Europeiska unionens råd

Bryssel den 6 december 2022
(OR. en)

15706/22

Interinstitutionellt ärende:
2021/0136 (COD)

TELECOM 519
COMPET 1006
MI 919
DATAPROTECT 352
JAI 1634
CODEC 1941

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	6 december 2022
till:	Delegationerna
Föreg. dok. nr:	14959/22 + ADD 1 + ADD 2
Komm. dok. nr:	9471/21
Ärende:	Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet – Allmän riktlinje (6 december 2022)

För delegationerna bifogas rådets allmänna riktlinje om det ovannämnda förslaget som godkändes av rådet (transport, telekommunikation och energi) vid dess 3917:e möte den 6 december 2022.

Den allmänna riktlinjen fastställer rådets preliminära ståndpunkt om detta förslag och utgör grunden för förberedelserna inför förhandlingarna med Europaparlamentet.

BILAGA

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk 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],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I kommissionens meddelande av den 19 februari 2020, Att forma EU:s digitala framtid[2], tillkännages det att Europaparlamentets och rådets förordning (EU) nr 910/2014 ska revideras i syfte att förbättra dess effektivitet, utvidga dess förmåner till den privata sektorn och främja betrodda digitala identiteter för alla européer.

[1] EUT C , , s. .
[2] COM/2020/67 final

(2) I sina slutsatser av den 1–2 oktober 2020[3] uppmanade Europeiska rådet kommissionen att föreslå en utveckling av ett EU-omfattande ramverk för säker offentlig elektronisk identifiering, inklusive interoperabla digitala 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 kommissionens meddelande av den 9 mars 2021, Digital kompass 2030: den europeiska vägen in i det digitala decenniet[4], fastställs målet att inrätta en EU-ram som senast 2030 ska ha medfört en omfattande utbyggnad av en betrodd, användarkontrollerad identitet, som innebär att alla medborgare kan kontrollera sin egen onlineinteraktion och onlinenärvaro.

(4) En mer harmoniserad strategi för digital identifiering bör minska de risker och kostnader som den nuvarande fragmenteringen har lett till på grund av användningen av olika nationella lösningar och kommer att stärka den inre marknaden genom att göra det möjligt för medborgarna, andra invånare enligt definitionen i den nationella lagstiftningen och företag att identifiera sig online på ett bekvämt och enhetligt sätt i hela unionen. Den europeiska e-identitetsplånboken kommer att förse fysiska och juridiska personer i hela unionen med harmoniserade medel för elektronisk identifiering som gör det möjligt för dem att autentisera och dela 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 attesteringar av attribut, till exempel en universitetsexamen som erkänns och godtas överallt i unionen. Syftet med ramen för europeisk digital identitet är att ersätta beroendet av nationella digitala id-lösningar med elektroniska attesteringar av attribut som är giltiga på europeisk nivå. Tillhandahållare av elektroniska intyg på attribut bör gynnas av en tydlig och enhetlig uppsättning av regler, och offentliga förvaltningar bör kunna förlita sig på elektroniska dokument i ett visst format.

---

3 https://www.consilium.europa.eu/sv/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020

4 COM/2021/118 final/2

(4a) Flera medlemsstater har infört och använder i stor utsträckning medel för elektronisk identifiering som i dag godtas av tjänsteleverantörer i unionen. Dessutom gjordes investeringar i både nationella och gränsöverskridande lösningar på grundval av den nuvarande eIDA-förordningen, inbegripet den tekniska infrastrukturen för interoperabilitet mellan eIDA-noder. För att garantera komplementaritet och ett snabbt ibruktagande av europeiska e-identitetsplånböcker av nuvarande användare av anmälda medel för elektronisk identifiering och för att minimera konsekvenserna för befintliga tjänsteleverantörer, förväntas de europeiska e-identitetsplånböckerna dra nytta av att bygga vidare på erfarenheterna av befintliga medel för elektronisk identifiering och utnyttja den införda eIDA-infrastrukturen på europeisk och nationell nivå.

(5) För att förbättra de europeiska företagens konkurrenskraft bör tillhandahållare av onlinetjänster kunna förlita sig på digitala id-lösningar som erkänns i hela unionen, oavsett vilken medlemsstat de har tillhandahållits i, och därmed dra nytta av en harmoniserad europeisk strategi för tillförlitlighet, säkerhet och interoperabilitet. Både användare och tjänsteleverantörer bör kunna gynnas av att samma rättsliga värde ges till elektroniska intyg på attribut i hela unionen.

(6) Förordning (EU) nr 2016/679[5] är tillämplig 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 intyg på attribut kombinerar personuppgifter från andra tjänster med personuppgifter som rör de tjänster som omfattas av tillämpningsområdet för denna förordning. Personuppgifter som rör tillhandahållandet av de europeiska e-identitetsplånböckerna bör hållas logiskt avskilda från andra data som innehas av utfärdaren. Denna förordning hindrar inte utfärdare av europeiska e-identitetsplånböcker från att tillämpa ytterligare tekniska åtgärder som bidrar till skyddet av personuppgifter, såsom fysisk åtskillnad mellan personuppgifter som rör tillhandahållandet av plånböcker och andra uppgifter som innehas av utfärdaren.

---

[5] 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.

(7) Harmoniserade villkor måste fastställas för inrättandet av en ram för de europeiska e-identitetsplånböcker som ska tillhandahållas av medlemsstaterna, så att alla unionsmedborgare och andra invånare enligt definitionen i nationell lagstiftning kan dela sina identitetsuppgifter på ett säkert, användarvänligt och bekvämt sätt under användarens egen kontroll. De tekniker som används för att uppnå dessa mål bör utformas för att uppnå högsta möjliga nivå av säkerhet, integritet, användarvänlighet och användbarhet. Medlemsstaterna bör säkerställa lika tillgång till digital identifiering för alla sina medborgare och invånare.

(8) För att säkerställa att förlitande parter kan förlita sig på att använda europeiska e-identitetsplånböcker och för att skydda användaren mot olaglig användning av känsliga uppgifter bör förlitande parter registreras som en del av ett anmälningsförfarande. De anmälningskrav som är tillämpliga på förlitande parter bör i de flesta fall baseras på tillhandahållandet av en begränsad mängd information som krävs för autentisering av den förlitande parten gentemot den europeiska e-identitetsplånboken. Kraven bör också medge användning av automatiska eller enkla förfaranden för rapportering på egen hand, inbegripet medlemsstaternas förlitan på och användning av befintliga register. För kategorier av känsliga uppgifter får det dock finnas särskilda ordningar på nationell nivå eller unionsnivå, som kan innebära strängare krav på registrering och tillstånd för förlitande parter för att förhindra olaglig användning av identitetsuppgifter i sådana fall. Vid annan användning kan förlitande parter undantas från att anmäla sin avsikt att använda den europeiska e-identitetsplånboken, till exempel när en rätt att verifiera specifika attribut inte kräver eller medger elektronisk autentisering av den förlitande parten. Vanligtvis kan användaren i dessa scenarier med fysiska möten identifiera den förlitande parten tack vare sammanhanget, som till exempel vid kontakt med en biluthyrare eller apotekare. Anmälningsförfarandet är tänkt att styras av sektorsspecifik unionslagstiftning eller nationell lagstiftning, eftersom detta gör det möjligt att hantera olika slags användning som kan skilja sig åt i fråga om registreringskrav, driftsätt (online/offline) eller i fråga om kravet på autentisering av enheter som kan samverka med den europeiska e-identitetsplånboken. Verifieringen av användningen av den europeiska e-identitetsplånboken av förlitande parter bör inte obligatoriskt verkställas på nivån för den europeiska e-identitetsplånboken.

(9) Alla europeiska e-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 plånböckerna även användas för att tillgodose de institutionella behoven vid offentliga förvaltningar, internationella organisationer samt EU:s institutioner, organ, kontor och byråer. I många sektorer är det viktigt att kunna använda plånböckerna offline, bland annat i hälso- och sjukvårdssektorn, där tjänsterna ofta tillhandahålla vid direkta kontakter, och e-recept bör kunna autentiseras med hjälp av QR-koder eller liknande tekniker. För att säkerställa en hög tillförlitlighetsnivå bör de europeiska e-identitetsplånböckerna gynnas av den potential som erbjuds via manipuleringssäkra lösningar såsom säkerhetsdetaljer för att uppfylla säkerhetskraven i denna förordning. De europeiska e-identitetsplånböckerna bör även göra det möjligt för användarna att skapa och använda kvalificerade elektroniska underskrifter och stämplar som godtas i hela EU. För att ge personer och företag i hela EU fördelar i form av enkel hantering och sänkta kostnader, däribland genom att tillåta behörigheter att företräda och elektroniska fullmakter, bör medlemsstaterna utfärda europeiska e-identitetsplånböcker på grundval av gemensamma standarder för att säkerställa sömlös interoperabilitet och en hög säkerhetsnivå. Det är endast medlemsstaternas behöriga myndigheter som kan fastställa identiteter med tillräckligt hög grad av tillförlitlighet och därmed garantera att en person faktiskt är den person som han eller hon påstår sig vara. Därför måste de europeiska e-identitetsplånböckerna bygga på den juridiska identiteten för medborgare, andra invånare och juridiska personer. Tilliten till de europeiska e-identitetsplånböckerna skulle förstärkas om de utfärdande parterna hade varit tvungna att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som står i rimlig proportion till riskerna för fysiska personers rättigheter och friheter i linje med förordning (EU) 2016/679. Utfärdandet, användningen av autentisering och återkallelsen av europeiska e-identitetsplånböcker ska vara avgiftsfri för fysiska personer. Tjänster som är beroende av användning av plånboken får leda till kostnader för exempelvis utfärdande av elektroniska intyg på attribut till plånboken.

(9a) Det är fördelaktigt att underlätta spridningen och användningen av europeiska e-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 får medlemsstaterna föreskriva rättsliga och organisatoriska åtgärder för att öka flexibiliteten för utfärdare av europeiska e-identitetsplånböcker och medge ytterligare funktioner i de europeiska e-identitetsplånböckerna utöver vad som fastställs i denna förordning, bland annat genom ökad interoperabilitet med befintliga nationella medel för elektronisk identifiering. Detta bör inte på något sätt inverka negativt på tillhandahållandet av de europeiska e-identitetsplånböckernas centrala funktioner i enlighet med denna förordning och inte heller främja befintliga nationella lösningar framför europeiska e-identitetsplånböcker. Eftersom dessa ytterligare funktioner går utöver denna förordning omfattas de inte av de bestämmelser om gränsöverskridande användning av europeiska e-identitetsplånböcker som fastställs i denna förordning.

(10) För att uppnå en hög nivå av dataskydd, säkerhet och tillförlitlighet bör denna förordning fastställa en harmoniserad ram om de gemensamma tillämpliga specifikationerna och kraven för de europeiska e-identitetsplånböckerna. Plånböckernas efterlevnad med dessa krav bör intygas av ackrediterade organ för bedömning av överensstämmelse som utses av medlemsstaterna. Certifieringen bör framför allt utgå från de relevanta europeiska ordningar för cybersäkerhetscertifiering, eller delar därav, som fastställts enligt förordning (EU) 2019/881[6], i den mån de omfattar de cybersäkerhetskrav som är tillämpliga på europeiska e-identitetsplånböcker. Att förlita sig på europeiska ordningar för cybersäkerhetscertifiering bör skapa en harmoniserad nivå av förtroende för säkerheten i de europeiska e-identitetsplånböckerna, oavsett var de utfärdas i hela unionen. Cybersäkerhetscertifieringen av de europeiska e-identitetsplånböckerna bör bygga på den roll som de nationella myndigheterna för cybersäkerhetscertifiering har när det gäller tillsyn och övervakning av att de certifikat som utfärdas av organen för bedömning av överensstämmelse inom deras jurisdiktion stämmer överens med de relevanta europeiska ordningarna för cybersäkerhet. På liknande vis bör certifieringen, beroende på vad som är lämpligt, dra nytta av standarder och tekniska specifikationer i förordning (EU) 2019/881. Sådana specifikationer får användas som mönsterdokument, enligt vad som anges i relevanta ordningar för cybersäkerhetscertifiering i enlighet med förordning (EU) 2019/881. Om inga relevanta europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med förordning (EU) 2019/881 täcker certifieringen av relevanta tjänster eller processer som bidrar till plånbokens säkerhet bör lämpliga ordningar inrättas i enlighet med avdelning III i förordning (EU) 2019/881. En gemensam och harmoniserad ordning för certifiering av europeiska e-identitetsplånböcker bör inrättas för bedömning av deras överensstämmelse med de gemensamma specifikationer och krav som föreskrivs i denna förordning, utöver dem som rör cybersäkerhet och dataskydd, särskilt sådana som omfattar funktionella och operativa aspekter. När det gäller denna certifiering bör det, för att en hög nivå av förtroende och öppenhet ska säkerställas, inrättas mekanismer och förfaranden som syftar till att främja ömsesidigt lärande och samarbete mellan medlemsstaterna om övervakningen och översynen av certifieringsorganen och de certifikat och certifieringsrapporter som de utfärdar. En sådan mekanism för ömsesidigt lärande bör inte påverka tillämpningen av förordning (EU) 2016/679 och förordning (EU) 2019/881. Certifiering av plånboken i enlighet med förordning (EU) 2016/679 är ett av flera frivilliga verktyg som kan användas för att påvisa överensstämmelse med de krav som fastställs i förordning (EU) 2016/679 såsom de tillämpas på europeiska e-identitetsplånböcker och tillhandahållandet av dessa till europeiska medborgare.

---

[6] 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.

