Raad van de
Europese Unie

Brussel, 6 december 2022
(OR. en)

15706/22

Interinstitutioneel dossier:
2021/0136(COD)

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

RESULTAAT BESPREKINGEN

van:	het secretariaat-generaal van de Raad
d.d.:	6 december 2022
aan:	de delegaties
nr. vorig doc.:	14959/22 + ADD 1 + ADD 2
nr. Comdoc.:	9471/21
Betreft:	Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit - Algemene oriëntatie (6 december 2022)

Voor de delegaties gaat hierbij de algemene oriëntatie van de Raad betreffende bovengenoemd voorstel, die de Raad (Vervoer, Telecommunicatie en Energie) op 6 december 2022 in zijn 3917e zitting heeft goedgekeurd.

De algemene oriëntatie bevat het voorlopig standpunt van de Raad over dit voorstel, en vormt de basis voor de voorbereiding van de onderhandelingen met het Europees Parlement.

BIJLAGE

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[1],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) In de mededeling van de Commissie van 19 februari 2020 met als titel "De digitale toekomst van Europa vormgeven"[2] wordt een herziening van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad aangekondigd om de doeltreffendheid ervan te verbeteren, de voordelen ervan voor particulieren uit te breiden en betrouwbare digitale identiteiten voor alle Europeanen te bevorderen.

1 PB C , blz. .
2 COM/2020/67 final.

(2) In zijn conclusies van 1-2 oktober 2020[3] heeft de Europese Raad de Commissie opgeroepen een EU-breed kader voor beveiligde openbare elektronische identificatie te ontwikkelen, inclusief interoperabele digitale handtekeningen, om mensen controle over hun online-identiteit en -gegevens te geven en toegang tot openbare, particuliere en grensoverschrijdende digitale diensten mogelijk te maken.

(3) In de mededeling van de Commissie van 9 maart 2021, met als titel "Het digitale kompas 2030: de Europese aanpak voor het digitale decennium"[4] is de doelstelling vastgelegd van een EU-kader dat tussen nu en 2030 moet leiden tot een brede uitrol van een betrouwbare, door de gebruiker gecontroleerde identiteit, zodat elke burger zelf zijn online-interactie en aanwezigheid kan beheren.

(4) Een meer geharmoniseerde benadering van digitale identificatie moet de risico's en de kosten van de huidige versnippering door uiteenlopende nationale oplossingen verkleinen en de eengemaakte markt versterken door burgers, andere krachtens nationaal recht gedefinieerde ingezetenen en ondernemingen zich op een gemakkelijke en uniforme manier in de hele Unie online te laten identificeren. De Europese portemonnee voor digitale identiteit zal natuurlijke en rechtspersonen in de hele Unie een geharmoniseerd elektronisch identificatiemiddel bieden dat hen in staat zal stellen de aan hun identiteit gekoppelde gegevens te authenticeren en te delen. Iedereen moet veilig toegang kunnen hebben tot openbare en particuliere diensten en kunnen vertrouwen op een verbeterd ecosysteem voor vertrouwensdiensten en op geverifieerde identiteitsbewijzen en attesteringen van attributen, zoals een universitair diploma, die overal in de Unie wettelijk worden erkend en aanvaard. Het Europese kader voor een digitale identiteit beoogt een verschuiving van het gebruik van nationale digitale-identiteitsoplossingen naar de verstrekking van elektronische attesteringen van attributen die op Europees niveau geldig zijn. Aanbieders van elektronische attesteringen van attributen moeten profijt trekken uit duidelijke en uniforme regels en overheidsdiensten moeten kunnen vertrouwen op elektronische documenten in een bepaald formaat.

---

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

4 COM/2021/118 final/2.

(4a) Verschillende lidstaten hebben elektronische identificatiemiddelen ingevoerd – die ze ook grotendeels gebruiken – die tegenwoordig door dienstverleners in de Unie worden aanvaard. Daarnaast is er geïnvesteerd in zowel nationale als grensoverschrijdende oplossingen op basis van de huidige eIDAS-verordening, ook wat betreft de technische infrastructuur voor de interoperabiliteit van eIDAS-knooppunten. Om complementariteit te waarborgen en ervoor te zorgen dat Europese portemonnees voor digitale identiteit snel ingang vinden bij de huidige gebruikers van aangemelde elektronische identificatiemiddelen, maar ook om de gevolgen voor bestaande dienstverleners tot een minimum te beperken, wordt verwacht dat de Europese portemonnees voor digitale identiteit profijt zullen trekken uit de ervaring met bestaande elektronische identificatiemiddelen en uit de eIDAS-infrastructuur die op Europees en nationaal niveau is uitgerold.

