcker som avses i punkterna 1, 2 och 3 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

7. Medlemsstaterna ska meddela kommissionen namn och adress för de organ för bedömning av överensstämmelse som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för samtliga medlemsstater.

8. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 47 om fastställande av särskilda kriterier som ska uppfyllas av de utsedda organ för bedömning av överensstämmelse som avses i punkt 1 i den här artikeln.

Artikel 5d

Offentliggörande av en förteckning över certifierade europeiska digitala identitetsplånböcker

1. Medlemsstaterna ska utan onödigt dröjsmål informera kommissionen och den samarbetsgrupp som inrättats i enlighet med artikel 46e.1 om europeiska digitala identitetsplånböcker som har tillhandahållits i enlighet med artikel 5a och som har certifierats av de organ för bedömning av överensstämmelse som avses i artikel 5c.1. De ska utan onödigt dröjsmål informera kommissionen och den samarbetsgrupp som inrättats i enlighet med artikel 46e.1 om en certifiering upphör att gälla och ange skälen till detta.

2. Utan att det påverkar tillämpningen av artikel 5a.18 ska den information som medlemsstaterna lämnar enligt punkt 1 i den här artikeln åtminstone omfatta uppgifter om följande:

   a) Certifikatet och rapporten om certifieringsbedömningen för den certifierade europeiska digitala identitetsplånboken.

   b) En beskrivning av det system för elektronisk identifiering inom ramen för vilket den europeiska digitala identitetsplånboken tillhandahålls.

   c) Det tillämpliga tillsynssystemet samt information om systemet för skadeståndsansvar med avseende på den part som tillhandahåller den europeiska digitala identitetsplånboken.

   d) Den myndighet eller de myndigheter som ansvarar för systemet för elektronisk identifiering.

   e) System för tillfälligt upphävande eller återkallande av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda äventyrade delarna.

3. Kommissionen ska på grundval av den information som inkommit upprätta, offentliggöra i *Europeiska unionens officiella tidning* och i maskinläsbar form upprätthålla en förteckning över certifierade europeiska digitala identitetsplånböcker.

4. En medlemsstat får lämna in en begäran till kommissionen om att ta bort en europeisk digital identitetsplånbok och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls från den förteckning som avses i punkt 3.

5. Om den information som lämnats i enlighet med punkt 1 ändras ska medlemsstaten förse kommissionen med uppdaterad information.

6. Kommissionen ska hålla den förteckning som avses i punkt 3 uppdaterad genom att i *Europeiska unionens officiella tidning* offentliggöra motsvarande ändringar av förteckningen inom en månad från mottagandet av en begäran enligt punkt 4 eller av uppdaterad information enligt punkt 5.

7. Senast den … [sex månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen fastställa de format och förfaranden som ska gälla vid tillämpning av punkterna 1, 4 och 5 i denna artikel; detta ska göras genom genomförandeakter om genomförandet av europeiska digitala identitetsplånböcker som avses i artikel 5a.23. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5e

Säkerhetsincidenter som rör europeiska digitala identitetsplånböcker

1. I de fall då europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med artikel 5a, de valideringsmekanismer som avses i artikel 5a.8 eller det system för elektronisk identifiering inom ramen för vilket de europeiska digitala identitetsplånböckerna tillhandahålls är föremål för incidenter eller delvis äventyras på ett sätt som påverkar deras tillförlitlighet, eller tillförlitligheten för andra europeiska digitala identitetsplånböcker, ska den medlemsstat som tillhandahöll de europeiska digitala identitetsplånböckerna utan onödigt dröjsmål tillfälligt upphäva tillhandahållandet och användningen av europeiska digitala identitetsplånböcker.

   När det är motiverat mot bakgrund av allvaret i den säkerhetsincident eller det äventyrande som avses i första stycket ska medlemsstaten återkalla europeiska digitala identitetsplånböcker utan onödigt dröjsmål.

Medlemsstaten ska informera de berörda användarna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1, de förlitande parterna och kommissionen om detta.

2. Om den säkerhetsincident eller det äventyrande som avses i punkt 1 första stycket i denna artikel inte åtgärdas inom tre månader från det tillfälliga upphävandet, ska den medlemsstat som tillhandahöll de europeiska digitala identitetsplånböckerna återkalla europeiska digitala identitetsplånböckerna och upphäva deras giltighet. Medlemsstaten ska informera de berörda användarna, de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1, de förlitande parterna och kommissionen om återkallandet.

3. I fall då den säkerhetsincident eller det äventyrande som avses i punkt 1 första stycket i denna artikel åtgärdas ska den tillhandahållande medlemsstaten återupprätta tillhandahållandet och användningen av europeiska digitala identitetsplånböcker och informera de berörda användarna och förlitande parterna samt de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 och kommissionen utan onödigt dröjsmål.

4. Kommissionen ska utan onödigt dröjsmål offentliggöra motsvarande ändringar i den förteckning som avses i artikel 5d i *Europeiska unionens officiella tidning*.

5. Senast den … [sex månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, fastställa en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de åtgärder som avses i punkterna 1, 2 och 3 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 5f

Gränsöverskridande användning av europeiska digitala identitetsplånböcker

1. I de fall då medlemsstater kräver elektronisk identifiering och autentisering för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ, ska de även godta europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med denna förordning.

2. I de fall då privata förlitande parter som tillhandahåller tjänster, med undantag för mikroföretag och små företag enligt definitionen i artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG[***], enligt unionsrätten eller nationell rätt är ålagda att använda stark användarautentisering för onlineidentifiering, eller om stark användarautentisering för onlineidentifiering krävs enligt avtalsförpliktelse, inbegripet på områdena transport, energi, banktjänster, finansiella tjänster, social trygghet, hälso- och sjukvård, dricksvatten, posttjänster, digital infrastruktur, utbildning eller telekommunikation, ska dessa privata förlitande parter senast 36 månader efter dagen för ikraftträdandet av de genomförandeakter som avses i artiklarna 5a.23 och 5c.6, och endast på användarens frivilliga begäran, även godta europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med denna förordning.

3. I de fall då tillhandahållare av mycket stora onlineplattformar enligt artikel 33 i Europaparlamentets och rådets förordning (EU) 2022/2065[****] kräver användarautentisering för att få åtkomst till nättjänster, ska dessa plattformar även godta och främja användningen av europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med denna förordning när det gäller användarautentisering endast på användarens frivilliga begäran och iaktta de minimidata som behövs för den specifika nättjänst som begäran om autentisering avser.

4. I samarbete med medlemsstaterna ska kommissionen främja utvecklingen av uppförandekoder i nära samarbete med berörda parter, inbegripet civilsamhället, för att bidra till en bred tillgång till och användbarhet för europeiska digitala identitetsplånböcker inom ramen för denna förordning, och för att uppmuntra tjänsteleverantörer att slutföra utarbetandet av uppförandekoder.

5. Inom 24 månader från införandet av europeiska digitala identitetsplånböcker ska kommissionen bedöma efterfrågan på, och tillgången till, europeiska digitala identitetsplånböcker samt deras användbarhet, med beaktande av kriterier såsom spridning bland användarna, tjänsteleverantörers gränsöverskridande närvaro, teknisk utveckling, användningsmönstrens utveckling och konsumenternas efterfrågan.

---

* Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

** Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten), (EUT L 151, 7.6.2019, s. 15).

*** Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

**** Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277 27.10.2022, s. 1).”

6. Följande rubrik ska införas före artikel 6:

”AVSNITT 2
SYSTEM FÖR ELEKTRONISK IDENTIFIERING”

7. I artikel 7 ska led g ersättas med följande:

”g) Minst sex månader före anmälan enligt artikel 9.1 ska den anmälande medlemsstaten för tillämpningen av artikel 12.5 förse andra medlemsstater med en beskrivning av detta system i enlighet med de förfaranden som fastställts genom de genomförandeakter som antas enligt artikel 12.6.”

8. I artikel 8.3 ska första stycket ersättas med följande:

”3. Senast den 18 september 2015 ska kommissionen, med beaktande av relevanta internationella standarder och om inte annat följer av punkt 2, genom genomförandeakter fastställa tekniska minimispecifikationer, standarder och förfaranden genom vilka tillitsnivåerna låg, väsentlig och hög specificeras för medel för elektronisk identifiering.”

9. Artikel 9.2 och 9.3 ska ersättas med följande:

”2. Kommissionen ska utan onödigt dröjsmål i *Europeiska unionens officiella tidning* offentliggöra en förteckning över de system för elektronisk identifiering som anmälts enligt punkt 1 tillsammans med de grundläggande uppgifterna om dessa system.

3. Kommissionen ska i *Europeiska unionens officiella tidning* offentliggöra ändringarna i den förteckning som avses i punkt 2 inom en månad från den dag då anmälan mottogs.”

10. I artikel 10 ska rubriken ersättas med följande:

”Säkerhetsincidenter som rör system för elektronisk identifiering”.

11. Följande artikel ska införas:

”*Artikel 11a*
Gränsöverskridande identitetsmatchning

1. När medlemsstater agerar som förlitande parter för gränsöverskridande tjänster ska de säkerställa otvetydig identitetsmatchning för fysiska personer som använder anmälda medel för elektronisk identifiering eller europeiska digitala identitetsplånböcker.

2. Medlemsstaterna ska föreskriva tekniska och organisatoriska åtgärder för att säkerställa en hög skyddsnivå för personuppgifter som används för identitetsmatchning och för att förhindra profilering av användare.

3. Senast den … [sex månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, fastställa en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

12. Artikel 12 ska ändras på följande sätt:

a) Rubriken ska ersättas med följande:

”Interoperabilitet”.

b) Punkt 3 ska ändras på följande sätt:

i) Led c ska ersättas med följande:

”c) Det ska främja genomförandet av inbyggt integritetsskydd och inbyggd säkerhet.”

ii) Led d ska utgå.

c) I punkt 4 ska led d ersättas med följande:

”d) Hänvisning till en minimuppsättning uppgifter för personidentifiering som krävs för att på ett unikt sätt avse en fysisk eller juridisk person eller en fysisk person som företräder en annan fysisk person eller en juridisk person och som är tillgänglig via system för elektronisk identifiering.”

d) Punkterna 5 och 6 ska ersättas med följande:

”5. Medlemsstaterna ska genomföra sakkunnigbedömningar av de system för elektronisk identifiering som omfattas av tillämpningsområdet för denna förordning och som ska anmälas enligt artikel 9.1 a.