(10a) Onboarding av medborgare och invånare avseende den europeiska e-identitetsplånboken bör underlättas genom att man förlitar sig på medel för elektronisk identifiering som utfärdats med ”hög” tillitsnivå. Medel för elektronisk identifiering som utfärdats med ”väsentlig ” tillitsnivå bör endast användas i fall där harmoniserade tekniska och operativa specifikationer med hjälp av medel för elektronisk identifiering som utfärdats med ”väsentlig ” tillitsnivå i kombination med andra kompletterande medel för kontroll av identitet möjliggör uppfyllande av kraven i denna förordning vad gäller ”hög” tillitsnivå. Sådana kompletterande medel eller åtgärder bör vara tillförlitliga och lätta att använda för användarna och skulle kunna bygga på möjligheten att använda förfaranden för onboarding på distans, kvalificerade certifikat som stöds av kvalificerade underskrifter, kvalificerade elektroniska intyg på attribut eller en kombination av dessa. För att säkerställa tillräcklig spridning av de europeiska e-identitetsplånböckerna bör harmoniserade tekniska och operativa specifikationer för onboarding av användare med hjälp av medel för elektronisk identifiering, inbegripet sådana som utfärdats med ”väsentlig ” tillitsnivå, fastställas i genomförandeakter.

(10b) Syftet med denna förordning är att förse användaren med en helt mobil, säker och användarvänlig europeisk e-identitetsplånbok. Som en övergångsåtgärd till dess att certifierade manipuleringssäkra lösningar, såsom säkerhetsdetaljer i användarnas enheter, finns tillgängliga får de europeiska e-identitetsplånböckerna förlita sig på certifierade externa säkerhetsdetaljer för skyddet av kryptografiskt material och andra känsliga uppgifter eller på anmälda nationella lösningar med ”hög” tillitsnivå för att påvisa överensstämmelse med de relevanta kraven i förordningen vad gäller plånbokens tillitsnivå. Användningen av ovannämnda övergångsåtgärd bör begränsas till fall som kräver ”hög” tillitsnivå, såsom onboarding av användaren till plånboken och autentisering till tjänster som kräver ”hög” tillitsnivå. Vid autentisering till tjänster som kräver en ”väsentlig” tillitsnivå bör de europeiska e-identitetsplånböckerna inte kräva användning av ovannämnda övergångsåtgärd. Denna förordning bör inte påverka nationella villkor för utfärdande och användning av certifierade externa säkerhetsdetaljer om denna övergångsåtgärd förlitar sig på dessa.

(11) De europeiska e-identitetsplånböckerna bör garantera högsta möjliga skydds- och säkerhetsnivå för de personuppgifter som används för autentisering, oavsett om uppgifterna lagras lokalt eller genom molnbaserade lösningar, där hänsyn tas till de olika risknivåerna. Behandling av biometriska uppgifter som en autentiseringsfaktor vid stark användarautentisering är en av de identifieringsmetoder som ger en hög konfidensnivå, framför allt i kombination med andra autentiseringsfaktorer. Eftersom biometriska uppgifter motsvarar en persons unika egenskaper är behandling av biometriska uppgifter endast tillåten inom ramen för undantagen i artikel 9.2 i förordning (EU) 2016/679 och kräver tillbörliga skyddsåtgärder, som står i rimlig proportion till de risker som denna behandling kan innebära för fysiska personers rättigheter och friheter.

(11a) De europeiska e-identitetsplånböckernas funktion bör vara transparent och medge kontrollerbar behandling av personuppgifter. För att uppnå detta uppmanas medlemsstaterna att lämna ut källkoden för programvarukomponenter i europeiska e-identitetsplånböcker som rör behandling av personuppgifter och uppgifter om juridiska personer. Offentliggörande av en sådan källkod gör det möjligt för samhället, inbegripet användare och utvecklare, att förstå hur den fungerar. Detta kan också öka användarnas förtroende för plånboksekosystemet och bidra till plånböckernas säkerhet genom att göra det möjligt för vem som helst att rapportera sårbarheter och fel i koden. Detta ger leverantörerna incitament att leverera och upprätthålla en mycket säker produkt. Dessutom och när så är lämpligt uppmanas medlemsstaterna också att göra källkoden tillgänglig genom en licens med öppen källkod. En licens med öppen källkod gör det möjligt för samhället, inklusive användare och utvecklare, att ändra och återanvända källkoden.

(12) För att säkerställa att ramen för europeisk digital identitet är öppen för innovation, teknisk utveckling och framtidssäkring bör medlemsstaterna uppmuntras att inrätta gemensamma testmiljöer där innovativa lösningar kan testas i en kontrollerad och säker miljö för att förbättra lösningarnas funktion, personuppgiftsskydd, säkerhet och interoperabilitet och därmed lägga grunden för framtida uppdateringar av tekniska referenser och rättsliga krav. Denna miljö bör även uppmuntra deltagande av europeiska små och medelstora företag, uppstartsföretag samt enskilda innovatörer och forskare.

(13) Genom förordning (EU) nr 2019/1157[7] kommer säkerheten för identitetskort att utökas med ytterligare säkerhetsfunktioner 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.

(14) 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 id-lösningar att erbjuda system för elektronisk identifiering till medlemsstaternas myndigheter för anmälning som nationella system för elektronisk identifiering enligt förordning (EU) nr 910/2014.

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

(16) Medlemsstaterna bör gynnas av nya, flexibla verktyg för att säkerställa att kraven i denna förordning och de relevanta genomförandeakterna uppfylls. Denna förordning bör ge medlemsstaterna möjlighet att använda rapporter och bedömningar, som utförts av ackrediterade organ för bedömning av överensstämmelse, såsom planeras i de certifieringssystem som ska inrättas på unionsnivå enligt förordning (EU) nr 2019/881, som stöd i deras arbete med att anpassa systemen, eller delar av dessa, till kraven i förordningen om interoperabiliteten och säkerheten hos de anmälda systemen för elektronisk identifiering.

[7] 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.

(17a) Användning av unika och beständiga identifierare som utfärdats av medlemsstaterna eller genererats av den europeiska e-identitetsplånboken, tillsammans med användning av personidentifieringsuppgifter, är avgörande för att säkerställa att användarens identitet, särskilt inom den offentliga sektorn och när detta föreskrivs i nationell lagstiftning eller unionslagstiftning, kan verifieras. Denna förordning bör säkerställa att den europeiska e-identitetsplånboken kan tillhandahålla en mekanism för att möjliggöra registermatchning, bland annat genom användning av kvalificerade elektroniska intyg på attribut, och göra det möjligt att inkludera unika och beständiga identifierare i uppsättningen av personidentifieringsuppgifter. En unik och beständig identifierare kan bestå av antingen en eller flera identifieringsuppgifter som kan vara sektorsspecifika så länge de tjänar till att unikt identifiera användaren i hela unionen. Den europeiska e-identitetsplånboken bör också tillhandahålla en mekanism som gör det möjligt att använda specifika identifierare för den förlitande parten i fall där användning av en unik och beständig identifierare krävs enligt nationell lagstiftning eller unionslagstiftning. I samtliga fall bör den mekanism som tillhandahålls för att underlätta registermatchning och användning av unika och beständiga identifierare säkerställa att användaren skyddas mot missbruk av personuppgifter i enlighet med denna förordning och tillämplig unionsrätt, särskilt förordning (EU) 2016/679, inbegripet mot risken för profilering och spårning i samband med användningen av den europeiska e-identitetsplånboken.

(17aa) Det är mycket viktigt att ta hänsyn till användarnas behov och därigenom öka efterfrågan på europeiska e-identitetsplånböcker. Det bör finnas meningsfulla användningsområden och onlinetjänster som förlitar sig på europeiska e-identitetsplånböcker. 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 onlinetjänster i alla medlemsstater. Icke-bindande riktlinjer för hur onlinetjänster som förlitar sig på europeiska e-identitetsplånböcker ska utformas, utvecklas och genomföras har potential att bli ett användbart verktyg för att uppnå detta mål. Dessa riktlinjer bör utarbetas med vederbörlig hänsyn till unionens interoperabilitetsramverk. Medlemsstaterna bör ha en ledande roll när det gäller att anta dem.

(18) I linje med direktiv (EU) 2019/882[8] bör personer med funktionsnedsättning kunna använda europeiska e-identitetsplånböcker, betrodda tjänster och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster på samma villkor som andra användare.

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

(20) Tillhandahållandet och användningen av betrodda tjänster blir allt viktigare för internationell handel och internationellt samarbete. EU:s internationella partner håller på att inrätta betrodda ramar som har inspirerats av förordning (EU) nr 910/2014. För att underlätta erkännandet av sådana tjänster och deras leverantörer kan genomförandelagstiftningen därför omfatta de villkor som måste uppfyllas av betrodda ramar i tredjeländer för att anses vara likvärdiga med den betrodda ramen för kvalificerade betrodda tjänster och leverantörer av betrodda tjänster i denna förordning, som ett komplement till det ömsesidiga erkännandet av betrodda tjänster och leverantörer av sådana som är etablerade i unionen och i tredjeländer i enlighet med artikel 218 i fördraget. Vid fastställandet av de villkor som måste uppfyllas av betrodda ramar i tredjeländer för att anses vara likvärdiga med den betrodda ramen för kvalificerade betrodda tjänster och leverantörer av betrodda tjänster i denna förordning, bör även efterlevnaden av de relevanta bestämmelserna i direktiv XXXX/XXXX, (NIS 2-direktivet) och förordning (EU) 2016/679 säkerställas, liksom användningen av förteckningar över betrodda tjänsteleverantörer som avgörande komponenter för att bygga upp förtroende.

[8] 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).

(21) Denna förordning bör bygga på unionsakter som säkerställer öppna och rättvisa marknader i den digitala sektorn. Den bygger framför allt på förordning (EU) 2022/1925, vilken inför regler för leverantörer av centrala plattformstjänster som betecknats som grindvakter, däribland förbud mot att grindvakter kräver att en företagsanvändare använder, erbjuder eller samverkar med en identifieringstjänst som erbjuds av grindvakten i samband med tjänster som företagsanvändaren erbjuder genom att använda grindvaktens centrala plattformstjänster. Enligt artikel 6.7 i förordning 2022/1925 ska grindvakter ge företagsanvändare och leverantörer av stödtjänster tillgång till och interoperabilitet med samma operativsystem eller hårdvaru- eller programvarufunktioner som är tillgängliga eller används när grindvakten tillhandahåller stödtjänster. Enligt artikel 2.15 i lagen om digitala marknader utgör identifieringstjänster en typ av kompletterande tjänst. Företagsanvändare och leverantörer av kompletterande tjänster bör därför ges tillgång till sådan maskinvaru- och programvaruinslag, t.ex. säkerhetsdetaljer i smarttelefoner, och samverka med dem med hjälp av europeiska e-identitetsplånböcker eller medlemsstaternas anmälda medel för elektronisk identifiering.

(22) 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 XXXX/XXXX (NIS2-direktivet), ska betrodda tjänster vidta lämpliga tekniska och organisatoriska åtgärder i enlighet med direktiv XXXX/XXXX (NIS2-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 direktiv XXXX/XXXX (NIS2-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 XXXXXX [NIS2] 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 XXXX/XXXX (NIS2-direktivet). Inget av kraven enligt denna förordning påverkar skyldigheten att anmäla personuppgiftsöverträdelser enligt förordning (EU) 2016/679.

(23) Vederbörlig hänsyn bör tas för att säkerställa ett effektivt samarbete mellan de myndigheter som är ansvariga för tillämpningen av NIS-direktivet och eIDA-förordningen. I de fall då tillsynsorganet enligt denna förordning skiljer sig från de behöriga myndigheter som utses enligt direktiv XXXX/XXXX [NIS2] bör dessa myndigheter bedriva ett nära och effektivt samarbete genom att utbyta relevant information för att säkerställa en effektiv tillsyn och att leverantörerna av betrodda tjänster uppfyller kraven i denna förordning och direktiv XXXX/XXXX [NIS2]. I synnerhet bör tillsynsorganen enligt denna förordning ha rätt att begära att den behöriga myndigheten enligt direktiv XXXXX/XXXX [NIS2] tillhandahåller all relevant information som behövs för att bevilja status som kvalificerad och för att utföra tillsynsåtgärder för att kontrollera att leverantörerna av betrodda tjänster uppfyller de relevanta kraven i NIS 2 eller kräva att de åtgärdar bristerna.

(24) 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 betrodda tjänster i unionen att erbjuda nya alleuropeiska 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 full säkerhet säkerställa identifieringen av adressaten, medan en hög konfidensnivå 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 tillhandahållare av kvalificerade betrodda tjänster i syfte att enkelt överföra elektroniska rekommenderade data mellan två eller flera tillhandahållare av kvalificerade betrodda tjänster och främja god sed på den inre marknaden.

(25) I de flesta fall kan medborgare och andra invånare inte utbyta information på digital väg 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 över gränserna.

(26) Det bör vara möjligt att utfärda och hantera tillförlitliga digitala attribut och bidra till att minska den administrativa bördan genom att ge medborgare och andra bosatta möjlighet att använda dem i privata och offentliga transaktioner. Medborgare och andra invånare 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.

(27) Varje enhet som samlar in, skapar och utfärdar attesterade attribut som examensbevis, intyg och personbevis bör kunna bli en tillhandahållare av elektroniska attesteringar av attribut. Förlitande parter bör använda de elektroniska intygen på attribut på samma sätt som attesteringar i pappersformat. Därför bör ett elektroniskt intyg på attribut inte förvägras rättslig verkan på grund av att det har elektronisk form eller inte uppfyller kraven för ett kvalificerat elektroniskt intyg på attribut. I detta syfte bör allmänna krav fastställas för att säkerställa att kvalificerade elektroniska intyg på attribut har samma rättsliga verkan som lagligen utfärdade attesteringar i pappersform. Sådana krav bör emellertid tillämpas utan hinder av unionslagstiftning eller nationell lagstiftning som omfattar ytterligare sektorsspecifika krav med underliggande rättsliga verkningar vad gäller formen och, i synnerhet, det gränsöverskridande erkännandet av kvalificerade elektroniska intyg på attribut i tillämpliga fall.