(5) Ter ondersteuning van het concurrentievermogen van Europese bedrijven moeten aanbieders van onlinediensten kunnen vertrouwen op digitale-identiteitsoplossingen die in de hele Unie worden erkend, ongeacht de lidstaat waar die worden verleend, en dus profiteren van een geharmoniseerde Europese benadering van vertrouwen, beveiliging en interoperabiliteit. Gebruikers en dienstverleners moeten er beide baat bij kunnen hebben dat de rechtskracht van elektronische attesteringen van attributen in de hele Unie gelijk is.

(6) Verordening (EU) 2016/679[5] is van toepassing op de verwerking van persoonsgegevens uit hoofde van deze verordening. Daarom moet deze verordening specifieke waarborgen bevatten om te voorkomen dat aanbieders van elektronische identificatiemiddelen en van elektronische attestering van attributen persoonsgegevens van andere diensten combineren met persoonsgegevens met betrekking tot de diensten die binnen het toepassingsgebied van deze verordening vallen. Persoonsgegevens met betrekking tot het aanbieden van de Europese portemonnees voor digitale identiteit moeten logisch gescheiden worden van andere gegevens die in het bezit zijn van de verstrekker. Deze verordening belet niet dat verstrekkers van Europese portemonnees voor digitale identiteit aanvullende technische maatregelen toepassen die bijdragen tot de bescherming van persoonsgegevens, zoals de fysieke scheiding van persoonsgegevens in verband met het aanbieden van portemonnees en andere gegevens die in het bezit zijn van de verstrekker.

---

[5] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

(7) Er moeten geharmoniseerde voorwaarden worden vastgesteld voor het opzetten van een kader voor door de lidstaten aan te bieden Europese portemonnees voor digitale identiteit, op grond waarvan alle Unieburgers en andere ingezetenen krachtens nationaal recht veilig, gebruiksvriendelijk en gemakkelijk gegevens over hun identiteit kunnen delen, waarbij de gebruiker volledige controle heeft. De op die doelstellingen gerichte technologieën moeten worden ontwikkeld met het oog op het hoogste niveau van beveiliging, privacy en gebruiksgemak en op brede inzetbaarheid. De lidstaten moeten voor al hun onderdanen en ingezetenen gelijke toegang tot digitale identificatie waarborgen.

(8) Om ervoor te zorgen dat vertrouwende partijen kunnen vertrouwen op het gebruik van Europese portemonnees voor digitale identiteit en om gebruikers te beschermen tegen onrechtmatig gebruik van gevoelige gegevens, moeten vertrouwende partijen geregistreerd zijn als onderdeel van een kennisgevingsproces. De kennisgevingsvereisten voor vertrouwende partijen moeten in de meeste gevallen gebaseerd zijn op het verstrekken van een beperkte hoeveelheid informatie die nodig is om de vertrouwende partij bij de Europese portemonnee voor digitale identiteit te authenticeren. De vereisten moeten ook het gebruik van geautomatiseerde of eenvoudige procedures voor zelfrapportage mogelijk maken, alsook dat lidstaten op bestaande registers kunnen vertrouwen en die kunnen gebruiken. Tegelijkertijd kunnen er op nationaal of Unieniveau voor categorieën gevoelige gegevens specifieke regelingen bestaan die aan vertrouwende partijen strengere registratie- en vergunningsvereisten kunnen opleggen om onrechtmatig gebruik van identiteitsgegevens in dergelijke gevallen te voorkomen. In andere praktijkvoorbeelden kunnen vertrouwende partijen worden vrijgesteld van kennisgeving van hun voornemen om op de Europese digitale portemonnee een beroep te doen, bijvoorbeeld wanneer een recht om specifieke attributen te verifiëren niet vereist of mogelijk maakt dat de vertrouwende partij langs elektronische weg wordt geauthenticeerd. In deze fysieke scenario's is de gebruiker doorgaans in staat de vertrouwende partij te identificeren dankzij de context, bijvoorbeeld in de communicatie met een autoverhuurder of apotheker. Het kennisgevingsproces moet worden gestuurd door sectorale Unie- of nationale wetgeving, aangezien dit ruimte biedt voor verschillende praktijkvoorbeelden die kunnen verschillen wat betreft registratievereisten, werkwijze (online/offline) of de verplichting tot authenticatie van apparaten die aan de Europese portemonnee voor digitale identiteit kunnen worden gekoppeld. Vertrouwende partijen mogen niet worden verplicht het gebruik van de Europese portemonnee voor digitale identiteit te verifiëren op niveau van de Europese portemonnee zelf.