6. Senast den 18 mars 2025 ska kommissionen genom genomförandeakter fastställa nödvändiga förfaranden för de sakkunnigbedömningar som avses i punkt 5 i denna artikel i syfte att främja en hög nivå av förtroende och säkerhet som står i proportion till risknivån. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

e) Punkt 7 ska utgå.

f) Punkt 8 ska ersättas med följande:

”8. Senast den 18 september 2025 ska kommissionen, för att fastställa enhetliga villkor för tillämpningen av kraven i punkt 1 i denna artikel, i enlighet med de kriterier som fastställs i punkt 3 i denna artikel och med beaktande av resultaten av samarbetet mellan medlemsstaterna, anta genomförandeakter om det interoperabilitetsramverk som anges i punkt 4 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

13. Följande artiklar ska införas i kapitel II:

”*Artikel 12a*

Certifiering av system för elektronisk identifiering

1. Överensstämmelse för system för elektronisk identifiering som ska anmälas med de cybersäkerhetskrav som fastställs i denna förordning, inbegripet överensstämmelse med de relevanta cybersäkerhetskrav som fastställs i artikel 8.2 vad gäller tillitsnivåerna för system för elektronisk identifiering, ska certifieras av organ för bedömning av överensstämmelse som utsetts av medlemsstaterna.

2. Den certifiering enligt punkt 1 i denna artikel ska utföras inom ramen för en relevant ordning för cybersäkerhetscertifiering enligt förordning (EU) 2019/881 eller delar därav, i den mån cybersäkerhetscertifikatet eller delar därav omfattar dessa cybersäkerhetskrav.

3. Certifiering i enlighet med punkt 1 ska gälla i upp till fem år, under förutsättning att en sårbarhetsbedömning genomförs vartannat år. Om en sårbarhet identifieras och inte åtgärdas inom tre månader från identifieringen, ska certifieringen upphöra att gälla.

4. Trots vad som sägs i punkt 2 får medlemsstaterna, i enlighet med den punkten, begära ytterligare information från en anmälande medlemsstat om system för elektronisk identifiering eller delar därav som certifieras.

5. Den sakkunnigbedömning av system för elektronisk identifiering som avses i artikel 12.5 ska inte tillämpas på de system för elektronisk identifiering, eller delar av sådana system, som certifierats i enlighet med punkt 1 i den här artikeln. Medlemsstaterna får använda ett certifikat eller en försäkran om överensstämmelse, som utfärdats i enlighet med en relevant europeisk ordning för cybersäkerhetscertifiering eller delar av en sådan ordning, när det gäller krav som inte avser cybersäkerhet enligt artikel 8.2 avseende tillitsnivån för system för elektronisk identifiering.

6. Medlemsstaterna ska meddela kommissionen namn och adress för de organ för bedömning av överensstämmelse som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för samtliga medlemsstater.

Artikel 12b

Tillgång till maskinvaru- och programvarufunktioner

Om tillhandahållare av europeiska digitala identitetsplånböcker och utfärdare av anmälda medel för elektronisk identifiering som agerar kommersiellt eller yrkesmässigt och använder centrala plattformstjänster enligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2022/1925[*] för eller i samband med tillhandahållande av tjänster relaterade till europeiska digitala identitetsplånböcker och medel för elektronisk identifiering till slutanvändare är företagsanvändare i enlighet med artikel 2.21 i den förordningen, ska grindvakter särskilt tillåta dem faktisk interoperabilitet med och, för interoperabilitetsändamål, åtkomst till samma operativsystem eller maskinvaru- eller programvarufunktioner. Sådan faktisk interoperabilitet och åtkomst ska tillåtas kostnadsfritt och oavsett om maskinvaru- eller programvarufunktionerna är en del av det operativsystem som grindvakten har tillgång till eller använder när denne tillhandahåller sådana tjänster, i den mening som avses i artikel 6.7 i förordning (EU) 2022/1925. Den här artikeln påverkar inte tillämpningen av artikel 5a.14 i den här förordningen.

---

[*] Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (förordningen om digitala marknader) (EUT L 265, 12.10.2022, s. 1).”

14. Artikel 13.1 ska ersättas med följande:

”1. Trots punkt 2 i denna artikel och utan att det påverkar tillämpningen av förordning (EU) 2016/679 ska tillhandahållare av betrodda tjänster ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom deras underlåtenhet att uppfylla sina skyldigheter enligt denna förordning. Varje fysisk eller juridisk person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning av en tillhandahållare av betrodda tjänster ska ha rätt att begära ersättning i enlighet med unionsrätten och nationell rätt.

Bevisbördan för avsikt eller oaktsamhet hos en icke-kvalificerad tillhandahållare av betrodda tjänster ska vila på den fysiska eller juridiska person som gör gällande sådan skada som avses i första stycket.

Avsikt eller oaktsamhet hos en kvalificerad tillhandahållare av betrodda tjänster med avseende på skada som avses i första stycket ska presumeras såvida inte den kvalificerade tillhandahållaren av betrodda tjänster bevisar att den skada som avses i första stycket har uppstått utan avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren av betrodda tjänster.”

15. Artiklarna 14, 15 och 16 ska ersättas med följande:

”*Artikel 14*

Internationella aspekter

1. Betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster som är etablerade i ett tredjeland eller av en internationell organisation ska erkännas som rättsligt likvärdiga med kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen, under förutsättning att de betrodda tjänsterna från tredjelandet eller från den internationella organisationen är erkända genom genomförandeakter eller ett avtal som ingåtts mellan unionen och tredjelandet eller den internationella organisationen enligt artikel 218 i EUF-fördraget.

   De genomförandeakter som avses i första stycket ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

2. De genomförandeakter och det avtal som avses i punkt 1 ska säkerställa att de krav som är tillämpliga på kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen och de kvalificerade betrodda tjänster som de tillhandahåller uppfylls av tillhandahållarna av betrodda tjänster i det berörda tredjelandet eller av den internationella organisationen och av de betrodda tjänster som de tillhandahåller. Tredjeländer och internationella organisationer ska särskilt upprätta, underhålla och offentliggöra en förteckning över erkända tillhandahållare av betrodda tjänster.

3. De avtal som avses i punkt 1 ska säkerställa att de kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen erkänns som rättsligt likvärdiga med betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster i det tredjeland eller av den internationella organisation med vilket eller vilken avtalet ingås.

Artikel 15
Tillgänglighet för personer med funktionsnedsättning och särskilda behov

Tillhandahållandet av medel för elektronisk identifiering, betrodda tjänster och slutanvändarprodukter som används vid tillhandahållandet av dessa tjänster ska göras tillgängliga på ett klart och begripligt språk, i enlighet med Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning och med tillgänglighetskraven i bilaga I till direktiv (EU) 2019/882, och därmed även gynna personer med funktionsbegränsningar, såsom äldre personer, och personer med begränsad tillgång till digital teknik. ”

Artikel 16
Sanktioner

1. Utan att det påverkar tillämpningen av artikel 31 i Europaparlamentets och rådets direktiv (EU) 2022/2555* ska medlemsstaterna fastställa bestämmelser om sanktioner som ska gälla vid överträdelser av denna förordning. Sanktionerna ska vara effektiva, proportionella och avskräckande.

2. Medlemsstaterna ska säkerställa att överträdelser av denna förordning som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster medför maximala administrativa sanktionsavgifter på minst

   a) 5 000 000 EUR om tillhandahållaren av betrodda tjänster är en fysisk person, eller

   b) om tillhandahållaren av betrodda tjänster är en juridisk person, 5 000 000 EUR eller 1 % av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade, beroende på vilket som är högst.

3. Beroende på medlemsstaternas rättssystem får reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att förfarandet inleds av det behöriga tillsynsorganet och sanktionsavgifterna påförs av behöriga nationella domstolar. Tillämpningen av sådana regler i dessa medlemsstater ska säkerställa att dessa rättsmedel är effektiva och har motsvarande verkan som de administrativa sanktionsavgifter som påförs direkt av tillsynsmyndigheter.

---

* Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80).”

16. I kapitel III avsnitt 2 ska titeln ersättas med följande:

”Icke-kvalificerade betrodda tjänster”

17. Artiklarna 17 och 18 ska utgå.

18. Följande artikel ska införas i kapitel III avsnitt 2:

”*Artikel 19a*
Krav på icke-kvalificerade tillhandahållare av betrodda tjänster

1. En icke-kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller icke-kvalificerade betrodda tjänster ska

a) ha lämpliga policyer och vidta motsvarande åtgärder för att hantera rättsliga, affärsmässiga, operativa och andra direkta eller indirekta risker för tillhandahållandet av icke-kvalificerade betrodda tjänster, som trots artikel 21 i direktiv (EU) 2022/2555, ska innefatta åtminstone åtgärder avseende

i) registrerings- och anslutningsförfaranden för en tjänst,

ii) förfarandemässiga eller administrativa kontroller som krävs för att tillhandahålla betrodda tjänster,

iii) förvaltning och genomförande av betrodda tjänster,

b) anmäla till tillsynsorganet, de identifierbara berörda personerna, allmänheten om det är av allmänt intresse och, om tillämpligt, andra relevanta behöriga myndigheter, alla säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avses i led a i, ii eller iii och som har en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar från säkerhetsincidenten eller störningen.

2. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden avseende punkt 1 a i denna artikel. Överensstämmelse med kraven i denna artikel ska presumeras om dessa standarder, specifikationer och förfaranden uppfylls. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

19. Artikel 20 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Granskningen ska bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning och i artikel 21 i direktiv (EU) 2022/2555. Kvalificerade tillhandahållare av betrodda tjänster ska lämna in den resulterande rapporten om bedömning av överensstämmelse till tillsynsorganet inom tre arbetsdagar från mottagandet.”

b) Följande punkter ska införas:

”1a. Kvalificerade tillhandahållare av betrodda tjänster ska senast en månad före en planerad revision informera tillsynsorganet och ska tillåta tillsynsorganet att på begäran delta som observatör.