(28) Om de europeiska e-identitetsplånböckerna ska kunna få en stor spridning och användning måste de godtas av privata tjänsteleverantörer. Privata förlitande parter som tillhandahåller tjänster inom områdena transport, energi, bankväsende, finansiella tjänster, social trygghet, hälso- och sjukvård, dricksvatten, posttjänster, digital infrastruktur, utbildning eller telekommunikation bör godta att de europeiska e-identitetsplånböckerna används i samband med tillhandahållandet av tjänster där en säker autentisering krävs enligt den nationella lagstiftningen eller unionslagstiftningen eller genom avtalsenliga skyldigheter. För att underlätta användningen och godtagandet av den europeiska e-identitetsplånboken bör allmänt accepterade branschstandarder och specifikationer beaktas. Om mycket stora onlineplattformar, enligt definitionen i artikel 25.1 i förordning [hänvisning till DSA-förordningen], kräver att användarna autentiserar sig för att få tillgång till onlinetjänster bör dessa plattformar godta europeiska e-identitetsplånböcker på användarens frivilliga begäran. Användarna bör inte vara tvungna att använda plånboken för att få tillgång till privata tjänster, men om de vill göra det bör stora onlineplattformar godta den europeiska e-identitetsplånboken i detta syfta med iakttagande av principen om uppgiftsminimering. Med tanke på de mycket stora onlineplattformarnas räckvidd, i synnerhet när det gäller antalet mottagare av tjänsten och antalet ekonomiska transaktioner, är detta nödvändigt för att öka användarnas skydd mot bedrägerier och säkerställa en hög nivå av dataskydd. Självreglerande uppförandekoder på unionsnivå (uppförandekoder) bör utarbetas för att förbättra tillgången till och användbarheten hos medel för elektronisk identifiering, däribland de europeiska e-identitetsplånböckerna, inom denna förordnings tillämpningsområde. Uppförandekoderna bör underlätta ett brett erkännande av medel för elektronisk identifiering, däribland europeiska e-identitetsplånböcker, bland de tjänsteleverantörer som inte klassificeras som mycket stora plattformar och som förlitar sig på elektroniska id-tjänster från tredje parter för användarautentisering. De bör utarbetas inom tolv månader efter antagandet av denna förordning. Kommissionen bör bedöma bestämmelsernas effektivitet när det gäller användarnas tillgång till och användbarheten hos de europeiska e-identitetsplånböckerna 24 månader efter deras införande.

(29) 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 krävs, t.ex. för att en användare endast ska behöva lämna ut sådana uppgifter till en förlitande part som är nödvändiga för tillhandahållandet av en tjänst som begärs av en användare. De europeiska e-identitetsplånböckerna bör ha tekniska egenskaper som möjliggör ett selektivt utlämnande av attribut till förlitande parter. Sådana selektivt utlämnade attribut, inbegripet när de ursprungligen ingår i flera olika elektroniska intyg, kan därefter kombineras och presenteras för förlitande parter. Denna funktion bör vara en grundläggande inbyggd funktion som förstärker bekvämligheten och skyddet av personuppgifter, inbegripet uppgiftsminimering.

(30) Attribut som tillhandahålls av tillhandahållare av betrodda tjänster som en del av kvalificerade intyg på attribut bör verifieras mot de autentiska källorna, antingen direkt av tillhandahållaren av kvalificerade betrodda tjänster eller via särskilt utsedda mellanhänder som erkänns på nationell nivå i enlighet med nationell lagstiftning eller unionslagstiftning för ett säkert utbyte av intyg på attribut mellan tillhandahållare av identitetsuppgifter eller intyg på attribut och förlitande parter. Medlemsstaterna bör inrätta lämpliga mekanismer på nationell nivå för att säkerställa att sådana tillhandahållare av kvalificerade betrodda tjänster som utfärdar kvalificerade elektroniska intyg på attribut, på grundval av samtycke från den person till vilken intyget utfärdas, kan kontrollera äktheten hos de attribut som bygger på autentiska källor. Lämpliga mekanismer kan omfatta användningen av särskilda mellanhänder eller tekniska lösningar som i enlighet med nationell lagstiftning ger tillgång till de autentiska källorna. Genom att säkerställa tillgången till en mekanism som gör det möjligt att kontrollera attribut mot autentiska källor bör det bli lättare för tillhandahållare av kvalificerade betrodda tjänster som utfärdar kvalificerade elektroniska intyg på attribut att uppfylla sina skyldigheter enligt denna förordning. Bilaga VI innehåller en förteckning över kategorier av attribut för vilka medlemsstaterna bör säkerställa att åtgärder vidtas för att göra det möjligt för de tillhandahållare av kvalificerade betrodda tjänster som utfärdar kvalificerade elektroniska intyg på attribut att på användarens begäran på elektronisk väg kontrollera deras äkthet gentemot den relevanta autentiska källan. Medlemsstaterna bör enas om specifika attribut som omfattas av dessa kategorier.

(31) Säker elektronisk identifiering och tillhandahållande av intyg på attribut 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 förordningen om bekämpning av penningtvätt [hänvisning ska infogas när förslaget har antagits] och lämplighetskraven i lagstiftningen om investerarskydd, eller för att bidra till efterlevnaden av höga krav på kundautentisering för onlineidentifiering vid kontoinloggning och inledande av transaktioner inom betaltjänstområdet.

(31a) För att säkerställa enhetliga certifieringsmetoder i hela EU 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 medlemsstaterna från att tillåta offentliga eller privata organ som har certifierade kvalificerade anordningar för skapande av elektroniska underskrifter att tillfälligt förlänga certifieringens giltighet när en omcertifiering av samma anordning inte kan utföras inom den rättsligt fastställda tidsramen av ett annat skäl än en överträdelse eller säkerhetstillbud, och utan att det påverkar tillämplig certifieringspraxis.

(32) Tjänster för autentisering av webbplatser gör att användarna med hög grad av säkerhet kan anta att en verklig och legitim enhet står bakom webbplatsen, oavsett vilken plattform som används för att visa den. Dessa tjänster bidrar till att bygga upp förtroendet för näthandeln och till att minska antalet bedrägerier online. Användningen av tjänster för autentisering av webbplatser 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 bör det i denna förordning fastställas minimiskyldigheter vad gäller säkerhet och skadeståndsansvar för tillhandahållare av tjänster för autentisering av webbplatser. För detta ändamål bör alla leverantörer av webbläsare säkerställa stöd och interoperabilitet med kvalificerade certifikat för autentisering av webbplatser enligt förordning (EU) nr 910/2014. De bör erkänna kvalificerade certifikat för autentisering av webbplatser och göra det möjligt att visa de certifierade identitetsuppgifterna för slutanvändaren i webbläsarmiljön på grundval av de specifikationer som fastställs i enlighet med denna förordning. Erkännandet av ett kvalificerat certifikat för autentisering av webbplatser som ett kvalificerat certifikat utfärdat av en tillhandahållare av kvalificerade betrodda tjänster bör säkerställa att de identitetsuppgifter som ingår i certifikatet kan autentiseras och kontrolleras i enlighet med denna förordning. Detta bör inte påverka möjligheten för leverantörer av webbläsare att åtgärda allvarliga avvikelser i samband med säkerhetsincidenter eller integritetsförluster vad gäller enskilda certifikat, och på så sätt bidra till slutanvändarnas onlinesäkerhet. För att ytterligare skydda medborgarna och främja användningen bör medlemsstaternas offentliga myndigheter överväga att införa kvalificerade certifikat för autentisering av webbplatser på sina egna webbplatser.

(33) Många av medlemsstaterna har infört nationella krav för tjänster som tillhandahåller säker och tillförlitlig digital arkivering för att möjliggöra långsiktig lagring av elektroniska data 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. Denna ram 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. Dessa bestämmelser bör tillämpas på elektroniskt skapade dokument samt på pappersdokument som har skannats och digitaliserats. När så krävs bör dessa bestämmelser göra det möjligt att portera de bevarade elektroniska uppgifterna till olika medier eller format i syfte att förlänga deras hållbarhet och läsbarhet bortom den tekniska giltighetstiden, samtidigt som förluster och ändringar minimeras i största möjliga utsträckning. När elektroniska uppgifter som lämnas till den digitala arkiveringstjänsten innehåller en eller flera kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar bör tjänsten använda förfaranden och teknik som kan förlänga deras tillförlitlighet genom bevarandeperioden för sådana uppgifter, eventuellt genom användning av andra kvalificerade elektroniska betrodda tjänster som inrättas genom denna förordning. För att skapa bevarandebevis när elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar används bör kvalificerade elektroniska betrodda tjänster användas. I den mån elektroniska arkiveringstjänster inte harmoniseras genom denna förordning får medlemsstaterna behålla eller införa nationella bestämmelser, i enlighet med unionsrätten, som rör dessa tjänster, såsom särskilda bestämmelser som tillåter vissa undantag för tjänster som är integrerade i en organisation och som uteslutande används för organisationens ”interna arkiv”. Denna förordning bör inte göra skillnad på elektroniskt skapade dokument och fysiska dokument som har digitaliserats.

(33a) Nationella arkiv och minnesinstitutioner har, i egenskap av organisationer som arbetar med att bevara det dokumenterade arvet i allmänhetens intresse, vanligtvis mandat att bedriva sin verksamhet enligt nationell lagstiftning och tillhandahåller inte nödvändigtvis betrodda tjänster i den mening som avses i denna förordning. I den mån dessa institutioner inte tillhandahåller sådana tjänster ska denna förordning inte påverka deras verksamhet.

(34) Elektroniska liggare är en sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i deras kronologiska ordning. Syftet med elektroniska liggare är att upprätta en kronologisk sekvens av dataloggar för att förhindra att digitala tillgångar kopieras och säljs till flera mottagare. Elektroniska liggare kan till exempel användas för digitala register över ägande inom global handel, leverantörsfinansiering, digitalisering av immateriella rättigheter eller över råvaror såsom el. Tillsammans med annan teknik kan de bidra till lösningar för effektivare och omdanande offentliga tjänster såsom elektronisk röstning, gränsöverskridande samarbete mellan tullmyndigheter, gränsöverskridande samarbete mellan akademiska institutioner eller registrering av äganderätt till fastigheter i decentraliserade fastighetsregister. Kvalificerade elektroniska liggare skapar en legal presumtion för den unika och korrekta kronologiska ordningsföljden och integriteten hos dataloggarna i liggaren. De särskilda egenskaperna hos elektroniska liggare, dvs. den sekventiella kronologiska ordningsföljden för dataloggar, skiljer elektroniska liggare från andra betrodda tjänster såsom elektroniska tidsstämplingar och elektroniska tjänster för rekommenderade leveranser. Varken tidsstämpling av digitala dokument eller överföring av dem med hjälp av elektroniska tjänster för rekommenderade leveranser skulle nämligen utan ytterligare tekniska eller organisatoriska åtgärder 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 (centraliserad eller distribuerad).

(35) För att förhindra en fragmentering av den inre marknaden bör en alleuropeisk rättslig ram inrättas som möjliggör ett gränsöverskridande erkännande av betrodda tjänster för registrering av uppgifter i kvalificerade elektroniska liggare. Tillhandahållare av kvalificerade betrodda tjänster för elektroniska liggare bör få i uppdrag att säkerställa den sekventiella registreringen av uppgifter i liggaren. Denna förordning påverkar inte eventuella rättsliga skyldigheter som användare av elektroniska liggare kan behöva uppfylla enligt unionsrätten och nationell rätt. Till exempel bör användningsfall som inbegriper behandlingen av personuppgifter uppfylla kraven i förordning (EU) 2016/679. Användningsfall som inbegriper kryptotillgångar bör vara förenliga med alla tillämpliga finansiella regler, inbegripet, till exempel, direktivet om marknader för finansiella instrument[9], direktivet om betaltjänster[10], e-penningdirektivet[11], samt med framtida eventuell lagstiftning om marknader för kryptotillgångar och med regler om bekämpning av penningtvätt som kan ingå i förordningen om överföringar av medel[12] och kan kräva att leverantörer av tjänster för kryptotillgångar kontrollerar identiteten hos användare av elektroniska liggare i syfte att efterleva internationella standarder för bekämpning av penningtvätt.

---

9 Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG, EUT L 173, 12.6.2014, s. 349.

10 Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, om ändring av direktiven 2002/65/EG, 2009/110/EG och 2013/36/EU samt förordning (EU) nr 1093/2010 och om upphävande av direktiv 2007/64/EG, EUT L 337, 23.12.2015, s. 35.

11 Europaparlamentets och rådets direktiv 2009/110/EG av den 16 september 2009 om rätten att starta och driva affärsverksamhet i institut för elektroniska pengar samt om tillsyn av sådan verksamhet, om ändring av direktiven 2005/60/EG och 2006/48/EG och om upphävande av direktiv 2000/46/EG (EUT L 267, 10.10.2009, s. 7).

12 Se kommissionens förslag av den 20 juli 2021 om en omarbetning av Europaparlamentets och rådets förordning (EU) 2015/847 av den 20 maj 2015 om uppgifter som ska åtföljа överföringar av medel, COM/2021/422 final.

(36) För att undvika fragmentering och hinder på grund av varierande standarder och tekniska begränsningar, och för att säkerställa en samordnad process för att undvika att genomförandet av den framtida ramen för europeisk digital identitet äventyras, krävs ett nära och strukturerat samarbete mellan kommissionen, medlemsstaterna och den privata sektorn. För att uppnå detta mål bör medlemsstaterna samarbeta inom den ram som fastställs i kommissionens rekommendation XXX/XXXX [Verktygslåda för en samordnad strategi mot en ram för europeisk digital identitet][13] för att utarbeta en verktygslåda för en ram för europeisk digital identitet. Verktygslådan bör omfatta ett heltäckande regelverk för tekniska strukturer och referenser, en uppsättning gemensamma standarder och tekniska referenser samt en uppsättning riktlinjer och beskrivningar av bästa praxis som åtminstone omfattar alla funktionalitets- och interoperabilitetsaspekter för de europeiska e-identitetsplånböckerna, inklusive elektroniska underskrifter, och för den kvalificerade betrodda tjänst för intyg på attribut som fastställs i denna förordning. I detta sammanhang bör medlemsstaterna även nå en överenskommelse om gemensamma inslag i en affärsmodell och en avgiftsstruktur för de europeiska e-identitetsplånböckerna 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 ramen för europeisk digital identitet.

(36a) 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 denna tillhandahållare är kvalificerade.

---

13 [infoga hänvisning när förordningen har antagits]

(36b) Denna förordning bör säkerställa 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 utanför unionen, om den tillhandahåller garantier och säkerställer att tillsynsverksamhet och revisioner kan verkställas som om dessa insatser hade utförts i unionen. Om efterlevnaden av förordningen inte kan garanteras fullt ut bör tillsynsorganen kunna vidta proportionella och motiverade åtgärder, inbegripet återkallande av den tillhandahållna betrodda tjänstens kvalificerade status.

(36c) För att säkerställa rättssäkerhet när det gäller giltigheten för avancerade elektroniska underskrifter baserade på kvalificerade certifikat är det viktigt att specificera komponenterna i en avancerad elektronisk underskrift baserad på kvalificerade certifikat, vilka bör bedömas av den förlitande part som utför valideringen av den underskriften.

(36d) Tillhandahållare av betrodda tjänster bör använda krypteringsalgoritmer som återspeglar rådande bästa praxis och tillförlitliga tillämpningar av dessa algoritmer för att säkerställa säkerheten och tillförlitligheten hos sina betrodda tjänster.

(36e) I denna förordning bör det fastställas en skyldighet för kvalificerade tillhandahållare av betrodda tjänster att kontrollera identiteten på en fysisk eller juridisk person till vilken det kvalificerade certifikatet utfärdas på grundval av olika harmoniserade metoder i hela EU. En sådan metod kan omfatta användning av medel för elektronisk identifiering som uppfyller kraven på tillitsnivån ”väsentlig” i kombination med ytterligare harmoniserade distansförfaranden som säkerställer identifiering av personen med en hög konfidensnivå.

(36f) Utfärdare av europeiska e-identitetsplånböcker och utfärdare av anmälda medel för elektronisk identifiering som agerar kommersiellt eller yrkesmässigt med hjälp av centrala plattformstjänster som erbjuds av grindvakter för eller i samband med tillhandahållande av varor och tjänster till slutanvändare bör anses vara företagsanvändare i enlighet med artikel 2.21 i förordning (EU) 2022/1925. Grindvakterna bör därför vara skyldiga att kostnadsfritt säkerställa faktisk interoperabilitet med och åtkomst för interoperabilitetsändamål till samma operativsystem eller maskinvaru- eller programvarufunktioner som är tillgängliga eller används när de tillhandahåller sina egna kompletterande och stödjande tjänster och maskinvara. Detta bör göra det möjligt för utfärdare av europeiska e-identitetsplånböcker och utfärdare av anmälda medel för elektronisk identifiering att koppla upp sig genom gränssnitt eller liknande lösningar mot de respektive funktionerna lika effektivt som grindvaktens egna tjänster eller maskinvara.

(36g) För att hålla denna förordning i linje med den aktuella 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 som framkommit på den inre marknaden.

(37) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1525[14].

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

---

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

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

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

1. Artikel 1 ska ersättas med följande:

”Denna förordning syftar till att säkerställa en väl fungerande inre marknad och tillhandahålla en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster. För dessa ändamål fastställs i denna förordning

aa) de villkor på vilka medlemsstaterna ska tillhandahålla och erkänna medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett anmält system för elektronisk identifiering hos en annan medlemsstat,

ab) de villkor enligt vilka medlemsstaterna ska tillhandahålla och erkänna europeiska e-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 validering av elektroniska underskrifter, elektroniska stämplar och deras certifikat, elektronisk validering av certifikat för autentisering av webbplatser, elektroniskt bevarande av elektroniska underskrifter, elektroniska stämplar och deras certifikat, elektronisk arkivering, elektroniska intyg på attribut, förvaltning av anordningar för skapande av kvalificerade elektroniska underskrifter och kvalificerade stämplar på distans, samt elektroniska liggare.”.

2. Artikel 2 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

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

b) Punkt 3 ska ersättas med följande:

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

3. Artikel 3 ska ändras på följande sätt:

X) Punkt 1 ska ersättas med följande:

”1. *elektronisk identifiering*: den process som använder personidentifieringsuppgifter i elektronisk form som representerar enbart en fysisk eller juridisk person eller en fysisk person som företräder en fysisk eller juridisk person.”.

a) Punkt 2 ska ersättas med följande:

”2. *medel för elektronisk identifiering*: en materiell och/eller immateriell enhet, inbegripet europeiska e-identitetsplånböcker, som innehåller personidentifieringsuppgifter och som används för autentisering för en tjänst online eller, i tillämpliga fall, offline.”.

aa) Punkt 3 ska ersättas med följande:

”3. *personidentifieringsuppgifter*: en uppsättning uppgifter, som utfärdas i enlighet med unionslagstiftning eller nationell lagstiftning, som gör det möjligt att identifiera en fysisk eller juridisk person eller en fysisk person som företräder en fysisk eller juridisk person.”.

b) Punkt 4 ska ersättas med följande:

”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 fysisk eller juridisk person.”.

ba) Punkt 5 ska ersättas med följande:

”5. *autentisering*: en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen av en fysisk eller juridisk person, eller ursprunget och integriteten för uppgifter i elektronisk form.”.

bb) Följande punkt ska införas som punkt 5a:

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

c) Punkt 14 ska ersättas med följande:

”14. *certifikat för elektroniska underskrifter*: ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk underskrift till en fysisk person och bekräftar åtminstone namnet eller pseudonymen på den personen.”.

d) Punkt 16 ska ersättas med följande:

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

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

aa) validering av certifikat för elektroniska underskrifter, certifikat för elektroniska stämplar, certifikat för autentisering av webbplatser eller certifikat för tillhandahållande av andra betrodda tjänster,

b) skapande av elektroniska underskrifter eller elektroniska stämplar,

c) validering av elektroniska underskrifter eller elektroniska stämplar,

d) bevarande av elektroniska underskrifter, elektroniska stämplar, certifikat för elektroniska underskrifter eller certifikat för elektroniska stämplar,

e) förvaltning av anordningar för skapande av kvalificerade elektroniska underskrifter på distans eller anordningar för skapande av kvalificerade elektroniska stämplar på distans,

f) utfärdande av elektroniska intyg på attribut,

fa) validering av elektroniska intyg på attribut,

g) skapande av elektroniska tidsstämplingar,

ga) validering av elektroniska tidsstämplingar,

gb) tillhandahållande av elektroniska tjänster för rekommenderade leveranser,

gc) validering av data som överförs via elektroniska tjänster för rekommenderade leveranser och tillhörande bevis,

h) elektronisk arkivering av elektroniska data, eller

i) registrering av elektroniska data i en elektronisk liggare.”.

da) Punkt 18 ska ersättas med följande:

”18. *organ för bedömning av överensstämmelse*: ett organ som definieras i artikel 2.13 i förordning (EG) nr 765/2008 och som ackrediteras i enlighet med den förordningen för att utföra bedömning av överensstämmelse av en tillhandahållare av kvalificerade betrodda tjänster och de kvalificerade betrodda tjänster som den tillhandahåller, eller för att utföra certifiering av europeiska e-identitetsplånböcker eller medel för elektronisk identifiering.”.

e) Punkt 21 ska ersättas med följande:

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

f) Följande punkter ska läggas till som punkterna 23a och 23b:

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

g) Punkt 29 ska ersättas med följande:

”29. *certifikat för elektroniska stämplar*: ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk stämpel till en juridisk person och bekräftar namnet på den personen.”.

h) Punkt 41 ska ersättas med följande:

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

i) Följande punkter ska läggas till som punkterna 42–55b:

”42. *europeisk e-identitetsplånbok*: ett medel för elektronisk identifiering som gör det möjligt för användaren att lagra och hämta identitetsuppgifter, inbegripet personidentifieringsuppgifter, och elektroniska intyg på attribut som är kopplade till användarens identitet, så att dessa kan tillhandahållas åt förlitande parter på begäran och användas för autentisering, online och, när så är lämpligt offline, för en tjänst i enlighet med artikel 6a, och gör det möjligt att underteckna med kvalificerade elektroniska underskrifter och 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 intyg på attribut*: ett intyg i elektronisk form som möjliggör autentisering av attribut.

45. *kvalificerat elektroniskt intyg på attribut*: ett elektroniskt intyg på attribut som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga V.

45a. *elektroniskt intyg på attribut utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa*: elektroniska intyg på attribut utfärdade av ett offentligt organ som ansvarar för en autentisk källa eller av ett offentligt organ som utsetts av medlemsstaten för att utfärda sådana intyg på attribut på uppdrag av de offentliga organ som ansvarar för autentiska källor i enlighet med artikel 45da och som uppfyller kraven i bilaga VII.

46. *autentisk källa*: datakatalog eller system, som innehas under ansvar av ett offentligt organ eller privat enhet, som innehåller och tillhandahåller attribut för en fysisk eller juridisk person och som anses vara en primärkälla för den informationen eller erkänns som autentisk enligt unionslagstiftning eller nationell lagstiftning, inbegripet administrativa förfaranden.

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

48. *kvalificerad elektronisk arkiveringstjänst*: en elektronisk arkiveringstjänst som uppfyller de krav som fastställs i artikel 45ga.

49. *EU:s förtroendemärke för e-identitetsplånböcker*: en kontrollerbar angivelse i enkel, igenkännlig och tydlig form som visar att en europeisk e-identitetsplånbok har tillhandahållits i enlighet med denna förordning.

50. *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 överträdelse avseende en av faktorerna inte äventyrar tillförlitligheten hos de andra, och som är utformad för att skydda konfidentialiteten för autentiseringsdata.

53. *elektronisk liggare*: en sekvens av elektroniska dataloggar som säkerställer dataintegriteten och riktigheten i deras kronologiska ordning.

53a. *kvalificerad elektronisk liggare*: en elektronisk liggare som uppfyller de krav som fastställs i artikel 45i.

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

55. *registermatchning*: en process där personidentifieringsuppgifter, medel för personidentifiering, kvalificerade elektroniska intyg på attribut eller intyg på attribut utfärdade av ett offentligt organ som ansvarar för en autentisk källa eller på uppdrag av ett sådant offentligt organ matchas med eller kopplas till ett befintligt konto som tillhör samma person.

55a. *unik och beständig identifierare*: en identifierare som kan bestå av antingen enskilda eller flera nationella eller sektorsspecifika identifieringsuppgifter, som är kopplad till en enskild användare inom ett givet system och som är ihållande över tid.

55b. *datalogg*: elektroniska data som registrerats med relaterade metadata (eller attribut) som stöder behandlingen av datan.

55c. *offline-användning av europeiska e-identitetsplånböcker*: en interaktion mellan en användare och en förlitande part på en fysisk plats, där plånboken inte måste få tillträde till system på distans via elektroniska kommunikationsnätverk för att genomföra interaktionen.”.

”*Artikel 5*

Pseudonymer vid elektroniska transaktioner

Utan att det påverkar pseudonymers rättsverkan enligt nationell rätt ska användningen av pseudonymer vid elektroniska transaktioner inte vara förbjuden.”.

5. I kapitel II ska följande rubrik införas före artikel 6a:

”AVSNITT I

Den europeiska e-identitetsplånboken

7. Följande artiklar ska läggas till som artiklarna 6a, 6b, 6c och 6d:

”*Artikel 6a*

Europeiska e-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 ska varje medlemsstat säkerställa att en europeisk e-identitetsplånbok tillhandahålls inom 24 månader från det att de genomförandeakter som avses i punkt 11 och artikel 6c.4 träder i kraft.

2. Europeiska e-identitetsplånböcker ska tillhandahållas

   a) av en medlemsstat,

   b) på uppdrag av en medlemsstat, eller

   c) oberoende av en medlemsstat men med erkännande av en medlemsstat.

3. Europeiska e-identitetsplånböcker är medel för elektronisk identifiering som ska göra det möjligt för användaren att på ett sätt som är transparent och spårbart för användaren

   a) på ett säkert sätt begära, välja, kombinera, lagra, radera och visa elektroniska intyg på attribut och personidentifieringsuppgifter för förlitande parter, inbegripet för autentisering online och, när så är lämpligt, offline i samband med användning av offentliga och privata tjänster, samtidigt som det säkerställs att selektivt utlämnande av data är möjligt, och

   b) underteckna med kvalificerade elektroniska underskrifter och stämpla med kvalificerade elektroniska stämplar.

4. Europeiska e-identitetsplånböcker ska i synnerhet

a) tillhandahålla en gemensam uppsättning gränssnitt

1. för utfärdande av personidentifieringsuppgifter, kvalificerade och icke-kvalificerade elektroniska intyg på attribut eller kvalificerade och icke-kvalificerade certifikat till den europeiska e-identitetsplånboken,

2. för förlitande parter så att de kan begära personidentifieringsuppgifter och elektroniska intyg på attribut,

3. för att visa förlitande parter personidentifieringsuppgifter eller elektroniska intyg på attribut online eller, när så är lämpligt, även offline,

4. för att användaren ska kunna tillåta samverkan med den europeiska e-identitetsplånboken och visa ”EU:s förtroendemärke för e-identitetsplånböcker”,

b) inte ge någon information till tillhandahållare av betrodda tjänster för elektroniska intyg på attribut om användningen av dessa attribut efter utfärdandet,

ba) säkerställa att de förlitande parternas identitet kan valideras genom att autentiseringsmekanismer genomförs i enlighet med artikel 6b.

c) uppfylla de krav i artikel 8 med avseende på ”hög” tillitsnivå som i tillämpliga delar är tillämplig på förvaltning och användning av personidentifieringsuppgifter via plånboken, inbegripet elektronisk identifiering och autentisering,

e) säkerställa att de personidentifieringsuppgifter som avses i artikel 12.4 d på ett unikt och beständigt sätt representerar den fysiska person, juridiska person eller fysiska person som företräder den fysiska eller juridiska person som är kopplad till plånboken.

4a. Medlemsstaterna ska föreskriva förfaranden som gör det möjligt för användaren att rapportera eventuell förlust eller missbruk av sin plånbok och begära att den återkallas.

5. Medlemsstaterna ska tillhandahålla valideringsmekanismer för de europeiska e-identitetsplånböckerna

a) för att säkerställa att deras äkthet och giltighet kan kontrolleras,

d) för att göra det möjligt för användaren att autentisera förlitande parter i enlighet med artikel 6b.