1b. Medlemsstaterna ska utan onödigt dröjsmål till kommissionen anmäla namn, adress och ackrediteringsuppgifter för de organ för bedömning av överensstämmelse som avses i punkt 1 och eventuella senare ändringar av dessa. Kommissionen ska göra den informationen tillgänglig för samtliga medlemsstater.”

c) Punkterna 2, 3 och 4 ska ersättas med följande:

”2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna av betrodda tjänster på dessa tillhandahållare av betrodda tjänsters egen bekostnad för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. Vid misstänkta överträdelser av reglerna om skydd av personuppgifter ska tillsynsorganet utan onödigt dröjsmål informera de behöriga tillsynsmyndigheterna som inrättats enligt artikel 51 i förordning (EU) 2016/679.

3. Om den kvalificerade tillhandahållaren av betrodda tjänster underlåter att uppfylla kraven i denna förordning ska tillsynsorganet ålägga denna tillhandahållare att åtgärda bristerna inom en fastställd tidsfrist, om tillämpligt.

Om tillhandahållaren inte åtgärdar bristerna, i tillämpliga fall inom den tidsfrist som fastställts av tillsynsorganet, ska tillsynsorganet, i synnerhet när det är motiverat av underlåtenhetens omfattning, varaktighet och följder, återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad.

3a. Om de behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555 informerar tillsynsorganet om att den kvalificerade tillhandahållaren av betrodda tjänster underlåter att uppfylla kraven i artikel 21 i det direktivet ska tillsynsorganet, i synnerhet när det är motiverat av underlåtenhetens omfattning, varaktighet och följder, återkalla status som kvalificerad för den tillhandahållaren eller den berörda tillhandahållna tjänst som denne tillhandahåller.

3b. Om tillsynsmyndigheterna som inrättats enligt artikel 51 i förordning (EU) 2016/679 informerar tillsynsorganet om att den kvalificerade tillhandahållaren av betrodda tjänster underlåter att uppfylla kraven i den förordningen ska tillsynsorganet, i synnerhet när det är motiverat av underlåtenhetens omfattning, varaktighet och följder, återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad.

3c. Tillsynsorganet ska informera den kvalificerade tillhandahållaren av betrodda tjänster om återkallandet av dess eller den berörda tjänstens status som kvalificerad. Tillsynsorganet ska informera det organ som anmälts i enlighet med artikel 22.3 i denna förordning i syfte att uppdatera de förteckningar över betrodda tjänsteleverantörer som avses i punkt 1 i den artikeln och den behöriga myndighet som utsetts eller inrättats i enlighet med artikel 8.1 i direktiv (EU) 2022/2555.

4. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för följande:

a) Ackreditering av organ för bedömning av överensstämmelse och för den rapport om bedömning av överensstämmelse som avses i punkt 1.

b) Granskningskrav för hur organ för bedömning av överensstämmelse ska göra sin bedömning av överensstämmelse, inbegripet sammansatt bedömning, vad gäller kvalificerade tillhandahållare av betrodda tjänster som avses i punkt 1.

c) De system för bedömning av överensstämmelse som gäller för den bedömning av överensstämmelsen för kvalificerade tillhandahållare av betrodda tjänster som utförs av organ för bedömning av överensstämmelse och för tillhandahållandet av den rapport som avses i punkt 1.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

20. Artikel 21 ska ändras på följande sätt:

a) Punkterna 1 och 2 ska ersättas med följande:

”1. När tillhandahållare av betrodda tjänster har för avsikt att börja tillhandahålla en kvalificerad betrodd tjänst, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om bedömning av överensstämmelse som utfärdats av ett organ för bedömning av överensstämmelse och som bekräftar att kraven i denna förordning och i artikel 21 i direktiv (EU) 2022/2555 är uppfyllda.

2. Tillsynsorganet ska kontrollera huruvida tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning, och i synnerhet kraven för kvalificerade tillhandahållare av betrodda tjänster och för de kvalificerade betrodda tjänster som de tillhandahåller.

För att kontrollera att tillhandahållaren av betrodda tjänster uppfyller de krav som fastställs i artikel 21 i direktiv (EU) 2022/2555 ska tillsynsorganet begära att de behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i det direktivet utför tillsynsverksamhet i det avseendet och tillhandahåller information om resultatet utan onödigt dröjsmål och under alla omständigheter inom två månader efter det att denna begäran har mottagits. Om kontrollen inte har slutförts inom två månader från anmälan, ska dessa behöriga myndigheter informera tillsynsorganet om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

Om tillsynsorganet kommer fram till att tillhandahållaren av betrodda tjänster, och de betrodda tjänster som denne tillhandahåller, uppfyller de krav som fastställs i denna förordning, ska tillsynsorganet bevilja tillhandahållaren av betrodda tjänster, och de betrodda tjänster som denne tillhandahåller, status som kvalificerad, samt informera det organ som avses i artikel 22.3 så att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 kan uppdateras, senast tre månader efter anmälan i enlighet med punkt 1 i denna artikel.

Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.”

b) Punkt 4 ska ersättas med följande:

”4. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen genom genomförandeakter fastställa formaten och förfarandena för anmälan och kontroll enligt punkterna 1 och 2 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

21. Artikel 24 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. En kvalificerad tillhandahållare av betrodda tjänster ska, när den utfärdar ett kvalificerat certifikat eller ett kvalificerat elektroniskt attributsintyg, kontrollera identiteten och, i förekommande fall, eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska attributsintyget ska utfärdas.

1a. Den kontroll av identiteten som avses i punkt 1 ska utföras på lämpligt sätt av den kvalificerade tillhandahållaren av betrodda tjänster, antingen direkt eller med hjälp av en tredje part, på grundval av en av följande metoder eller vid behov en kombination av dessa, i enlighet med de genomförandeakter som avses i punkt 1c:

a) Genom den europeiska digitala identitetsplånboken eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 vad gäller tillitsnivå hög.

b) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med led a, c eller d.

c) Genom användning av andra identifieringsmetoder som säkerställer identifiering av personen med en hög tillförlitlighetsnivå, vars överensstämmelse ska ha bekräftats av ett organ för bedömning av överensstämmelse.

d) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen, med hjälp av lämpliga bevis och förfaranden och i enlighet med nationell rätt.

1b. Den kontroll av attribut som avses i punkt 1 ska utföras på lämpligt sätt av den kvalificerade tillhandahållaren av betrodda tjänster, antingen direkt eller med hjälp av en tredje part, på grundval av en av följande metoder eller vid behov en kombination av dessa, i enlighet med de genomförandeakter som avses i punkt 1c:

a) Genom den europeiska digitala identitetsplånboken eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 vad gäller tillitsnivå hög.

b) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med punkt 1 a, c eller d.

c) Genom ett kvalificerat elektroniskt attributsintyg.

d) Genom användning av andra metoder som säkerställer kontroll av attributen med en hög tillförlitlighetsnivå, vars överensstämmelse ska ha bekräftats av ett organ för bedömning av överensstämmelse.

e) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen, med hjälp av lämpliga bevis, förfaranden och i enlighet med nationell rätt.”

”1c. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kontrollen av identitet och attribut i enlighet med punkterna 1, 1 a och 1b i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2. ”

b) Punkt 2 ska ändras på följande sätt:

i) Led a ska ersättas med följande:

”a) informera tillsynsorganet minst en månad innan någon ändring av tillhandahållandet av dess kvalificerade betrodda tjänster genomförs, eller minst tre månader om det finns en avsikt att upphöra med denna verksamhet;”,

ii) Leden d och e ska ersättas med följande:

”d) innan den ingår ett avtalsförhållande, på ett tydligt, uttömmande och lättillgängligt sätt, på en allmänt tillgänglig plats och individuellt, informera de personer som vill använda en kvalificerad betrodd tjänst om de exakta villkor som gäller för användning av den tjänsten, inbegripet om eventuella begränsningar av användningen,

e) använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos de processer som stöds av dessa, och även använda lämpliga krypteringstekniker,”.

iii) Följande led ska läggas till:

”fa) trots artikel 21 i direktiv (EU) 2022/2555, ha lämpliga policyer och vidta motsvarande åtgärder för att hantera rättsliga, affärsmässiga, operativa och andra direkta eller indirekta risker för tillhandahållandet av kvalificerade betrodda tjänster, inbegripet åtminstone åtgärder avseende följande:

i) registrerings- och anslutningsförfaranden för en tjänst,

ii) förfarandemässiga eller administrativa kontroller,

iii) förvaltning och genomförande av tjänster,

fb) anmäla till tillsynsorganet, de identifierbara berörda personerna, andra relevanta behöriga organ om tillämpligt och, på begäran av tillsynsorganet, allmänheten om det är av allmänt intresse, alla säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avses i led fa i, ii eller iii och som har en betydande inverkan på den tillhandahållna betrodda tjänsten eller de personuppgifter som lagras däri, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar från händelsen.”

iv) Leden g, h och i ska ersättas med följande:

”g) vidta lämpliga åtgärder mot förfalskning, stöld eller felaktigt förvärv av data eller mot radering, ändring eller otillgängliggörande av data om rättighet till detta saknas,

h) under en så lång tid som är nödvändig efter det att den kvalificerade tillhandahållaren av betrodda tjänster har upphört med sin verksamhet, registrera och tillgänglighålla all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, för att kunna lägga fram bevis vid rättsliga förfaranden och för att säkerställa tjänstens kontinuitet; registreringen får göras elektroniskt,

i) ha en uppdaterad plan för verksamhetens upphörande i syfte att säkerställa tjänstens kontinuitet i enlighet med bestämmelser som kontrolleras av tillsynsorganet enligt artikel 46b.4 i,”.

v) Led j ska utgå.

vi) Följande stycke ska läggas till:

”Tillsynsorganet får begära information utöver den information som anmälts i enlighet med första stycket a eller resultatet av en bedömning av överensstämmelse och får villkora beviljandet av tillståndet att genomföra de avsedda ändringarna av de kvalificerade betrodda tjänsterna. Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd,”

c) Punkt 5 ska ersättas med följande:

”4a. Punkterna 3 och 4 ska i enlighet med detta tillämpas vid återkallelse av kvalificerade elektroniska attributsintyg.