6. De europeiska e-identitetsplånböckerna ska utfärdas enligt ett anmält system för elektronisk identifiering med tillitsnivån ”hög”.

6a. Utfärdandet, användningen av autentisering och återkallelsen av europeiska e-identitetsplånböcker ska vara avgiftsfri för fysiska personer.

6b. Utan att det påverkar tillämpningen av artikel 6db får medlemsstaterna, i enlighet med nationell rätt, föreskriva ytterligare funktioner för de europeiska e-identitetsplånböckerna, inbegripet interoperabilitet med befintliga nationella medel för elektronisk identifiering.

7. Användarna ska ha full kontroll över användningen av den europeiska e-identitetsplånboken och över uppgifterna i sin europeiska e-identitetsplånbok. Utfärdaren av den europeiska e-identitetsplånboken ska inte samla in sådan information om plånbokens användning som inte är nödvändig för tillhandahållandet av plånbokstjänster, den ska inte heller kombinera personidentifieringsuppgifter och några andra personuppgifter som lagras eller som rör användningen av den europeiska e-identitetsplånboken med personuppgifter från andra tjänster som erbjuds av denna utfärdare eller av tredjepartstjänster och som inte krävs för tillhandahållandet av plånbokstjänsterna, om inte användaren uttryckligen har begärt detta. Personuppgifter som rör tillhandahållandet av de europeiska e-identitetsplånböckerna ska hållas logiskt avskilda från andra data som innehas av utfärdaren av de europeiska e-identitetsplånböckerna. Om den europeiska e-identitetsplånboken tillhandahålls av privata parter, i enlighet med punkt 2 b och c, ska bestämmelserna i artikel 45f.4 gälla i tillämpliga delar.

7a. Medlemsstaterna ska utan onödigt dröjsmål ge kommissionen information om följande:

a) Det organ som ansvarar för att upprätta och underhålla förteckningen över anmälda förlitande parter som förlitar sig på de europeiska e-identitetsplånböckerna i enlighet med artikel 6b.2.

b) De organ som ansvarar för tillhandahållandet av de europeiska e-identitetsplånböckerna i enlighet med artikel 6a.1.

c) De organ som ansvarar för att säkerställa att personidentifieringsuppgifterna är kopplade till plånboken i enlighet med artikel 6a.4 e.

Underrättelsen ska också innehålla information om den mekanism som gör det möjligt att validera de personidentifieringsuppgifter som avses i artikel 12.4 och om de förlitande parternas identitet.

Kommissionen ska se till att den information som avses i denna punkt genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller förseglad form som lämpar sig för automatiserad behandling.

8. Artikel 11 ska i tillämpliga delar gälla för den europeiska e-identitetsplånboken.

9. Artikel 24.2 b, e, g och h ska gälla i tillämpliga delar för utfärdaren av de europeiska e-identitetsplånböckerna.

10. Den europeiska e-identitetsplånboken ska göras tillgänglig för personer med funktionsnedsättning i enlighet med tillgänglighetskraven i direktiv 2019/882.

11. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa tekniska och operativa specifikationer och referensstandarder för de krav som avses i punkterna 3, 4, 5 och 7a; detta ska göras genom en genomförandeakt om genomförandet av den europeiska e-identitetsplånboken. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

11a. Kommissionen ska fastställa tekniska och operativa specifikationer samt referensstandarder för att underlätta onboarding för användare vad gäller den europeiska e-identitetsplånboken med hjälp av antingen medel för elektronisk identifiering som överensstämmer med nivån ”hög” eller medel för elektronisk identifiering som överensstämmer med nivån ”väsentlig” i kombination med ytterligare förfaranden för onboarding på distans som tillsammans uppfyller kraven för ”hög” tillitsnivå. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 6b

Europeiska e-identitetsplånböcker – förlitande parter

1. Om förlitande parter som tillhandahåller privata eller offentliga tjänster avser att förlita sig på europeiska e-identitetsplånböcker som tillhandahålls i enlighet med denna förordning ska de anmäla detta till den medlemsstat där de förlitande parterna är etablerade.

1a. Anmälningsförfarandet ska vara kostnadseffektivt och proportionellt mot risk och säkerställa att förlitande parter tillhandahåller åtminstone den information som krävs för autentisering med europeiska e-identitetsplånböcker. Detta ska åtminstone omfatta den medlemsstat där de är etablerade och namnet på den förlitande parten och, i tillämpliga fall, dess registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna.

1b. Anmälningsskyldigheten ska inte påverka andra anmälnings- och registreringskrav i enlighet med unionslagstiftning eller nationell lagstiftning, såsom de som är tillämpliga på särskilda kategorier av personuppgifter, som kan kräva ytterligare tillståndskrav.

1c. Medlemsstaterna får undanta förlitande parter från anmälningskravet om unionslagstiftningen eller den nationella lagstiftningen inte föreskriver särskilda anmälnings- eller registreringskrav för tillgång till information som tillhandahålls genom den europeiska e-identitetsplånboken. De undantagna förlitande parterna kan slippa att autentisera med den europeiska e-identitetsplånboken.

1d. Förlitande parter som lämnat information i enlighet med denna artikel ska utan dröjsmål informera medlemsstaten om eventuella senare ändringar av den information som ursprungligen lämnades.

2. Förlitande parter ska säkerställa genomförandet av de autentiseringsmekanismer som avses i artikel 6a.4 ba.

3. Förlitande parter ska ansvara för genomförandet av förfarandet för autentisering av personer och validering av elektroniska intyg på attribut som härrör från europeiska e-identitetsplånböcker som erhållits genom det gemensamma gränssnittet i enlighet med artikel 6a.4 a 2.

4. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa tekniska och operativa specifikationer för de krav som avses i punkterna 1, 1a och 1d; detta ska göras genom en genomförandeakt om det genomförande av den europeiska e-identitetsplånboken som avses i artikel 6a.11. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 6c

Certifiering av europeiska e-identitetsplånböcker

1. De europeiska e-identitetsplånböckernas överensstämmelse med kraven i artikel 6a.3, 6a.4 och 6a.5, kravet på logiskt avskiljande i artikel 6a.7, och i tillämpliga fall med kraven i artikel 6a.11a, ska certifieras av organ för bedömning av överensstämmelse som ackrediterats i enlighet med artikel 60 i cybersäkerhetsakten och med de system, specifikationer, standarder och förfaranden som det hänvisas till i enlighet med punkt 4 a, 4 aa och 4 aaa, och som utsetts av medlemsstaterna. Certifieringen får inte överstiga fem år, på villkor att det görs en regelbunden sårbarhetsbedömning vartannat år. Om sårbarheter identifieras och inte åtgärdas inom tre månader ska certifieringen upphöra att gälla.

2. När det gäller efterlevnaden av dataskyddskraven i artikel 6a.7 får certifieringen i enlighet med punkt 1 kompletteras med en certifiering i enlighet med artikel 42 i förordning (EU) 2016/679.

3. Överensstämmelsen för de europeiska e-identitetsplånböckerna, eller delar av dem, med de relevanta cybersäkerhetskrav som fastställs i artikel 6a.3, 6a.4, 6a.5, 6a.7, och i tillämpliga fall 6a.11, ska certifieras av de organ för bedömning av överensstämmelse som avses i punkt 1, inom ramen för relevanta certifieringssystem för cybersäkerhet i enlighet med förordning (EU) 2019/881, i enlighet med vad som avses i punkt 4 a och 4 aa.

3a. Certifierade europeiska e-identitetsplånböcker ska inte omfattas av de krav som avses i artiklarna 7 och 9.

4. Inom sex månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, fastställa

a) en förteckning över certifieringssystem för cybersäkerhet i enlighet med förordning (EU) 2019/881 som krävs för certifiering av de europeiska e-identitetsplånböckerna i enlighet med vad som avses i punkt 3,

aa) specifikationer, förfaranden och referensstandarder för användningen av dem inom ramen för de relevanta certifieringssystem för cybersäkerhet som förtecknas i enlighet med led a,

aaa) en förteckning över specifikationer, förfaranden och referensstandarder som etablerar gemensamma certifieringskrav som inte omfattas av de relevanta certifieringssystemen för cybersäkerhet i enlighet med förordning (EU) 2019/881 i syfte att genomföra sådan certifiering som avses i punkt 1 för att visa att en europeisk e-identitetsplånbok uppfyller de krav som avses i punkt 1,

b) tekniska, förfarandemässiga, organisatoriska och operativa specifikationer för utseende av de organ för bedömning av överensstämmelse som avses i punkt 1 och, när det gäller de certifieringskrav som fastställs i enlighet med led aaa, för övervakning och översyn av de certifieringssystem och tillhörande utvärderingsmetoder som dessa organ använder och de certifikat och certifieringsrapporter som de utfärdar.

5. Medlemsstaterna ska meddela kommissionen namn och adress för de offentliga eller privata organ som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för medlemsstaterna.

6. De genomförandeakter som avses i punkt 4 ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 6d

Offentliggörande av en förteckning över certifierade europeiska e-identitetsplånböcker

1. Medlemsstaterna ska utan onödigt dröjsmål informera kommissionen om de europeiska e-identitetsplånböcker som har tillhandahållits i enlighet med artikel 6a och som certifierats av de organ som avses i artikel 6c.1. De ska också utan onödigt dröjsmål informera kommissionen om en certifiering ställs in.

2. Kommissionen ska på grundval av den information som inkommit upprätta, offentliggöra och uppdatera en maskinläsbar förteckning över certifierade europeiska e-identitetsplånböcker.

3. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa de format och förfaranden som ska gälla vid tillämpning av punkterna 1 och 2; detta ska göras genom en genomförandeakt om det genomförande av den europeiska e-identitetsplånboken som avses i artikel 6a.11. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 6da

Säkerhetsincidenter som rör de europeiska e-identitetsplånböckerna

1. I de fall då europeiska e-identitetsplånböcker som tillhandahålls i enlighet med artikel 6a eller de valideringsmekanismer som avses i artikel 6a.5 a, d eller e är föremål för incidenter eller delvis äventyras på ett sätt som påverkar deras tillförlitlighet, eller tillförlitligheten för andra europeiska e-identitetsplånböcker, ska utfärdaren av de berörda plånböckerna utan onödigt dröjsmål tillfälligt upphäva utfärdandet och användningen av den europeiska e-identitetsplånboken. Den medlemsstat där de berörda plånböckerna tillhandahölls ska utan onödigt dröjsmål informera medlemsstaterna och kommissionen om detta. Utfärdaren av de berörda plånböckerna eller medlemsstaten ska informera förlitande parter och användarna om detta.

2. När en incident eller ett äventyrande som avses i punkt 1 har åtgärdats ska utfärdaren av plånboken återinföra utfärdandet och användningen av den europeiska e-identitetsplånboken. Den medlemsstat där de berörda plånböckerna tillhandahölls ska utan onödigt dröjsmål informera medlemsstaterna och kommissionen. Utfärdaren av de berörda plånböckerna eller medlemsstaten ska utan onödigt dröjsmål informera förlitande parter och användarna.

3. När en incident eller ett äventyrande som avses i punkt 1 inte åtgärdas inom tre månader från det tillfälliga upphävandet, ska den berörda medlemsstaten dra in den berörda europeiska e-identitetsplånboken och informera övriga medlemsstater och kommissionen om detta. När det är motiverat mot bakgrund av incidentens allvar ska den berörda europeiska e-identitetsplånboken dras in utan onödigt dröjsmål.

4. Kommissionen ska utan onödigt dröjsmål offentliggöra motsvarande ändringar i den förteckning som avses i artikel 6d i Europeiska unionens officiella tidning.

5. Inom sex månader från denna förordnings ikraftträdande ska kommissionen ytterligare specificera de åtgärder som avses i punkterna 1, 2 och 3 genom en genomförandeakt om det genomförande av den europeiska e-identitetsplånboken som avses i artikel 6a.11. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 6db

Gränsöverskridande användning av europeiska e-identitetsplånböcker

1. I de fall då medlemsstaterna kräver en elektronisk identifiering med användning av medel för elektronisk identifiering och autentisering för att få åtkomst till en onlinetjänst som tillhandahålls av ett offentligt organ, ska de även godta europeiska e-identitetsplånböcker som tillhandahålls i enlighet med denna förordning för autentisering av användaren.

2. I de fall då privata förlitande parter som tillhandahåller tjänster, med undantag för mikroföretag och små företag enligt definitionen i kommissionens rekommendation 2003/361/EG, enligt nationell rätt eller unionsrätten är ålagda att använda stark användarautentisering för onlineidentifiering, eller om stark användarautentisering krävs enligt avtalsförpliktelser, däribland på områdena transport, energi, finansiella tjänster, banktjänster, social trygghet, hälsa, dricksvatten, posttjänster, digital infrastruktur, utbildning eller telekommunikation, ska dessa privata förlitande parter senast 12 månader efter det datum då den europeiska e-identitetsplånboken tillhandahölls i enlighet med artikel 6a.1 och strikt baserat på en frivillig begäran från användaren, även godta användningen av europeiska e-identitetsplånböcker som tillhandahålls i enlighet med denna förordning när det gäller de minimidata som behövs för den specifika onlinetjänst som begäran om autentisering avser.

3. I de fall då mycket stora onlineplattformar enligt definitionen i artikel 25.1 i förordning [referens till förordningen om digitala tjänster] kräver autentisering av användare för att de ska kunna få tillgång till onlinetjänster, ska dessa plattformar även godta användningen av europeiska e-identitetsplånböcker som tillhandahålls i enlighet med denna förordning när det gäller autentisering av användaren; detta ska strikt baseras på en frivillig begäran från användaren och iaktta de minimidata som behövs för den specifika onlinetjänst som begäran om autentisering avser.

4. I samarbete med medlemsstaterna ska kommissionen uppmuntra och främja utvecklingen av uppförandekoder, för att bidra till en bred tillgång till och användbarhet för europeiska e-identitetsplånböcker inom ramen för denna förordning. Dessa uppförandekoder ska underlätta ett godtagande av elektroniska medel för identifiering, inbegripet europeiska e-identitetsplånböcker, inom ramen för denna förordning, i synnerhet hos tjänsteleverantörer som förlitar sig på tredje parts elektroniska identifieringstjänster för användarautentisering. Kommissionen kommer att främja utvecklingen av sådana uppförandekoder i nära samarbete med alla berörda parter och uppmuntra tjänsteleverantörerna att slutföra utvecklingen av uppförandekoder inom tolv månader från denna förordnings ikraftträdande och genomföra dessa i praktiken inom 18 månader från denna förordnings ikraftträdande.

5. Kommissionen ska inom 24 månader från införandet av de europeiska e-identitetsplånböckerna göra en bedömning, baserad på fakta om efterfrågan på, tillgången till och användbarheten för den europeiska e-identitetsplånboken, av om ytterligare privata leverantörer av onlinetjänster ska få i uppdrag att godta användning av den europeiska e-identitetsplånboken, strikt baserat på en frivillig begäran från användaren. Bedömningskriterierna ska omfatta användarbasens omfattning, tjänsteleverantörernas gränsöverskridande närvaro, den tekniska utvecklingen, användningsmönstrens utveckling och konsumenternas efterfrågan.”.

8. Följande rubrik ska införas före artikel 7:

”AVSNITT II

SYSTEM FÖR ELEKTRONISK IDENTIFIERING”.

9. I artikel 7 ska inledningsfrasen ersättas med följande:

”I enlighet med artikel 9.1 ska medlemsstater som ännu inte har gjort detta inom 24 månader från ikraftträdandet av de genomförandeakter som avses i artiklarna 6a.11 och 6c.4 anmäla minst ett system för elektronisk identifiering som omfattar minst ett medel för identifiering med ”hög” tillitsnivå. Ett system för elektronisk identifiering ska vara berättigat till anmälan enligt artikel 9.1 om samtliga följande villkor är uppfyllda:”.

10. I artikel 9 ska punkterna 2 och 3 ersättas med följande:

”2. Kommissionen ska i *Europeiska unionens officiella tidning* offentliggöra en förteckning över de system för elektronisk identifiering som anmälts i enlighet med punkt 1 i denna artikel samt grundläggande information om dessa.

3. Kommissionen ska i *Europeiska unionens officiella tidning* offentliggöra ändringar av den förteckning som avses i punkt 2 inom en månad från mottagandet av den anmälan.”.

12. Följande artikel ska införas som artikel 11a:

”*Artikel 11a*

Registermatchning

1. När anmälda medel för elektronisk identifiering eller de europeiska e-identitetsplånböckerna används för autentisering ska medlemsstaterna när de agerar förlitande parter säkerställa registermatchning.

2. Medlemsstaterna ska vid tillhandahållandet av europeiska e-identitetsplånböcker i den minimiuppsättning personidentifieringsuppgifter som avses i artikel 12.4 d inbegripa åtminstone en unik och beständig identifierare i enlighet med unionsrätten och nationell rätt för att identifiera användaren, på deras begäran i de fall då identifiering av användaren föreskrivs enligt lagstiftning.

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

2aa. Medlemsstaterna får, i enlighet med nationell rätt, föreskriva att användaren av den europeiska e-identitetsplånboken ska kunna begära att en unik och beständig identifierare som ingår i minimiuppsättningen personidentifieringsuppgifter och som är kopplad till plånboken i enlighet med artikel 6a.4 e ersätts med en annan unik och beständig identifierare som utfärdats av medlemsstaten.

3. Inom sex månader från denna förordnings ikraftträdande ska kommissionen ytterligare specificera de åtgärder som avses i punkt 1 genom en genomförandeakt. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

3a. Inom sex månader från denna förordnings ikraftträdande ska kommissionen ange de åtgärder som avses i punkterna 2 och 2aa genom en genomförandeakt. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

13. Artikel 12 ska ändras på följande sätt:

Samarbete och interoperabilitet

a) I punkt 3 ska led d utgå.

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

”d) Hänvisning till en minimiuppsättning personidentifieringsuppgifter som krävs för att på ett unikt och beständigt sätt representera en fysisk person, juridisk person eller en fysisk person som företräder fysiska eller juridiska personer.”.

ba) I punkt 5 ska följande led införas som led c:

”c) En liknande strategi för onlinetjänster som godtar användning av europeiska e-identitetsplånböcker som tillhandahålls i enlighet med denna förordning.”.

c) I punkt 6 ska led a ersättas med följande:

”a) Utbyte av information, erfarenheter och god praxis när det gäller system för elektronisk identifiering och särskilt i fråga om tekniska krav avseende interoperabilitet, registermatchning och tillitsnivåer.”.

ca) I punkt 6 ska följande led införas som led e:

”e) Utbyte av information, erfarenheter och god praxis samt utfärdande av riktlinjer för hur onlinetjänster kan utformas, utvecklas och genomföras i syfte att förlita sig på de europeiska digitala plånböckerna.”.

14. Följande artiklar ska införas som artiklarna 12a och 12b:

”*Artikel 12a*

Certifiering av system för elektronisk identifiering

1. Överensstämmelse för system för elektronisk identifiering som ska anmälas med de krav som fastställs i denna förordning ska certifieras för att visa att sådana system eller delar av dem uppfyller kraven i artikel 8.2 vad gäller tillitsnivåerna för system för elektronisk identifiering inom ramen för ett relevant certifieringssystem för cybersäkerhet i enlighet med förordning (EU) 2019/881 eller delar därav, i den mån cybersäkerhetscertifikatet eller delar därav omfattar de krav som anges i artikel 8.2 avseende tillitsnivåerna för system för elektronisk identifiering. Certifieringen får inte överstiga fem år, på villkor att det görs en regelbunden sårbarhetsbedömning vartannat år. Om sårbarheter identifieras och inte åtgärdas inom tre månader ska certifieringen upphöra att gälla.

   Certifieringen ska utföras av ackrediterade offentliga eller privata organ för bedömning av överensstämmelse som utsetts av medlemsstaterna och i enlighet med förordning (EG) nr 765/2008.

2. Sakkunnighetsbedömning av system för elektronisk identifiering enligt artikel 12.6 c ska inte tillämpas på de system för elektronisk identifiering, eller de delar av sådana system, som certifierats i enlighet med punkt 1.

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

3. Medlemsstaterna ska underrätta kommissionen om namnet på och adressen till det offentliga eller privata organ som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för medlemsstaterna.”.

”*Artikel 12b*

Tillgång till maskinvaru- och programvarufunktioner

Utfärdare av europeiska e-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 förordning (EU) 2022/1925 för eller i samband med tillhandahållande av tjänster som gäller europeiska e-identitetsplånböcker och medel för elektronisk identifiering till slutanvändare är företagsanvändare i enlighet med artikel 2.21 i förordning (EU) 2022/1925.”.

17. Artikel 13.1 ska ersättas med följande:

”1. Trots punkt 2 i denna artikel 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.”.

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 ska anses föreligga såvida inte en kvalificerad tillhandahållare 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.

18. Artikel 14 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 den internationella organisationen är erkända enligt ett genomförandebeslut eller ett avtal som ingåtts mellan unionen och tredjelandet eller en internationell organisation i enlighet med artikel 218 i EUF-fördraget.

2. De genomförandebeslut och 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 tredjelandet eller den internationella organisationen och av de betrodda tjänster som de tillhandahåller. Tredjeländer och internationella organisationer ska särskilt upprätta, underhålla och offentliggöra en förseglad förteckning över erkända tillhandahållare av betrodda tjänster.

   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 den internationella organisation med vilket eller vilken avtalet ingås.

3. De genomförandebeslut som avses i punkt 1 ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

19. Artikel 15 ska ersättas med följande:

”*Artikel 15*

Tillgänglighet för personer med funktionsnedsättning

Tillhandahållandet av betrodda tjänster och slutanvändarprodukter som används för tillhandahållandet av dessa tjänster ska göras tillgängliga för personer med funktionsnedsättning i enlighet med tillgänglighetskraven i direktiv 2019/882 om tillgänglighetskrav för produkter och tjänster.”.

20. Artikel 17 ska ändras på följande sätt:

a) Punkt 4 ska ändras på följande sätt:

1. Led c i punkt 4 ska ersättas med följande:

”c) Tillsynsorganet ska via den berörda medlemsstatens gemensamma kontaktpunkt, som utsetts i enlighet med direktiv (EU) XXXX/XXXX [NIS2], informera den berörda medlemsstatens berörda nationella behöriga myndigheter, som utsetts i enlighet med direktiv (EU) XXXX/XXXX (NIS2) och de tillsynsorgan som utsetts i enlighet med artikel 17 i denna förordning i de övriga berörda medlemsstaterna, om alla säkerhetsincidenter eller integritetsförluster man får kännedom om vid utförandet av sina uppgifter, om den betydande säkerhetsincidenten eller integritetsförlusten rör andra medlemsstater. Det underrättade tillsynsorganet ska informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör det, om den slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten ligger i allmänhetens intresse.”.

2. Led f ska ersättas med följande:

”f) Samarbete med behöriga tillsynsmyndigheter som inrättats enligt förordning (EU) 2016/679, i synnerhet genom att utan onödigt dröjsmål informera dem vid misstänkta överträdelser av dataskyddsreglerna, och om misstänkta säkerhetsincidenter som gäller personuppgifter.”.

b) Punkt 6 ska ersättas med följande:

”6. Senast den 31 mars varje år ska varje tillsynsorgan till kommissionen överlämna en rapport om det föregående kalenderårets huvudverksamhet.”.

c) Punkt 8 ska ersättas med följande:

”8. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen anta riktlinjer för tillsynsorganens utövande av de uppgifter som avses i punkt 4 och genom genomförandeakter som antagits i enlighet med det granskningsförfarande som avses i artikel 48.2 fastställa formaten och förfarandena för den rapport som avses i punkt 6.”

21. Artikel 18 ska ändras på följande sätt:

a) Rubriken till artikel 18 ska ersättas med följande:

”Ömsesidigt bistånd och samarbete”.

b) Punkt 1 ska ersättas med följande:

”1. Tillsynsorgan ska samarbeta med sikte på att utbyta god praxis och information om tillhandahållandet av betrodda tjänster.”.

c) Följande punkter ska läggas till som punkterna 4 och 5:

”4. Tillsynsorgan och nationella behöriga myndigheter enligt Europaparlamentets och rådets direktiv (EU) XXXX/XXXX [NIS2] ska samarbeta och bistå varandra för att säkerställa att tillhandahållare av betrodda tjänster uppfyller de krav som fastställs i denna förordning och i direktiv (EU) XXXX/XXXX [NIS2]. Tillsynsorganen ska begära att de nationella behöriga myndigheterna enligt direktiv XXXX/XXXX [NIS2] utför tillsynsåtgärder för att kontrollera att tillhandahållare av betrodda tjänster uppfyller kraven enligt direktiv XXXX/XXXX (NIS2), kräver att tillhandahållare av betrodda tjänster åtgärdar eventuella brister i uppfyllandet av dessa krav, i rätt tid tillhandahåller resultaten av all tillsynsverksamhet som rör tillhandahållare av betrodda tjänster och underrättar tillsynsorganen om relevanta incidenter som anmälts i enlighet med direktiv XXXX/XXXX [NIS2].

5. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter införa de nödvändiga förfarandemässiga arrangemangen för att främja samarbete mellan de tillsynsmyndigheter som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

21a. Följande artikel ska införas som 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; trots bestämmelserna i artikel 18 i direktiv EU XXXX/XXX [NIS2] ska dessa åtgärder innefatta åtminstone

i) åtgärder avseende registrering och onboarding-förfaranden för en tjänst,

ii) åtgärder avseende förfarandemässiga eller administrativa kontroller,

iii) åtgärder avseende förvaltning och genomförande av tjänster,

b) utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter upptäckt, anmäla till tillsynsorganet, de identifierbara berörda personerna, allmänheten om det är av allmänt intresse och, om tillämpligt, andra relevanta behöriga organ, alla överträdelser eller störningar som rör genomförandet av de åtgärder som avses i led a i), ii) och iii) och som har en betydande inverkan på den betrodda tjänst som tillhandahålls eller de personuppgifter som lagras där.

2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter specificera de tekniska egenskaperna hos de åtgärder som avses i punkt 1 a. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”

22. 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 18 i direktiv (EU) XXXX/XXXX [NIS2]. De kvalificerade tillhandahållarna av betrodda tjänster ska lämna rapporten från bedömningen av överensstämmelse till tillsynsorganet inom tre arbetsdagar från mottagandet.”.

aa) Följande punkt ska införas:

”1a. Medlemsstaterna får föreskriva att kvalificerade tillhandahållare av betrodda tjänster i förväg ska informera tillsynsorganet om planerade granskningar och på begäran tillåta tillsynsorganet att delta som observatör.”

b) I punkt 2 ska den sista meningen ersättas med följande:

”Vid misstänkta överträdelser av reglerna om skydd för personuppgifter ska tillsynsorganet utan onödigt dröjsmål informera de behöriga tillsynsmyndigheterna enligt förordning (EU) 2016/679.”.

c) Punkterna 3 och 4 ska ersättas med följande:

”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 inom den tidsfrist som fastställts av tillsynsorganet, om tillämpligt, får tillsynsorganet, med beaktande av i synnerhet denna underlåtenhets omfattning, varaktighet och konsekvenser, dra in tillhandahållarens status som kvalificerad tillhandahållare, eller den berörda tillhandahållna tjänstens status som kvalificerad tjänst.

3a. Om tillsynsorganet informeras av de nationella behöriga myndigheterna enligt direktiv (EU) XXXX/XXXX [NIS 2] om att den kvalificerade tillhandahållaren av betrodda tjänster inte uppfyller något av kraven i artikel 18 i direktiv (EU) XXXX/XXXX [NIS 2] får tillsynsorganet, med särskilt beaktande av varaktigheten för och omfattningen och konsekvenserna av detta misslyckande, dra in den berörda tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad.