4b. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 47, för fastställande av ytterligare åtgärder som avses i punkt 2 fa i den här artikeln.

5. Senast … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som avses i punkt 2 b–h i denna artikel. Överensstämmelse med kraven i denna punkt i denna artikel ska förutsättas när dessa standarder, specifikationer och förfaranden uppfylls. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

22. Följande artikel ska införas i kapitel III, avsnitt 3:

”*Artikel 24a*

Erkännande av kvalificerade betrodda tjänster

”1. Kvalificerade elektroniska underskrifter baserade på ett kvalificerat certifikat som utfärdats i en medlemsstat, och kvalificerade elektroniska stämplar baserade på ett kvalificerat certifikat som utfärdats i en medlemsstat, ska erkännas som kvalificerade elektroniska underskrifter respektive kvalificerade elektroniska stämplar i alla andra medlemsstater.

2. Kvalificerade anordningar för skapande av elektroniska underskrifter och kvalificerade anordningar för skapande av elektroniska stämplar som certifierats i en medlemsstat ska erkännas som kvalificerade anordningar för skapande av elektroniska underskrifter respektive kvalificerade anordningar för skapande av elektroniska stämplar i alla andra medlemsstater.

3. Ett kvalificerat certifikat för elektroniska underskrifter, ett kvalificerat certifikat för elektroniska stämplar, en kvalificerad betrodd tjänst för förvaltning av en kvalificerad anordning för skapande av elektroniska underskrifter på distans och en kvalificerad betrodd tjänst för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplar på distans, tillhandahållna i en medlemsstat, ska erkännas som ett kvalificerat certifikat för elektroniska underskrifter, ett kvalificerat certifikat för elektroniska stämplar, en kvalificerad betrodd tjänst för förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans och en kvalificerad betrodd tjänst för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplar på distans i alla andra medlemsstater.

4. En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter och en kvalificerad valideringstjänst för kvalificerade elektroniska stämplar, tillhandahållna i en medlemsstat, ska erkännas som en kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter respektive en kvalificerad valideringstjänst för kvalificerade elektroniska stämplar i alla andra medlemsstater.

5. En kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter och en kvalificerad tjänst för bevarande av kvalificerade elektroniska stämplar, tillhandahållna i en medlemsstat, ska erkännas som en kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter respektive en kvalificerad tjänst för bevarande av kvalificerade elektroniska stämplar i alla andra medlemsstater.

6. En kvalificerad elektronisk tidsstämpling, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk tidsstämpling i alla andra medlemsstater.

7. Ett kvalificerat certifikat för autentisering av webbplatser, utfärdat i en medlemsstat, ska erkännas som ett kvalificerat certifikat för autentisering av webbplatser i alla andra medlemsstater.

8. En kvalificerad elektronisk tjänst för rekommenderade leveranser, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk tjänst för rekommenderade leveranser i alla andra medlemsstater.

9. Ett kvalificerat elektroniskt attributsintyg, utfärdat i en medlemsstat, ska erkännas som ett kvalificerat elektroniskt attributsintyg i alla andra medlemsstater.

10. En kvalificerad elektronisk arkiveringstjänst, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk arkiveringstjänst i alla andra medlemsstater.

11. En kvalificerad elektronisk liggare, tillhandahållen i en medlemsstat, ska erkännas som en kvalificerad elektronisk liggare i alla andra medlemsstater.”

23. Artikel 25.3 ska utgå.

26. Artikel 26 ska ändras på följande sätt:

a) Det enda stycket ska benämnas punkt 1.

b) Följande punkt ska läggas till:

2. Senast den … [24 månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen bedöma huruvida det är nödvändigt att anta genomförandeakter för att upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för avancerade elektroniska underskrifter. På grundval av resultatet av den bedömningen får kommissionen anta sådana genomförandeakter. Överensstämmelse med kraven för avancerade elektroniska underskrifter ska presumeras om en avancerad elektronisk underskrift överensstämmer med dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

25. Artikel 27.4 ska utgå.

26. Artikel 28.6 ska ersättas med följande:

”6. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade certifikat för elektroniska underskrifter. Överensstämmelse med kraven i bilaga I ska presumeras om ett kvalificerat certifikat för elektroniska underskrifter uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

27. I artikel 29 ska följande punkt införas:

”1a. Generering eller hantering av uppgifter för skapande av elektroniska underskrifter eller kopiering av sådana uppgifter för skapande av underskrifter för framställning av säkerhetskopior får utföras endast för undertecknarens räkning, på undertecknarens begäran, av en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller en kvalificerad betrodd tjänst för förvaltningen av en kvalificerad anordning för skapande av elektroniska underskrifter på distans.”

28. Följande artikel ska införas:

”*Artikel 29a*

Krav för kvalificerade tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans

1. Förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter på distans som en kvalificerad tjänst får utföras endast av en kvalificerad tillhandahållare av betrodda tjänster som

   a) genererar eller hanterar uppgifter för skapande av elektroniska underskrifter för undertecknarens räkning,

   b) trots punkt 1 d i bilaga II, kopierar uppgifterna för skapande av elektroniska underskrifter endast för framställning av säkerhetskopior, förutsatt att följande krav uppfylls:

      i) Säkerheten för de kopierade datauppsättningarna måste vara på samma nivå som för de ursprungliga datauppsättningarna.

      ii) Antalet kopierade datauppsättningar får inte överskrida det minsta antal som krävs för att säkerställa tjänstens kontinuitet.

   c) uppfyller alla krav som anges i certifieringsrapporten för den specifika kvalificerade anordning för skapande av elektroniska underskrifter på distans som utfärdats i enlighet med artikel 30.

2. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, specifikationer och förfaranden för tillämpningen av punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

29. I artikel 30 ska följande punkt införas:

”3a. Giltigheten för den certifiering som avses i punkt 1 får inte överstiga fem år, förutsatt att sårbarhetsbedömningar genomförs vartannat år. Om sårbarheter identifieras och inte åtgärdas ska certifieringen upphöra att gälla.”

30. Artikel 31.3 ska ersättas med följande:

”3. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen genom genomförandeakter fastställa format och förfaranden som ska vara tillämpliga för de ändamål som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

31. Artikel 32 ska ändras på följande sätt:

a) I punkt 1 ska följande stycke läggas till:

”Överensstämmelse med kraven i första stycket i denna artikel ska presumeras om valideringen av kvalificerade elektroniska underskrifter följer de standarder, specifikationer och förfaranden som avses i punkt 3.”

b) Punkt 3 ska ersättas med följande:

”3. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för validering av kvalificerade elektroniska underskrifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

32. Följande artikel ska införas:

”*Artikel 32a*
Krav för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat

1. Genom valideringsförfarandet för en avancerad elektronisk underskrift baserad på ett kvalificerat certifikat ska giltigheten för en avancerad elektronisk underskrift baserad på ett kvalificerat certifikat bekräftas under förutsättning att

a) det certifikat som stöder underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med bilaga I,

b) det kvalificerade certifikatet har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och var giltigt vid tidpunkten för undertecknandet,

c) valideringsuppgifterna för underskriften överensstämmer med de uppgifter som lämnats till den förlitande parten,

d) certifikatets unika uppsättning uppgifter som avser undertecknaren har tillhandahållits den förlitande parten på rätt sätt,

e) användningen av en eventuell pseudonym tydligt har angetts för den förlitande parten om en pseudonym användes vid tidpunkten för undertecknandet,

f) integriteten hos de undertecknade uppgifterna inte har äventyrats,

g) kraven i artikel 26 var uppfyllda vid tidpunkten för undertecknandet.

2. Det system som används för att validera den avancerade elektroniska underskriften baserad på kvalificerade certifikat ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och ska göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten.

3. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat. Överensstämmelse med kraven i punkt 1 i denna artikel ska presumeras om valideringen av avancerade elektroniska underskrifter baserade på kvalificerade certifikat uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

33. Artikel 33.2 ska ersättas med följande text:

”2. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för den kvalificerade valideringstjänst som avses i punkt 1 i denna artikel. Överensstämmelse med kraven i punkt 1 i denna artikel ska presumeras om den kvalificerade valideringstjänsten för kvalificerade elektroniska underskrifter uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

34. Artikel 34 ska ändras på följande sätt:

a) Följande punkt ska införas:

”1a. Överensstämmelse med kraven i punkt 1 ska presumeras om arrangemangen för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 2.”

b) Punkt 2 ska ersättas med följande:

”2. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2. ”

35. Artikel 35.3 ska utgå.

36. Artikel 36 ska ändras på följande sätt:

a) Det enda stycket ska benämnas punkt 1.

b) Följande punkt ska läggas till:

”2. Senast den … [24 månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen bedöma huruvida det är nödvändigt att anta genomförandeakter i syfte att upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för avancerade elektroniska stämplar. På grundval av resultatet av den bedömningen får kommissionen anta sådana genomförandeakter. Överensstämmelse med kraven för avancerade elektroniska stämplar ska presumeras om en avancerad elektronisk stämpel uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

37. Artikel 37.4 ska utgå.

38. Artikel 38.6 ska ersättas med följande:

”6. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade certifikat för elektroniska stämplar. Överensstämmelse med kraven i bilaga III ska presumeras om ett kvalificerat certifikat för elektroniska stämplar uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

39. Följande artikel ska införas:

”*Artikel 39a*
Krav för kvalificerade tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplar på distans

Artikel 29a ska i tillämpliga delar gälla för kvalificerade tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska stämplar på distans.”

40. Följande artikel ska införas i kapitel III avsnitt 5:

”*Artikel 40a*
Krav för validering av avancerade elektroniska stämplar baserade på kvalificerade certifikat

Artikel 32a ska i tillämpliga delar gälla för validering av avancerade elektroniska stämplar baserade på kvalificerade certifikat.”

41. Artikel 41.3 ska utgå.

42. Artikel 42 ska ändras på följande sätt:

a) Följande punkt ska införas:

”1a. Överensstämmelse med kraven i punkt 1 ska presumeras om bindningen av datum och tidpunkt till uppgifter och korrektheten för tidskällan uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 2.”

b) Punkt 2 ska ersättas med följande:

”2. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för bindningen av datum och tidpunkt till uppgifter och fastställande av korrektheten för tidskällor. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2. ”

43. Artikel 44 ska ändras på följande sätt:

a) Följande punkt ska införas:

”1a. Överensstämmelse med kraven i punkt 1 ska presumeras om en process för att sända och ta emot uppgifter uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 2.”

b) Punkt 2 ska ersättas med följande:

”2. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för processer för att sända och ta emot uppgifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

c) Följande punkter ska införas:

”2a. Tillhandahållare av kvalificerade elektroniska tjänster för rekommenderade leveranser får komma överens om interoperabilitet mellan de kvalificerade elektroniska tjänster för rekommenderade leveranser som de tillhandahåller. Ett sådant interoperabilitetsramverk ska uppfylla kraven i punkt 1 och denna uppfyllelse ska bekräftas av ett organ för bedömning av överensstämmelse.

2b. Kommissionen får, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för det interoperabilitetsramverk som avses i punkt 2a i denna artikel. Standarderna ska, vad gäller tekniska specifikationer och innehåll, vara kostnadseffektiva och proportionerliga. Genomförandeakterna ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

44. Artikel 45 ska ersättas med följande:

”*Artikel 45*

Krav på kvalificerade certifikat för autentisering av webbplatser

1. Kvalificerade certifikat för autentisering av webbplatser ska uppfylla de krav som fastställs i bilaga IV. Bedömningen av huruvida dessa krav är uppfyllda ska utföras i enlighet med de standarder, specifikationer och förfaranden som avses i punkt 2 i denna artikel.

1a. Kvalificerade certifikat för autentisering av webbplatser som utfärdats i enlighet med punkt 1 ska erkännas av tillhandahållare av webbläsare. Tillhandahållare av webbläsare ska säkerställa att identitetsuppgifter som intygas i certifikatet och ytterligare intygade attribut visas på ett användarvänligt sätt. Tillhandahållare av webbläsare ska säkerställa stöd och interoperabilitet med kvalificerade certifikat för autentisering av webbplatser enligt punkt 1 i denna artikel, med undantag för mikroföretag eller små företag enligt definitionen i artikel 2 i bilagan till rekommendation 2003/361/EG under de fem första år som de är verksamma som tillhandahållare av webbläsartjänster.

1b. Kvalificerade certifikat för autentisering av webbplatser ska inte omfattas av några obligatoriska krav utöver de krav som fastställs i punkt 1.

2. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de kvalificerade certifikat för autentisering av webbplatser som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

45. Följande artikel ska införas:

”*Artikel 45a*
Säkerhetsåtgärder för cybersäkerhet

1. Tillhandahållare av webbläsare ska inte vidta några åtgärder som strider mot deras skyldigheter enligt artikel 45, särskilt kraven på att erkänna kvalificerade certifikat för autentisering av webbplatser och att visa de identitetsuppgifter som tillhandahålls på ett användarvänligt sätt.

2. Genom undantag från punkt 1 och endast vid väl underbyggda farhågor om säkerhetsincidenter eller integritetsförlust hos ett identifierat certifikat eller en identifierad uppsättning certifikat får tillhandahållare av webbläsare vidta säkerhetsåtgärder med avseende på det certifikatet eller den uppsättningen av certifikat.

3. Om en tillhandahållare av en webbläsare vidtar säkerhetsåtgärder enligt punkt 2 ska tillhandahållaren av webbläsaren utan onödigt dröjsmål skriftligen meddela sina farhågor, tillsammans med en beskrivning av de åtgärder som vidtagits för att hantera dessa farhågor, till kommissionen, det behöriga tillsynsorganet, den enhet till vilken certifikatet utfärdades och den kvalificerade tillhandahållare av betrodda tjänster som utfärdade certifikatet eller uppsättningen av certifikat. Vid mottagandet av ett sådant meddelande ska det behöriga tillsynsorganet utfärda ett mottagningsbevis till tillhandahållaren av webbläsaren i fråga.

4. Det behöriga tillsynsorganet ska undersöka de frågor som tas upp i meddelandet i enlighet med artikel 46b.4 k. Om resultatet av utredningen inte leder till att certifikatets status som kvalificerat återkallas ska tillsynsorganet informera tillhandahållaren av webbläsaren om detta och begära att den tillhandahållaren avbryter de säkerhetsåtgärder som avses i punkt 2 i den här artikeln.”

46. Följande avsnitt ska läggas till i kapitel III:

”AVSNITT 9
ELEKTRONISKA ATTRIBUTSINTYG

Artikel 45b
Rättslig verkan av elektroniska attributsintyg

1. Ett elektroniskt attributsintyg får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska attributsintyg.

2. Ett kvalificerat elektroniskt attributsintyg och attributsintyg utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska ha samma rättsliga verkan som lagligt utfärdade intyg i pappersformat.

3. Ett attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa i en medlemsstat ska erkännas som ett attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa i alla medlemsstater.

Artikel 45c

Elektroniska attributsintyg i offentliga tjänster

I de fall då det enligt nationell rätt krävs elektronisk identifiering med användning av ett medel för elektronisk identifiering och autentisering för åtkomst till en nättjänst som tillhandahålls av ett offentligt organ, ska inte uppgifterna för personidentifiering i det elektroniska attributsintyget ersätta den elektroniska identifieringen med användning av medel för elektronisk identifiering och autentisering om inte detta specifikt tillåts av medlemsstaten. I sådana fall ska kvalificerade elektroniska attributsintyg från andra medlemsstater också godtas.

Artikel 45d

Krav på kvalificerade elektroniska attributsintyg

1. Kvalificerade elektroniska attributsintyg ska uppfylla de krav som fastställs i bilaga V.

2. Bedömningen av huruvida kraven i bilaga V är uppfyllda ska utföras i enlighet med de standarder, specifikationer och förfaranden som avses i punkt 5 i denna artikel.

3. Kvalificerade elektroniska attributsintyg ska inte omfattas av några obligatoriska krav utöver de krav som fastställs i bilaga V.

4. Om ett kvalificerat elektroniskt attributsintyg har återkallats efter det ursprungliga utfärdandet, ska det förlora sin giltighet från och med tidpunkten för återkallandet och dess status som giltigt ska inte under några omständigheter återställas.

5. Senast den … [sex månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade elektroniska attributsintyg. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 45e

Kontroll av attribut mot autentiska källor

1. Medlemsstaterna ska inom 24 månader från dagen för ikraftträdandet av de genomförandeakter som avses i artiklarna 5a.23 och 5c.6, åtminstone för de attribut som förtecknas i bilaga VI när dessa attribut baseras på autentiska källor inom offentliga sektorn, säkerställa att åtgärder vidtas som gör det möjligt för kvalificerade tillhandahållare av betrodda tjänster för elektroniska attributsintyg att på användarens begäran, i enlighet med unionsrätten eller nationell rätt på elektronisk väg kontrollera dessa attribut.

2. Senast den … [sex månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, med beaktande av relevanta internationella standarder, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för katalogen med attribut, liksom system för attributsintyg och kontrollförfaranden för kvalificerade elektroniska attributsintyg för tillämpningen av punkt 1 i denna artikel. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 45f

Krav på elektroniska attributsintyg utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa

1. Ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska uppfylla följande krav:

   a) De som anges i bilaga VII.

   b) Det kvalificerade certifikat som stöder den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln från det offentliga organ som avses i artikel 3.46 och som identifierats som den utfärdare som avses i led b i bilaga VII, som innehåller en särskild uppsättning certifierade attribut i en form som lämpar sig för automatiserad behandling och

      i) som anger att det utfärdande organet är inrättat i enlighet med unionsrätten eller nationell rätt som ansvarigt för den autentiska källa på grundval av vilken det elektroniska attributsintyget utfärdas eller som det organ som utsetts att agera på dess vägnar,

      ii) som tillhandahåller en uppsättning uppgifter som otvetydigt avser den autentiska källa som avses i led i, och

      iii) som identifierar den unionsrätt eller nationella rätt som avses i led i.

2. Den medlemsstat där de offentliga organ som avses i artikel 3.46 är etablerade ska säkerställa att de offentliga organ som utfärdar elektroniska attributsintyg har en tillförlitlighetsnivå som är likvärdig med den hos kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 24.

3. Medlemsstaterna ska underrätta kommissionen om de offentliga organ som avses i artikel 3.46. Denna anmälan ska innehålla en rapport om bedömning av överensstämmelse som utfärdats av ett organ för bedömning av överensstämmelse och som bekräftar att kraven i punkterna 1, 2 och 6 i denna artikel är uppfyllda. Kommissionen ska säkerställa att en förteckning över de offentliga organ som avses i avses i artikel 3.46 genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller stämplad form som lämpar sig för automatiserad behandling.

4. Om ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa har återkallats efter det ursprungliga utfärdandet ska det förlora sin giltighet från och med tidpunkten för återkallandet, och dess status ska inte återställas.

5. Ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska anses uppfylla kraven i punkt 1 om det uppfyller kraven i de standarder, specifikationer och förfaranden som avses i punkt 6.

6. Senast den … [sex månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

7. Senast den … [sex månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för tillämpningen av punkt 3 i denna artikel. Dessa genomförandeakter ska vara förenliga med de genomförandeakter som avses i artikel 5a.23 om genomförandet av den europeiska digitala identitetsplånboken. De ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

8. Offentliga organ som avses i artikel 3.46 som utfärdar elektroniska attributsintyg ska tillhandahålla ett gränssnitt med de europeiska digitala identitetsplånböcker som utfärdas i enlighet med artikel 5a.

Artikel 45g

Utfärdande av elektroniska attributsintyg till europeiska digitala identitetsplånböcker

1. Tillhandahållare av elektroniska attributsintyg ska ge användare av den europeiska digitala identitetsplånböcker möjlighet att begära, erhålla, lagra och hantera det elektroniska attributsintyget, oavsett i vilken medlemsstat den europeiska digitala identitetsplånboken tillhandahålls.

2. Tillhandahållare av kvalificerade elektroniska attributsintyg ska tillhandahålla ett gränssnitt med europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med artikel 5a.