3b. Om tillsynsorganet informeras av tillsynsmyndigheterna enligt förordning (EU) 2016/679 om att den kvalificerade tillhandahållaren av betrodda tjänster inte uppfyller något av kraven i förordning (EU) 2016/679 får tillsynsorganet, med särskilt beaktande av varaktigheten för och omfattningen och konsekvenserna av detta misslyckande, dra in den berörda tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad.

3c. Tillsynsorganet ska informera den kvalificerade tillhandahållaren av betrodda tjänster om indragandet av dess eller den berörda tjänstens status som kvalificerad. Tillsynsorganet ska informera det organ som avses i artikel 22.3 för uppdatering av den förteckning över betrodda tjänsteleverantörer som avses i artikel 22.1 och den nationella behöriga myndighet som avses i direktiv XXXX [NIS2].

4. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, fastställa tekniska specifikationer och referensnummer för följande standarder:

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

b) Granskningsregler för hur organ för bedömning av överensstämmelse ska göra sin bedömning av överensstämmelse 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.”.

23. Artikel 21 ska ändras på följande sätt:

”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 18 i direktiv (EU) XXXX/XXXX [NIS2] är uppfyllda.”.

a) Punkt 2 ska ersättas med följande:

”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 18 i direktiv XXXX [NIS2] ska tillsynsorganet begära att de behöriga myndigheter som avses i direktiv XXXX [NIS2] utför tillsynsverksamhet i det avseendet och tillhandahåller information om resultatet utan onödigt dröjsmål och senast två månader efter mottagandet av denna begäran från de behöriga myndigheter som avses i direktiv XXXX [NIS2]. Om kontrollen inte har slutförts inom två månader från anmälan, ska de behöriga myndigheter som avses i direktiv XXXX [NIS2] 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.

I de fall då 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. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa formaten och förfarandena för anmälan och kontroll enligt punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

25. 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 intyg på attribut, kontrollera identiteten och, i förekommande fall, eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet eller det kvalificerade elektroniska intyget på attribut ska utfärdas.

Den information som avses i första stycket ska kontrolleras av den kvalificerade tillhandahållaren av betrodda tjänster, antingen direkt eller via tredje part, på något av följande sätt:

a) Genom den europeiska e-identitetsplånboken eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 vad gäller tillitsnivån ”hög”.

b) Genom ett kvalificerat elektroniskt intyg på attribut eller 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 konfidensnivå, vars överensstämmelse ska ha bekräftats av ett organ för bedömning av överensstämmelse.

d) Genom fysisk närvaro av den fysiska personen eller den juridiska personens behöriga ombud inom ramen för lämpliga förfaranden och i enlighet med nationell rätt.”.

b) Följande punkt ska införas som punkt 1a:

”1a. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa minimikrav vad gäller tekniska specifikationer, standarder och förfaranden med avseende på kontrollen av identitet och attribut i enlighet med punkt 1 c. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

c) Punkt 2 ska ändras på följande sätt:

0. Led a ska ändras på följande sätt:

”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. Tillsynsorganet får begära ytterligare information eller resultatet av en bedömning av överensstämmelse innan det beviljar tillstånd 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.”

1. Leden d och e ska ersättas med följande:

”d) innan den ingår ett avtalsförhållande, på ett tydligt och uttömmande och lättillgängligt sätt, på en allmänt tillgänglig plats och individuellt, informera 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 krypteringsalgoritmer, nyckellängder och hashfunktioner i systemen, produkterna och i de processer som stöds av dessa.”.

2. Följande led ska införas som leden fa och fb:

”fa) 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; trots bestämmelserna i artikel 18 i direktiv EU XXXX/XXX [NIS2] ska dessa åtgärder innefatta åtminstone

i) åtgärder avseende registrering och onboarding-förfaranden för en tjänst,

ii) åtgärder avseende förfarandemässiga eller administrativa kontroller,

iii) åtgärder avseende förvaltning och genomförande av tjänster,”,

”fb) utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter incidenten, 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 överträdelser eller störningar som rör genomförandet av de åtgärder som avses i led a i), ii) och iii) och som har en betydande inverkan på den betrodda tjänst som tillhandahålls eller de personuppgifter som lagras där.”

3. Leden g och h 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) så lång tid som är nödvändig efter det att den kvalificerade tillhandahållaren av betrodda uppgifter 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.”.

4. Punkt j ska utgå.

d) Följande punkt ska införas som punkt 4a:

”4a. Punkterna 3 och 4 ska i enlighet med detta tillämpas vid återkallelse av kvalificerade intyg på attribut.”.

e) Punkt 5 ska ersättas med följande:

”5. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer, förfaranden och referensnummer för standarder för de krav som avses i punkt 2. Överensstämmelse med kraven i denna artikel ska förutsättas när dessa tekniska specifikationer, förfaranden och standarder uppfylls. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

f) Följande punkt ska införas som punkt 6:

”6. Kommissionen ska ges befogenhet att anta genomförandeakter med angivande av de tekniska egenskaperna hos de åtgärder som avses i punkt 2 fa.”.

25a. Artikel 26 ska ändras på följande sätt:

2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, fastställa tekniska specifikationer och referensnummer för standarder för avancerade elektroniska underskrifter. Överensstämmelse med kraven för avancerade elektroniska underskrifter ska förutsättas när en avancerad elektronisk signatur uppfyller dessa specifikationer och standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

25b. Artikel 27 ska ändras på följande sätt:

Artikel 4 ska utgå.

26. Artikel 28.6 ska ersättas med följande:

”6. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer och referensnummer för standarder för kvalificerade certifikat för elektroniska underskrifter. Överensstämmelse med kraven i bilaga I ska förutsättas när ett kvalificerat certifikat för elektroniska underskrifter uppfyller dessa specifikationer och standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

27 I artikel 29 ska följande punkt läggas till som punkt 1a:

”1a. Generering och hantering av data för skapande av elektroniska underskrifter för undertecknarens räkning eller kopiering av sådana data för skapande av underskrifter för backup-ändamål får endast utföras av en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller en kvalificerad betrodd tjänst för förvaltningen av en anordning för skapande av kvalificerade elektroniska underskrifter på distans.”.

28 Följande artikel ska införas som artikel 29a:

”*Artikel 29a*

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

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

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

b) trots punkt 1 d i bilaga II, får kopiera uppgifterna för skapande av elektroniska underskrifter endast för backup-ändamål och förutsatt att följande krav uppfylls, nämligen

i) att säkerheten för de kopierade datauppsättningarna måste vara på samma nivå som för de ursprungliga datauppsättningarna,

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

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

2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, fastställa tekniska specifikationer och referensnummer för de standarder som avses i punkt 1.”.

29. I artikel 30 ska följande punkt införas som punkt 3a:

”3a. Giltigheten för den certifiering som avses i punkt 1 ska inte överstiga 5 år, villkorat med en regelbunden sårbarhetsanalys vartannat år. Om sårbarheter identifieras och inte åtgärdas ska certifieringen upphöra att gälla.”.

30. Artikel 31.3 ska ersättas med följande:

”3. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa de format och förfaranden som ska tillämpas inom ramen för punkt 1. 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 ska förutsättas när valideringen av kvalificerade elektroniska underskrifter uppfyller de specifikationer och standarder som avses i punkt 3.”.

b) Punkt 3 ska ersättas med följande:

”3. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, föreskriva specifikationer och referensnummer för standarder för validering av kvalificerade elektroniska underskrifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

31a. Följande artikel ska införas som artikel 32a:

Krav för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat

1. Genom valideringsförfarandet för en avancerad elektronisk underskrift baserad på kvalificerade certifikat ska giltigheten för den avancerade elektroniska underskriften baserad på kvalificerade 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.

Överensstämmelse med kraven i första stycket ska förutsättas när valideringen av avancerade elektroniska underskrifter baserade på kvalificerade certifikat uppfyller de specifikationer och standarder som avses i punkt 3.

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. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, föreskriva specifikationer och referensnummer för standarder för validering av avancerade elektroniska underskrifter baserade på kvalificerade certifikat. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

31b. Artikel 33 ska ändras på följande sätt:

”1. En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som”.

”2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer och referensnummer för standarder för den kvalificerade valideringstjänst som avses i punkt 1. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringstjänsten för kvalificerade elektroniska underskrifter uppfyller dessa specifikationer och standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

32. Artikel 34 ska ersättas med följande:

”*Artikel 34*

Kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter

1. En kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet.

2. Överensstämmelse med kraven i punkt 1 ska förutsättas när arrangemangen för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter uppfyller de specifikationer och standarder som avses i punkt 3.

3. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer och referensnummer för standarder för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

32a. I artikel 36 ska en ny punkt 2 läggas till:

2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, fastställa tekniska specifikationer och referensnummer för standarder för avancerade elektroniska stämplar.

Överensstämmelse med kraven för avancerade elektroniska stämplar ska förutsättas när en avancerad elektronisk stämpel uppfyller dessa specifikationer och standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

33. Artikel 37 ska ändras på följande sätt:

Artikel 4 ska utgå.

34. Artikel 38 ska ändras på följande sätt:

a) Punkt 1 ska ersättas med följande:

”1. Kvalificerade certifikat för elektroniska stämplar ska uppfylla de krav som fastställs i bilaga III. Överensstämmelse med kraven i bilaga III ska förutsättas när ett kvalificerat certifikat för elektroniska stämplar uppfyller de specifikationer och standarder som avses i punkt 6.”.

b) Punkt 6 ska ersättas med följande:

”6. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer och referensnummer för standarder för kvalificerade certifikat för elektroniska stämplar. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

35. Följande artikel ska införas som artikel 39a:

”*Artikel 39a*

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

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

35a. Följande artikel ska införas som artikel 40a:

”*Artikel 40a*

Krav för validering av avancerade elektroniska stämplar baserade på kvalificerade certifikat

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

36. Artikel 42 ska ändras på följande sätt:

a) Följande punkt ska införas som punkt 1a:

”1a. Överensstämmelse med kraven i punkt 1 ska förutsättas när bindningen av datum och tidpunkt till uppgifter och den korrekta tidskällan uppfyller de specifikationer och standarder som avses i punkt 2.”.

b) Punkt 2 ska ersättas med följande:

”2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer och referensnummer för standarder för bindningen av datum och tidpunkt till uppgifter och för korrekta tidskällor. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

36a. I artikel 43 ska en ny punkt 3 läggas till:

2a. En kvalificerad elektronisk tjänst för rekommenderade leveranser i en medlemsstat ska erkännas som en kvalificerad elektronisk tjänst för rekommenderade leveranser i alla andra medlemsstater.”.

37. Artikel 44 ska ändras på följande sätt:

a) Följande punkt ska införas som punkt 1a:

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

b) Punkt 2 ska ersättas med följande:

”2. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter fastställa tekniska specifikationer och referensnummer för standarder 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 läggas till som punkterna 3 och 4:

”3. Tillhandahållare av kvalificerade elektroniska tjänster för rekommenderade leveranser får komma överens om interoperabiliteten mellan de kvalificerade elektroniska tjänster för rekommenderade leveranser som de tillhandahåller. Ett sådant interoperabilitetsramverk ska uppfylla de krav som fastställs i punkt 1. Överensstämmelsen ska bekräftas av ett organ för bedömning av överensstämmelse.”.

”4. Kommissionen får genom en genomförandeakt fastställa tekniska specifikationer och referensnummer för standarder för att underlätta överföringen av uppgifter mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster. Standarderna ska, vad gäller tekniska specifikationer och innehåll, vara kostnadseffektiva och proportionerliga. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

38. 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 överensstämmelsen med kraven i bilaga IV ska utföras i enlighet med de specifikationer och standarder som avses i punkt 4.

2. Kvalificerade certifikat för autentisering av webbplatser enligt punkt 1 ska kännas igen av webbläsare. Webbläsare ska för detta ändamål säkerställa att identitetsuppgifter som tillhandahålls, oavsett använd metod, visas på ett användarvänligt sätt. Webbläsarna ska säkerställa stöd och interoperabilitet med kvalificerade certifikat för autentisering av webbplatser enligt punkt 1, med undantag för företag som anses vara mikroföretag eller små företag i enlighet med kommissionens rekommendation 2003/361/EG under de första fem år som de är verksamma som leverantörer av webbläsartjänster.

4. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen genom genomförandeakter tillhandahålla specifikationer och referensnummer för standarder för de kvalificerade certifikat för autentisering av webbplatser som avses i punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

39. Följande avsnitt ska införas efter artikel 45 som avsnitten 9, 10 och 11:

”AVSNITT 9

ELEKTRONISKA INTYG PÅ ATTRIBUT

Artikel 45a

Rättslig verkan av elektroniska intyg på attribut

1. Ett elektroniskt intyg på attribut 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 intyg på attribut.

2. Ett kvalificerat elektroniskt intyg på attribut och intyg på attribut 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 kvalificerat elektroniskt intyg på attribut som utfärdats i en medlemsstat ska erkännas som ett kvalificerat elektroniskt intyg på attribut i alla andra medlemsstater.

4. Ett intyg på attribut utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska erkännas som ett intyg på attribut utfärdat av eller på uppdrag av en offentlig myndighet som ansvarar för en autentisk källa i alla medlemsstater.

Artikel 45b

Elektroniska intyg på attribut i offentliga tjänster

I de fall då det enligt nationell rätt krävs en elektronisk identifiering med användning av medel för elektronisk identifiering och autentisering för åtkomst till en onlinetjänst som tillhandahålls av ett offentligt organ, ska inte personidentifieringsuppgifterna i det elektroniska intyget på attribut 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 intyg på attribut från andra medlemsstater också godtas.

Artikel 45c

Krav för kvalificerade elektroniska intyg på attribut

1. Kvalificerade elektroniska intyg på attribut ska uppfylla de krav som fastställs i bilaga V.

1a. Bedömningen av överensstämmelsen med kraven i bilaga V ska utföras i enlighet med de specifikationer och standarder som avses i punkt 4.

2. Om ett kvalificerat elektroniskt intyg på attribut 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 återgå.

3. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa referensnummer för standarder för kvalificerade elektroniska intyg på attribut;

4. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa tekniska specifikationer och referensnummer för standarder för kvalificerade elektroniska intyg på attribut; detta ska göras genom en genomförandeakt om det genomförande av den europeiska e-identitetsplånboken som avses i artikel 6a.11.