Artikel 45h

Ytterligare regler för tillhandahållande av tjänster för elektroniska attributsintyg

1. Tillhandahållare av kvalificerade och icke-kvalificerade tjänster för elektroniska attributsintyg får inte kombinera personuppgifter som rör tillhandahållandet av dessa tjänster med personuppgifter från några andra tjänster som de eller deras affärspartner erbjuder.

2. Personuppgifter som rör tillhandahållande av tjänster för elektroniska attributsintyg ska hållas logiskt åtskilda från andra data som innehas av tillhandahållaren av elektroniska attributsintyg.

3. Tillhandahållare av tjänster för kvalificerade elektroniska attributsintyg ska genomföra tillhandahållandet av sådana kvalificerade betrodda tjänster på ett sätt som till sin funktion är åtskilt från andra tjänster som de tillhandahåller.

AVSNITT 10

ELEKTRONISKA ARKIVERINGSTJÄNSTER

Artikel 45i

Rättslig verkan av elektroniska arkiveringstjänster

1. Elektroniska uppgifter och elektroniska dokument som bevaras genom en elektronisk arkiveringstjänst får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller inte är bevarade genom en kvalificerad elektronisk arkiveringstjänst.

2. Elektroniska uppgifter och elektroniska dokument som bevaras genom en kvalificerad elektronisk arkiveringstjänst ska omfattas av en presumtion om deras integritet och ursprung under hela den period som de bevaras av den kvalificerade tillhandahållaren av betrodda tjänster.

Artikel 45j

Krav på kvalificerade elektroniska arkiveringstjänster

1. Kvalificerade elektroniska arkiveringstjänster ska uppfylla följande krav:

   a) De ska tillhandahållas av kvalificerade tillhandahållare av betrodda tjänster.

   b) De ska använda förfaranden och teknik som kan säkerställa att elektroniska uppgifter och elektroniska dokument håller och är läsbara även efter den tekniska giltighetstiden och åtminstone under hela den rättsliga eller avtalsenliga bevarandeperioden, samtidigt som deras integritet och korrekta ursprung bibehålls.

c) De ska säkerställa att dessa elektroniska uppgifter och elektroniska dokument bevaras på ett sådant sätt att de skyddas mot förlust och ändring, med undantag för ändringar som rör deras medium eller elektroniska format.

d) De ska göra det möjligt för behöriga förlitande parter att ta emot en rapport på ett automatiserat sätt som bekräftar att elektroniska uppgifter och elektroniska dokument som hämtats från ett kvalificerat elektroniskt arkiv omfattas av presumtionen om uppgifternas integritet från början av bevarandeperioden till tidpunkten för hämtningen.

Den rapport som avses i första stycket led d ska tillhandahållas på ett tillförlitligt och effektivt sätt och ska vara försedd med den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln för tillhandahållaren av den kvalificerade elektroniska arkiveringstjänsten.

2. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för kvalificerade elektroniska arkiveringstjänster. Överensstämmelse med kraven på kvalificerade elektroniska arkiveringstjänster ska presumeras om en kvalificerad elektronisk arkiveringstjänst uppfyller kraven i dessa standarder, specifikationer och förfaranden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

AVSNITT 11

ELEKTRONISKA LIGGARE

Artikel 45k

Rättslig verkan av elektroniska liggare

1. En elektronisk liggare får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att den har elektronisk form eller inte uppfyller kraven på kvalificerade elektroniska liggare.

2. Dataloggar i en kvalificerad elektronisk liggare ska omfattas av en presumtion om deras unika och korrekta sekventiella kronologiska ordningsföljd och deras integritet.

Artikel 45l

Krav på kvalificerade elektroniska liggare

1. Kvalificerade elektroniska liggare ska uppfylla följande krav:

   a) De ska skapas och förvaltas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.

   b) De ska fastställa ursprunget till dataloggarna i liggaren.

   c) De ska säkerställa unik sekventiell kronologisk ordning för dataloggarna i liggaren.

   d) De ska registrera data på ett sådant sätt att alla senare ändringar av uppgifterna omedelbart kan upptäckas, varvid deras integritet säkerställs över tid.

2. Uppfyllelse av kraven i punkt 1 ska presumeras om en elektronisk liggare uppfyller kraven ide standarder, specifikationer och förfaranden som avses i punkt 3.

3. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen, genom genomförandeakter, upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer och förfaranden för de krav som fastställs i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

47. Följande kapitel ska införas:

”KAPITEL IVa
STYRNINGSRAMVERK

Artikel 46a
Tillsyn över ramverket för den europeiska digitala identitetsplånboken

1. Medlemsstaterna ska utse ett eller flera tillsynsorgan som är etablerade på deras territorium.

De tillsynsorgan som utses enligt första stycket ska ges nödvändiga befogenheter och adekvata resurser för att de ska kunna utföra sina uppgifter på ett ändamålsenligt, effektivt och oberoende sätt.

2. Medlemsstaterna ska till kommissionen anmäla namn och adresser för de tillsynsorgan som utsetts enligt punkt 1 och eventuella senare ändringar av dessa. Kommissionen ska offentliggöra en förteckning över de anmälda tillsynsorganen.

3. De tillsynsorgan som utsetts enligt punkt 1 ska ha följande roll:

   a) Utöva tillsyn över tillhandahållare av europeiska digitala identitetsplånböcker etablerade i den medlemsstat där de har utsetts och, genom tillsynsverksamhet på förhand och i efterhand, säkerställa att dessa tillhandahållare och de europeiska digitala identitetsplånböcker som de tillhandahåller uppfyller kraven i denna förordning.

   b) Vid behov vidta åtgärder med avseende på tillhandahållare av europeiska digitala identitetsplånböcker etablerade på territoriet för den medlemsstat som utsett den, genom tillsynsverksamhet i efterhand, när de informeras om att tillhandahållarna eller de europeiska digitala identitetsplånböcker som de tillhandahåller inte uppfyller kraven i denna förordning.

4. Uppgifterna för det tillsynsorgan som utsetts enligt punkt 1 ska särskilt inbegripa följande:

   a) Samarbeta med andra tillsynsorgan och bistå dem i enlighet med artiklarna 46c och 46e.

   b) Begära information som är nödvändig för att övervaka efterlevnaden av denna förordning.

c) Informera de relevanta behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555 i berörda medlemsstater om alla betydande säkerhetsincidenter eller integritetsförluster som de får kännedom om vid utförandet av sina uppgifter och, i händelse av en betydande säkerhetsincident eller integritetsförlust som berör andra medlemsstater, informera den gemensamma kontaktpunkt som utsetts eller inrättats enligt artikel 8.3 i direktiv (EU) 2022/2555 i den berörda medlemsstaten och de gemensamma kontaktpunkter som utsetts i enlighet med artikel 46c.1 i denna förordning i övriga berörda medlemsstater, och informera allmänheten eller kräva att tillhandahållare av europeiska digitala identitetsplånböcker gör detta om tillsynsorganet slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten skulle ligga i allmänhetens intresse.

d) Utföra inspektioner på plats och utöva tillsyn på distans.

e) Kräva att tillhandahållare av europeiska digitala identitetsplånböcker åtgärdar varje underlåtenhet att uppfylla kraven i denna förordning.

f) Tillfälligt eller permanent upphäva registreringen och inkluderingen av förlitande parter i den mekanism som avses i artikel 5b.7 vid olaglig eller bedräglig användning av den europeiska digitala identitetsplånboken.

g) Samarbeta med behöriga tillsynsmyndigheter som inrättats enligt artikel 51 i förordning (EU) 2016/679, särskilt genom att utan onödigt dröjsmål informera dem vid misstänkta överträdelser av reglerna om skydd av personuppgifter, och om säkerhetsincidenter som förefaller utgöra personuppgiftsincidenter.

5. Om det tillsynsorgan som utsetts enligt punkt 1 kräver att tillhandahållaren av en europeisk digital identitetsplånbok åtgärdar en underlåtenhet att uppfylla kraven enligt denna förordning i enlighet med punkt 4 e, och tillhandahållaren inte agerar i enlighet med detta och, i tillämpliga fall, inom en tidsfrist som fastställts av det tillsynsorganet, får det tillsynsorgan som utsetts enligt punkt 1, särskilt med beaktande av denna underlåtenhets omfattning, varaktighet och följder, ålägga tillhandahållaren att tillfälligt eller permanent upphöra med tillhandahållandet av den europeiska digitala identitetsplånboken. Tillsynsorganet ska utan onödigt dröjsmål informera tillsynsorganen i övriga medlemsstater, kommissionen, förlitande parter och användare av den europeiska digitala identitetsplånboken om beslutet att kräva att tillhandahållandet av den europeiska digitala identitetsplånboken tillfälligt eller permanent upphör.

6. Senast den 31 mars varje år ska varje tillsynsorgan som utsetts enligt punkt 1 överlämna en rapport om det föregående kalenderårets huvudverksamhet till kommissionen. Kommissionen ska göra de årliga rapporterna tillgängliga för Europaparlamentet och rådet.

7. Senast den … [tolv månader från dagen för denna ändringsförordnings ikraftträdande] ska kommissionen genom genomförandeakter fastställa formaten och förfarandena för den rapport som avses i punkt 6 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 46b

Tillsyn över betrodda tjänster

1. Medlemsstaterna ska utse ett tillsynsorgan som är etablerat på deras territorium eller utse, efter ömsesidig överenskommelse med en annan medlemsstat, ett tillsynsorgan som är etablerat i den andra medlemsstaten. Det tillsynsorganet ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet vad gäller betrodda tjänster.

   De tillsynsorgan som utses enligt första stycket ska ges nödvändiga befogenheter och adekvata resurser för att de ska kunna utföra sina uppgifter.

2. Medlemsstaterna ska till kommissionen anmäla namn och adresser för de tillsynsorgan som utsetts enligt punkt 1 och eventuella senare ändringar av dessa. Kommissionen ska offentliggöra en förteckning över de anmälda tillsynsorganen.

3. De tillsynsorgan som utses enligt punkt 1 ska ha följande roll:

   a) Utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts och, genom tillsynsverksamhet på förhand och i efterhand, säkerställa att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning.

   b) Vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts genom tillsynsverksamhet i efterhand om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning.

4. Uppgifterna för det tillsynsorgan som utsetts enligt punkt 1 ska särskilt inbegripa följande:

a) Informera de relevanta behöriga myndigheter som utsetts eller inrättats enligt artikel 8.1 i direktiv (EU) 2022/2555 i de berörda medlemsstaterna om alla betydande säkerhetsincidenter eller integritetsförluster som de får kännedom om under utförandet av sina uppgifter och, i händelse av en betydande säkerhetsincident eller integritetsförlust som berör andra medlemsstater, informera den gemensamma kontaktpunkt som utsetts eller inrättats enligt artikel 8.3 i direktiv (EU) 2022/2555 i den berörda medlemsstaten och de gemensamma kontaktpunkter som utsetts enligt artikel 46c.1 i denna förordning i övriga berörda medlemsstater, och informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör detta om tillsynsorganet slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten skulle ligga i allmänhetens intresse.

b) Samarbeta med andra tillsynsorgan och bistå dem i enlighet med artiklarna 46c och 46e.

c) Analysera de rapporter om bedömning av överensstämmelse som avses i artiklarna 20.1 och 21.1.

d) Rapportera till kommissionen om sin huvudverksamhet i enlighet med punkt 6 i denna artikel.

e) Granska eller begära att ett organ för bedömning av överensstämmelse gör en bedömning av överensstämmelse avseende kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 20.2.

f) Samarbeta med behöriga tillsynsmyndigheter som inrättats enligt artikel 51 i förordning (EU) 2016/679, särskilt genom att utan onödigt dröjsmål informera dem vid misstänkta överträdelser av reglerna om skydd av personuppgifter, och om säkerhetsincidenter som förefaller utgöra personuppgiftsincidenter.

g) Bevilja status som kvalificerad tillhandahållare av betrodda tjänster och till de tjänster som de tillhandahåller samt återkalla denna status i enlighet med artiklarna 20 och 21.

h) Informera det organ som är ansvarigt för den nationella förteckning över tillhandahållare av betrodda tjänster som avses i artikel 22.3 om sina beslut om beviljande eller återkallande av status som kvalificerad, såvida inte det organet även är det tillsynsorgan som utsetts enligt punkt 1 i denna artikel.

i) Kontrollera befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande i sådana fall när den kvalificerade tillhandahållaren av betrodda tjänster upphör med sin verksamhet, inbegripet hur information hålls tillgänglig i enlighet med artikel 24.2 h.

j) Kräva att tillhandahållare av betrodda tjänster åtgärdar varje underlåtenhet att uppfylla kraven i denna förordning.

k) Undersöka påståenden från tillhandahållare av webbläsare enligt artikel 45a och vid behov vidta åtgärder.

5. Medlemsstaterna får kräva att det tillsynsorgan som utsetts enligt punkt 1 inrättar, underhåller och uppdaterar en infrastruktur för betrodda tjänster i enlighet med nationell rätt.

6. Senast den 31 mars varje år ska varje tillsynsorgan som utsetts enligt punkt 1 överlämna en rapport om det föregående kalenderårets huvudverksamhet till kommissionen. Kommissionen ska göra de årliga rapporterna tillgängliga för Europaparlamentet och rådet.

7. Senast den … [12 månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen anta riktlinjer för utövningen, av det tillsynsorgan som utsetts enligt punkt 1 i denna artikel, av de uppgifter som avses i punkt 4 i denna artikel och, genom genomförandeakter, fastställa format och förfaranden för den rapport som avses i punkt 6 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 46c

Gemensamma kontaktpunkter

1. Varje medlemsstat ska utse en gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering.

2. Varje gemensam kontaktpunkt ska utöva en sambandsfunktion för att underlätta gränsöverskridande samarbete mellan tillsynsorganen för tillhandahållare av betrodda tjänster och mellan tillsynsorganen för tillhandahållare av europeiska digitala identitetsplånböcker och, när så är lämpligt, med kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) och med andra behöriga myndigheter i sin medlemsstat.

3. Varje medlemsstat ska offentliggöra och utan onödigt dröjsmål meddela kommissionen namnen på och adresserna till den gemensamma kontaktpunkt som utsetts enligt punkt 1 och eventuella senare ändringar av denna.

4. Kommissionen ska offentliggöra en förteckning över den gemensamma kontaktpunkt som utsetts enligt punkt 3.

Artikel 46d

Ömsesidigt bistånd

1. För att underlätta tillsynen och efterlevnaden av skyldigheterna enligt denna förordning får de tillsynsorgan som utsetts enligt artikel 46a.1, bland annat genom den samarbetsgrupp som inrättats enligt artikel 46e.1, söka ömsesidigt bistånd från tillsynsorganen i en annan medlemsstat där tillhandahållaren av den europeiska digitala identitetsplånboken eller tillhandahållaren av betrodda tjänster är etablerad, eller där dennes nätverks- och informationssystem är belägna eller dess tjänster tillhandahålls.

2. Det ömsesidiga biståndet ska åtminstone innebära att

a) det tillsynsorgan som tillämpar tillsyns- och verkställighetsåtgärder i en medlemsstat ska informera och samråda med tillsynsorganet i den andra berörda medlemsstaten,

b) ett tillsynsorgan får begära att tillsynsorganet i en annan berörd medlemsstat vidtar tillsyns- eller verkställighetsåtgärder, till exempel begäranden om att utföra inspektioner i samband med de rapporter om bedömning av överensstämmelse som avses i artiklarna 20 och 21 avseende tillhandahållandet av betrodda tjänster,

c) vid behov får tillsynsorganen genomföra gemensamma utredningar tillsammans med tillsynsmyndigheterna i andra medlemsstater.

De berörda medlemsstaterna ska i enlighet med sin nationella rätt besluta om och inrätta arrangemangen och förfarandena för gemensamma åtgärder enligt första stycket.

3. Ett tillsynsorgan till vilket en begäran om bistånd riktas får vägra att tillmötesgå denna begäran på grundval av något av följande skäl:

a) Det begärda biståndet står inte i proportion till den tillsynsverksamhet som tillsynsorganet utför i enlighet med artiklarna 46a och 46b.

b) Tillsynsorganet är inte behörigt att tillhandahålla det begärda biståndet.

c) Det skulle stå i strid med denna förordning att tillhandahålla det begärda biståndet.

4. Senast den … [12 månader efter dagen för denna ändringsförordnings ikraftträdande] och därefter vartannat år ska den samarbetsgrupp som inrättats enligt artikel 46e.1 utfärda riktlinjer om organisatoriska aspekter och förfaranden för det ömsesidiga bistånd som avses i punkterna 1 och 2 i den här artikeln.

Artikel 46e

Den europeiska samarbetsgruppen för digital identitet

1. För att stödja och underlätta medlemsstaternas gränsöverskridande samarbete och informationsutbyte om betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering ska kommissionen inrätta en europeisk samarbetsgrupp för digital identitet (*samarbetsgruppen*).

2. Samarbetsgruppen ska bestå av företrädare som utnämns av medlemsstaterna och av kommissionen. Samarbetsgruppen ska ledas av kommissionen. Kommissionen ska tillhandahålla samarbetsgruppens sekretariat.

3. Företrädare för berörda parter får, på ad hoc-basis, inbjudas att närvara vid samarbetsgruppens möten och delta i dess arbete som observatörer.

4. Enisa ska bjudas in att delta som observatör i samarbetsgruppens arbete när den utbyter åsikter, bästa praxis och information om relevanta cybersäkerhetsaspekter såsom anmälan av säkerhetsincidenter, och när användning av cybersäkerhetscertifikat eller cybersäkerhetsstandarder behandlas.

5. Samarbetsgruppen ska ha följande uppgifter:

   a) Utbyta råd och samarbeta med kommissionen om nya politiska initiativ på området digitala identitetsplånböcker, medel för elektronisk identifiering och betrodda tjänster.

   b) Vid behov ge kommissionen råd vid utarbetandet av utkast till genomförandeakter och delegerade akter som ska antas enligt denna förordning.

   c) För att stödja tillsynsorganens genomförande av bestämmelserna i denna förordning:

      i) Utbyta bästa praxis och information om genomförandet av bestämmelserna i denna förordning.

      ii) Bedöma den relevanta utvecklingen inom sektorerna för digitala identitetsplånböcker, elektronisk identifiering och betrodda tjänster.

      iii) Anordna gemensamma möten med relevanta intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta synpunkter på framväxande politiska utmaningar.

iv) Med stöd av Enisa utbyta åsikter, bästa praxis och information om relevanta cybersäkerhetsaspekter när det gäller europeiska digitala identitetsplånböcker, system för elektronisk identifiering och betrodda tjänster.

v) Utbyta bästa praxis om utarbetande och genomförande av strategier för anmälan av säkerhetsincidenter, och gemensamma åtgärder enligt artiklarna 5e och 10.

vi) Anordna gemensamma möten med den samarbetsgrupp för nät- och informationssäkerhet som inrättats enligt artikel 14.1 i direktiv (EU) 2022/2555 för att utbyta relevant information om betrodda tjänster och elektronisk identifiering som är relaterade till cyberhot, incidenter, sårbarheter, medvetandehöjande initiativ, utbildning, övningar och kompetens, kapacitetsuppbyggnad, kapacitet för standarder och tekniska specifikationer samt standarder och tekniska specifikationer.

vii) På begäran av ett tillsynsorgan diskutera specifika begäranden om ömsesidigt bistånd enligt artikel 46d.

viii) Underlätta informationsutbytet mellan tillsynsorganen genom att ge vägledning om organisatoriska aspekter och förfaranden för det ömsesidiga bistånd som avses i artikel 46d.

d) Anordna sakkunnigbedömningar av system för elektronisk identifiering som ska anmälas enligt denna förordning.

6. Medlemsstaterna ska säkerställa att deras utsedda företrädare samarbetar på ett effektivt och ändamålsenligt sätt i samarbetsgruppen.

7. Senast den … [tolv månader efter dagen för denna ändringsförordnings ikraftträdande] ska kommissionen genom genomförandeakter införa de nödvändiga förfarandemässiga arrangemangen för att främja samarbete mellan medlemsstaterna enligt punkt 5 d i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

48. Artikel 47 ska ändras på följande sätt:

a) Punkterna 2 och 3 ska ersättas med följande:

”2. Den befogenhet att anta delegerade akter som avses i artiklarna 5c.7, 24.6 och 30.4 ska ges till kommissionen tills vidare från och med den 17 september 2014.