Artikel 45d

Kontroll av attribut mot autentiska källor

1. Medlemsstaterna ska inom 24 månader från ikraftträdandet av de genomförandeakter som avses i artiklarna 6a.11 och 6c.4, åtminstone för de attribut som förtecknas i bilaga VI och när dessa attribut baseras på autentiska källor inom offentliga sektorn, säkerställa att åtgärder vidtas som gör det möjligt för kvalificerade tillhandahållare av elektroniska intyg på attribut att, på användarens begäran, på elektronisk väg kontrollera dessa attributet i enlighet med nationell rätt eller unionsrätten.

2. Inom sex månader från denna förordnings ikraftträdande ska kommissionen, med beaktande av relevanta internationella standarder, fastställa minimikrav för tekniska specifikationer, standarder och förfaranden med avseende på katalogen med attribut och system för intyg på attribut och kontrollförfaranden för kvalificerade elektroniska intyg på attribut; detta ska göras genom en genomförandeakt om det genomförande av de europeiska e-identitetsplånböckerna som avses i artikel 6a.11.

Artikel 45da

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

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

   a) De krav som anges i bilaga VII.

b) Det kvalificerade certifikat som stöder den kvalificerade elektroniska underskrift eller den kvalificerade elektroniska stämpel från det offentliga organ som avses i artikel 3.45a och som identifierats som den utfärdare som avses i led b i bilaga VII ska innehålla en särskild uppsättning certifierade attribut i en form som lämpar sig för automatiserad behandling

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

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

iii) som identifierar den nationella lagstiftning eller unionslagstiftning som avses i led i.

2. Den medlemsstat där de offentliga organ som avses i artikel 3.45a är etablerade ska säkerställa att de offentliga organ som utfärdar elektroniska intyg på attribut uppfyller likvärdig tillförlitlighetsnivå som kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 24.

2a. Medlemsstaterna ska underrätta kommissionen om de offentliga organ som avses i artikel 3.45a. Denna anmälan ska innehålla en rapport om en 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 se till att den förteckning över offentliga organ som avses i avses i artikel 3.45a genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller förseglad form som lämpar sig för automatiserad behandling.

3. Om ett elektroniskt intyg på attribut som utfärdats 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. Efter återkallandet ska det elektroniska intygets återkallade status inte återställas.

4. Ett elektroniskt intyg på attribut som utfärdats av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska anses uppfylla kraven i punkt 1 i denna artikel om det uppfyller de standarder som avses i punkt 5.

5. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa tekniska specifikationer och referensnummer för standarder för elektroniska intyg på attribut utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa; detta ska göras genom en genomförandeakt om det genomförande av den europeiska e-identitetsplånboken som avses i artikel 6a.11.

5a. Inom sex månader från denna förordnings ikraftträdande ska kommissionen fastställa formaten, förfarandena, specifikationerna och standarderna för tillämpningen av punkt 2a; detta ska göras genom en genomförandeakt om det genomförande av den europeiska e-identitetsplånboken som avses i artikel 6a.11.

6. Offentliga organ som avses i artikel 3.45a som utfärdar elektroniska intyg på attribut ska tillhandahålla ett gränssnitt med de europeiska e-identitetsplånböcker som utfärdas i enlighet med artikel 6a.

Artikel 45e

Utfärdande av elektroniska intyg på attribut till de europeiska e-identitetsplånböckerna

Tillhandahållare av kvalificerade elektroniska intyg på attribut ska tillhandahålla ett gränssnitt med de europeiska e-identitetsplånböcker som tillhandahålls i enlighet med artikel 6a.

Artikel 45f

Ytterligare regler för tjänster för tillhandahållande av elektroniska intyg på attribut

1. Tillhandahållare av kvalificerade och icke-kvalificerade tjänster för elektroniska intyg på attribut 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 tjänster för tillhandahållande av elektroniska intyg på attribut ska hållas logiskt åtskilda från andra data som innehas av tillhandahållaren av elektroniska intyg på attribut.

4. Tillhandahållare av tjänster för kvalificerade elektroniska intyg på attribut ska genomföra funktionell åtskillnad för tillhandahållande av sådana tjänster.

AVSNITT 10

ELEKTRONISKA ARKIVERINGSTJÄNSTER

Artikel 45g

Rättslig verkan av en elektronisk arkiveringstjänst

1. Elektroniska data som lagras 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 lagrade genom en kvalificerad elektronisk arkiveringstjänst.

2. Elektroniska data som lagras genom en kvalificerad elektronisk arkiveringstjänst ska omfattas av en presumtion om deras integritet och ursprung under hela bevarandeperioden av den kvalificerade tillhandahållaren av betrodda tjänster.

3. En kvalificerad elektronisk arkiveringstjänst i en medlemsstat ska erkännas som en kvalificerad elektronisk arkiveringstjänst i alla andra medlemsstater.

Artikel 45ga

Krav för 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 förlänga hållbarheten och läsbarheten för elektroniska data efter den tekniska giltighetstiden och åtminstone under hela den rättsliga eller avtalsenliga bevarandeperioden, samtidigt som deras integritet och ursprung bibehålls.

c) De ska säkerställa att elektroniska data 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 data som hämtats från ett kvalificerat elektroniskt arkiv omfattas av presumtionen om uppgifternas integritet från början av bevarandeperioden till tidpunkten för hämtningen. Denna rapport 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. Inom tolv månader från denna förordnings ikraftträdande ska kommissionen, genom genomförandeakter, fastställa tekniska specifikationer och referensnummer för standarder för kvalificerade elektroniska arkiveringstjänster. Överensstämmelse med kraven för kvalificerade elektroniska arkiveringstjänster ska förutsättas när en kvalificerad elektronisk arkiveringstjänst uppfyller dessa specifikationer och standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 11

ELEKTRONISKA LIGGARE

Artikel 45h

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 för 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.

3. En kvalificerad elektronisk liggare i en medlemsstat ska erkännas som en kvalificerad elektronisk liggare i alla andra medlemsstater.

Artikel 45i

Krav för kvalificerade elektroniska liggare

1. Kvalificerade elektroniska liggare ska uppfylla följande krav:

   a) De ska skapas 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. Överensstämmelse med kraven i punkt 1 ska förutsättas när en elektronisk liggare uppfyller de specifikationer och standarder som avses i punkt 3.

3. Kommissionen ska genom genomförandeakter fastställa tekniska specifikationer och referensnummer till standarder för skapande och drift av en kvalificerad elektronisk liggare. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.”.

40. Följande artikel ska införas som artikel 48a:

”*Artikel 48a*

Rapporteringskrav

1. Medlemsstaterna ska säkerställa att det samlas in statistik om hur de europeiska e-identitetsplånböckerna fungerar när de har börjat tillhandahållas på deras territorium.

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 e-identitetsplånbok.

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

c) Sammanfattande rapport med uppgifter om incidenter som hindrar användningen av den europeiska e-identitetsplånboken.

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.”.

41. Artikel 49 ska ersättas med följande:

”*Artikel 49*

Översyn

1. Kommissionen ska göra en översyn över denna förordnings tillämpning och rapportera resultaten till Europaparlamentet och rådet inom 36 månader från dess ikraftträdande. Kommissionen ska särskilt utvärdera tillämpningsområdet för artikel 6 och 6db samt huruvida det är lämpligt att ändra denna förordnings tillämpningsområde eller dess särskilda bestämmelser, med beaktande av den erfarenhet som erhållits vid tillämpningen av denna förordning samt kundernas efterfrågan, den tekniska och rättsliga utvecklingen och marknadsutvecklingen. Rapporten ska vid behov åtföljas av förslag till ändringar av denna förordning.

2. Utvärderingsrapporten ska innehålla en bedömning av tillgängligheten och användbarheten vad gäller de europeiska e-identitetsplånböckerna, som omfattas av denna förordning, och bedöma om alla privata tillhandahållare av onlinetjänster som använder sig av tredje parts elektroniska identifieringstjänster för användarautentisering ska få i uppdrag att godta användningen av de europeiska e-identitetsplånböckerna.

3. Dessutom ska kommissionen vart fjärde år efter den rapport som avses i första stycket lämna en rapport till Europaparlamentet och rådet om framstegen i förhållande till denna förordnings mål.

42. 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 som kvalificerade anordningar för skapande av elektroniska underskrifter enligt denna förordning fram till 36 månader från denna förordnings ikraftträdande.

2. Kvalificerade certifikat som utfärdas åt fysiska personer inom ramen för direktiv 1999/93/EG ska även fortsättningsvis anses som kvalificerade certifikat för elektroniska underskrifter enligt denna förordning fram till 24 månader från denna förordnings ikraftträdande.

2a. Förvaltningen av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplar på distans av andra kvalificerade tillhandahållare av betrodda tjänster än 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 ska fortsätta att övervägas utan att behöva erhålla kvalificerad status för tillhandahållandet av dessa förvaltningstjänster fram till 24 månader efter denna förordnings ikraftträdande.

2b. Kvalificerade tillhandahållare av betrodda tjänster som har beviljats sin kvalificerade status enligt denna förordning före den [dagen för ändringsförordningens ikraftträdande] och som använder metoder för identitetskontroll för utfärdande av kvalificerade certifikat i enlighet med artikel 24.1 ska lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet som styrker överensstämmelse med artikel 24.1 så snart som möjligt men senast 30 månader efter ändringsförordningens ikraftträdande. Fram till dess att en sådan rapport om bedömning av överensstämmelse har lämnats in och tillsynsorganet har slutfört sin bedömning får den kvalificerade tillhandahållaren av betrodda tjänster fortsätta att förlita sig på användningen av de metoder för identitetskontroll som anges i artikel 24.1 i förordning (EU) nr 910/2014.”.

43. Bilaga I ska ändras i enlighet med bilaga I till denna förordning.

44. Bilaga II ska ersättas med texten i bilaga II till denna förordning.

45. Bilaga III ska ändras i enlighet med bilaga III till denna förordning.

46. Bilaga IV ska ändras i enlighet med bilaga IV till denna förordning.

47. En ny bilaga V, enligt lydelsen i bilaga V till denna förordning, ska läggas till.

48. En ny bilaga VI ska läggas till denna förordning.

Artikel 52

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 Bryssel den

På Europaparlamentets vägnar	På rådets vägnar
Ordförande	Ordförande

BILAGA I

I bilaga I 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 är lokaliserade.”.

BILAGA II

KRAV PÅ KVALIFICERADE ANORDNINGAR FÖR SKAPANDE AV ELEKTRONISKA UNDERSKRIFTER

1. Kvalificerade anordningar för skapande av elektroniska underskrifter ska genom lämpliga tekniker och förfaranden säkerställa att åtminstone

   a) konfidentialiteten för de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter är säkerställd på rimligt sätt,

   b) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter i praktiken endast kan förekomma en gång,

   c) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter med rimlig säkerhet inte kan härledas och att den elektroniska underskriften på ett tillförlitligt sätt är skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig,

   d) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter kan skyddas på ett tillförlitligt sätt av den legitime undertecknaren så att andra inte kan använda dem.

2. Kvalificerade anordningar för skapande av elektroniska underskrifter får inte förändra de uppgifter som ska undertecknas eller hindra att dessa uppgifter läggs fram för undertecknaren före undertecknandet.

BILAGA III

I bilaga III 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 är lokaliserade.”.

BILAGA IV

I bilaga IV ska led j) ersättas med följande:

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

BILAGA V

KRAV PÅ KVALIFICERAD ELEKTRONISK ATTESTERING AV ATTRIBUT

Kvalificerad elektronisk attestering av attribut ska omfatta följande:

e) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att attesteringen har utfärdats som en kvalificerad elektronisk attestering av attribut.

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

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

– för en fysisk person: personens namn.

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

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

i) Detaljerade uppgifter om när attesteringen börjar respektive upphör att gälla.

j) Attesteringens identitetskod, vilken måste vara unik för tillhandahållaren av kvalificerade betrodda tjänster, och, i tillämpliga fall, uppgift om det attesteringssystem som attesteringen av attribut omfattas av.

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

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

m) Information om den kvalificerade attesteringens giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar är lokaliserade.

BILAGA VI

MINIMIFÖRTECKNING ÖVER ATTRIBUT

Enligt artikel 45d ska medlemsstaterna säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade tillhandahållare av elektroniska attesteringar av attribut att med elektroniska medel, och på begäran av användaren, 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 nationell lagstiftning eller unionslagstiftning och i de fall då dessa attribut utgår från autentiska källor inom offentlig sektor:

1. Adress.
2. Ålder.
3. Kön.
4. Civilstånd.
5. Familjesituation.
6. Nationalitet eller medborgarskap.
7. Utbildning, titlar och licenser.
8. Yrkeskvalifikationer, titlar och licenser.
9. Offentliga tillstånd och licenser.
10. Finansiella uppgifter och företagsuppgifter.

BILAGA VII

KRAV PÅ ELEKTRONISK ATTESTERING AV ATTRIBUT UTFÄRDAD AV ELLER PÅ UPPDRAG AV ETT OFFENTLIGT ORGAN SOM ANSVARAR FÖR EN AUTENTISK KÄLLA

En elektronisk attestering av attribut utfärdad 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 attesteringen har utfärdats som ett elektroniskt intyg på attribut 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 intyget på attribut, 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 attesterade attributen hänvisar till; om en pseudonym används ska detta anges tydligt.
d) Det attesterade attributet eller de attesterade attributen, inbegripet, i tillämpliga fall, de uppgifter som är nödvändiga för att fastställa omfattningen för dessa attribut.
e) Detaljerade uppgifter om när attesteringen börjar respektive upphör att gälla.
f) Attesteringens identitetskod, vilken måste vara unik för det utfärdande offentliga organet, och, i tillämpliga fall, uppgift om det attesteringssystem som attesteringen av attribut 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 attesteringens giltighet, eller uppgift om var de tjänster som kan användas för att göra förfrågningar är lokaliserade.