3. Den delegering av befogenhet som avses i artiklarna 5c.7, 24.6 och 30.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.”

b) Punkt 5 ska ersättas med följande:

”5. En delegerad akt som antas enligt artikel 5c.7, 24.6 eller 30.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.”

49. Följande artikel ska införas i kapitel VI:

”*Artikel 48a*
Rapporteringskrav

1. Medlemsstaterna ska säkerställa att det samlas in statistik om hur europeiska digitala identitetsplånböcker och de kvalificerade betrodda tjänster som tillhandahålls på deras territorium används.

2. Den statistik som samlas in i enlighet med punkt 1 ska omfatta följande:

a) Antalet fysiska och juridiska personer som har en giltig europeisk digital identitetsplånbok.

b) Antalet och typen av tjänster som godtar användning av den europeiska digitala identitetsplånboken.

c) Antalet klagomål från användare och konsumentskydds- eller dataskyddsincidenter som rör förlitande parter och kvalificerade betrodda tjänster.

d) En sammanfattande rapport med uppgifter om incidenter som hindrar användningen av den europeiska digitala identitetsplånboken.

e) En sammanfattning av betydande säkerhetsincidenter, dataöverträdelser och berörda användare av europeiska digitala identitetsplånböcker eller kvalificerade betrodda tjänster.

3. Den statistik som avses i punkt 2 ska göras tillgänglig för allmänheten i ett öppet och allmänt använt maskinläsbart format.

4. Senast den 31 mars varje år ska medlemsstaterna lämna en rapport om den statistik som samlats in i enlighet med punkt 2 till kommissionen.”

50. Artikel 49 ska ersättas med följande:

”*Artikel 49*
Översyn

1. Kommissionen ska senast den … [24 månader efter dagen för denna ändringsförordnings ikraftträdande], göra en översyn över denna förordnings tillämpning och rapportera resultaten till Europaparlamentet och rådet. I den rapporten ska kommissionen särskilt utvärdera huruvida det är lämpligt att ändra denna förordnings tillämpningsområde eller dess särskilda bestämmelser, inbegripet särskilt bestämmelserna i artikel 5c.5, med beaktande av den erfarenhet som erhållits vid tillämpningen av denna förordning samt den tekniska och rättsliga utvecklingen och marknadsutvecklingen. Rapporten ska vid behov åtföljas av ett förslag till ändringar av denna förordning.

2. Den rapport som avses i punkt 1 ska innehålla en bedömning av tillgängligheten, säkerheten och användbarheten för de anmälda elektroniska medel för identifiering och de europeiska digitala identitetsplånböcker som omfattas av denna förordning, och bedöma om alla privata tillhandahållare av nättjänster som använder sig av tredje parts tjänster för elektronisk identifiering för användarautentisering ska åläggas att godta användningen av anmälda medel för elektronisk identifiering och den europeiska digitala identitetsplånboken.

3. Senast den … [6 år efter dagen för denna ändringsförordnings ikraftträdande] och vart fjärde år därefter ska kommissionen lämna den rapport som avses i första stycket till Europaparlamentet och rådet om de framsteg som gjorts i förhållande till denna förordnings mål.”

51. Artikel 51 ska ersättas med följande:

”*Artikel 51*
Övergångsbestämmelser

1. Säkra anordningar för skapande av underskrifter för vilka överensstämmelsen har fastställts i enlighet med artikel 3.4 i direktiv 1999/93/EG ska även fortsättningsvis anses vara kvalificerade anordningar för skapande av elektroniska underskrifter enligt denna förordning fram till och med den … [36 månader efter dagen för denna ändringsförordnings ikraftträdande].

2. Kvalificerade certifikat som utfärdas till fysiska personer enligt direktiv 1999/93/EG ska även fortsättningsvis anses som kvalificerade certifikat för elektroniska underskrifter enligt denna förordning fram till och med den … [24 månader från dagen för denna ändringsförordnings ikraftträdande].

3. Förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar på distans som utförs av andra kvalificerade tillhandahållare av betrodda tjänster än sådana kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade betrodda tjänster för förvaltning av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar på distans i enlighet med artiklarna 29a och 39a får utföras utan att status som kvalificerad för tillhandahållandet av dessa förvaltningstjänster behöver erhållas förrän den … [24 månader från dagen för denna ändringsförordnings ikraftträdande].

4. Kvalificerade tillhandahållare av betrodda tjänster som har beviljats status som kvalificerad enligt denna förordning före den … [dagen för denna ändringsförordnings ikraftträdande] ska lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet som styrker överensstämmelse med artikel 24.1, 24.1a och 24.1b så snart som möjligt och i alla händelser senast den … [24 månader efter dagen för denna ändringsförordnings ikraftträdande].”.

52. Bilagorna I–IV ska ändras i enlighet med bilagorna I–IV till den här förordningen.

53. Nya bilagor V, VI och VII ska läggas till i enlighet med bilagorna V, VI och VII till den här förordningen.

Artikel 2

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i …

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA I

I bilaga I till förordning (EU) nr 910/2014 ska led i ersättas med följande:

”i) Information om det kvalificerade certifikatets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.”

BILAGA II

I bilaga II till förordning (EU) nr 910/2014 ska punkterna 3 och 4 utgå.

BILAGA III

I bilaga III till förordning (EU) nr 910/2014 ska led i ersättas med följande:

”i) Information om det kvalificerade certifikatets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.”

BILAGA IV

Bilaga IV till förordning (EU) nr 910/2014 ska ändras på följande sätt:

1. Led c ska ersättas med följande:

”c) För fysiska personer: åtminstone namnet på den person som certifikatet utfärdats till eller en pseudonym; om en pseudonym används ska detta tydligt anges.

ca) För juridiska personer: en unik uppsättning uppgifter som otvetydigt avser den juridiska person som certifikatet utfärdats till, med åtminstone namnet på den juridiska person som intyget utfärdats till och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i de officiella registren.”

2. Led j ska ersättas med följande:

”j) Information om det kvalificerade certifikatets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.”

BILAGA V

”BILAGA V

KRAV PÅ KVALIFICERADE ELEKTRONISKA ATTRIBUTSINTYG

Kvalificerade elektroniska attributsintyg ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att intyget har utfärdats som ett kvalificerat elektroniskt attributsintyg.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar det kvalificerade elektroniska attributsintyget, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

   i) för en juridisk person: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,

   ii) för en fysisk person: personens namn.

c) En uppsättning uppgifter som otvetydigt avser den enhet som de intygade attributen hänvisar till; om en pseudonym används ska detta anges tydligt.

d) Det intygade attributet eller de intygade attributen, inbegripet, i tillämpliga fall, de uppgifter som är nödvändiga för att fastställa omfattningen för dessa attribut.

e) Detaljerade uppgifter om när intyget börjar respektive upphör att gälla.

f) Intygets identitetskod, vilken måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster, och, i tillämpliga fall, uppgift om det intygssystem som attributsintyget omfattas av.

g) Den kvalificerade elektroniska underskriften eller den kvalificerade elektroniska stämpeln för den utfärdande kvalificerade tillhandahållaren av betrodda tjänster.

h) Uppgift om var det certifikat som stöder den kvalificerade elektroniska underskrift eller den kvalificerade elektroniska stämpel som avses i led g är tillgängligt kostnadsfritt.

i) Information om det kvalificerade intygets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar är lokaliserade.”

BILAGA VI

”BILAGA VI

MINIMIFÖRTECKNING ÖVER ATTRIBUT

Enligt artikel 45e ska medlemsstaterna säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller elektroniska attributsintyg att på användarens begäran på elektronisk väg kontrollera äktheten hos följande attribut gentemot den relevanta autentiska källan på nationell nivå eller via särskilt utsedda mellanhänder som är erkända på nationell nivå, i enlighet med unionsrätten eller nationell rätt och i de fall då dessa attribut utgår från autentiska källor inom den offentliga sektorn:

1. Adress.

2. Ålder.

3. Kön.

4. Civilstånd.

5. Familjesammansättning.

6. Nationalitet eller medborgarskap.

7. Utbildningskvalifikationer, titlar och licenser.

8. Yrkeskvalifikationer, titlar och licenser.

9. Befogenheter och uppdrag att företräda fysiska eller juridiska personer

10. Offentliga tillstånd och licenser.

11. För juridiska personer, finansiella uppgifter och företagsuppgifter.”

BILAGA VII

”BILAGA VII

KRAV PÅ ELEKTRONISKA INTYG PÅ
ATTRIBUT UTFÄRDADE AV ELLER PÅ UPPDRAG AV ETT OFFENTLIGT ORGAN SOM ANSVARAR FÖR EN AUTENTISK KÄLLA

Ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att intyget har utfärdats som ett elektroniskt attributsintyg utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.

b) En uppsättning uppgifter som otvetydigt avser det offentliga organ som utfärdar det elektroniska attributsintyget, inbegripet åtminstone den medlemsstat där det offentliga organet är etablerat och dess namn och, i tillämpliga fall, dess registreringsnummer i enlighet med vad som anges i de officiella registren.

c) En uppsättning uppgifter som otvetydigt avser den enhet som de intygade attributen hänvisar till; om en pseudonym används ska detta anges tydligt.

d) Det intygade attributet eller de intygade attributen, inbegripet, i tillämpliga fall, de uppgifter som är nödvändiga för att fastställa omfattningen för dessa attribut.

e) Detaljerade uppgifter om när intyget börjar respektive upphör att gälla.

f) Intygets identitetskod, vilken måste vara unik för det utfärdande offentliga organet, och, i tillämpliga fall, uppgift om det intygssystem som attributsintyget omfattas av.

g) Det utfärdande organets kvalificerade elektroniska underskrift eller kvalificerade elektroniska stämpel.

h) Uppgift om var det certifikat som stöder den kvalificerade elektroniska underskrift eller den kvalificerade elektroniska stämpel som avses i led g är tillgängligt kostnadsfritt.

i) Information om intygets giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar om intygets giltighet är lokaliserade.”