(9) Alle Europese portemonnees voor digitale identiteit moeten gebruikers in staat stellen om zich online en offline grensoverschrijdend te identificeren en te authenticeren om toegang tot een breed scala openbare en particuliere diensten te krijgen. Onverminderd de prerogatieven van de lidstaten betreffende de identificatie van hun onderdanen en ingezetenen, kunnen deze portemonnees ook tegemoetkomen aan de institutionele behoeften van overheids-instanties, internationale organisaties en de instellingen, organen en instanties van de Unie. Offlinegebruik is van belang in veel sectoren, zoals de gezondheidssector waar diensten vaak via persoonlijke interactie worden verleend, en waar voor e-recepten op QR-codes of soortgelijke technologieën moet kunnen worden vertrouwd om de authenticiteit te verifiëren. Op basis van betrouwbaarheidsniveau "hoog" moeten de Europese portemonnees voor digitale identiteit kunnen gebruikmaken van het potentieel van onvervalsbare oplossingen, zoals beveiligde elementen, ter naleving van de beveiligingsvoorschriften krachtens deze verordening. Met de Europese portemonnees voor digitale identiteit moeten gebruikers ook in de hele EU aanvaarde gekwalificeerde elektronische handtekeningen en zegels kunnen aanmaken en gebruiken. Met het oog op vereenvoudiging en kostenbesparingen voor personen en bedrijven in de hele EU, onder meer door de mogelijkheid van vertegenwoordigingsbevoegdheden en e-mandaten, moeten de lidstaten gemeenschappelijke normen gebruiken wanneer zij Europese portemonnees voor digitale identiteit uitgeven zodat naadloze interoperabiliteit en een hoog beveiligingsniveau worden gewaarborgd. Alleen de bevoegde instanties van de lidstaten kunnen een hoge mate van vertrouwen bieden bij de vaststelling van de identiteit van een persoon en aldus uitmaken of de persoon die stelt een bepaalde identiteit te hebben, daadwerkelijk is wie de persoon zegt te zijn. Daarom moeten de Europese portemonnees voor digitale identiteit gebruikmaken van de wettelijke identiteit van burgers, andere ingezetenen of rechtspersonen. Het vertrouwen in de Europese portemonnees voor digitale identiteit zou nog hoger worden als de verstrekkende partijen verplicht zijn passende technische en organisatorische maatregelen te treffen om een beveiligingsniveau te waarborgen dat in overeenstemming is met de risico's voor de rechten en vrijheden van natuurlijke personen, conform Verordening (EU) 2016/679. Het uitgeven, gebruiken voor authenticatie en intrekken van Europese portemonnees voor digitale identiteit is gratis voor natuurlijke personen. Diensten die afhankelijk zijn van het gebruik van de portemonnee kunnen kosten in rekening brengen, bijvoorbeeld in verband met het afgeven van elektronische attesteringen van attributen aan de portemonnee.

(9a) Om de invoering en het gebruik van Europese portemonnees voor digitale identiteit te vergemakkelijken is het nuttig die naadloos te integreren in het ecosysteem van openbare en particuliere digitale diensten die reeds op nationaal, lokaal of regionaal niveau worden toegepast. Om dit doel te bereiken, kunnen de lidstaten met wettelijke en organisatorische maatregelen instellingen die Europese portemonnees voor digitale identiteit afgeven meer flexibiliteit bieden en meer functionaliteiten van Europese portemonnees voor digitale identiteit mogelijk maken dan in deze verordening is bepaald, onder meer door een betere interoperabiliteit met bestaande nationale eID-middelen. Dit mag geenszins ten koste gaan van het aanbod van de kernfuncties van de Europese portemonnees voor digitale identiteit, zoals vastgesteld in deze verordening, en mag evenmin tot doel hebben bestaande nationale oplossingen aan te prijzen ten koste van Europese portemonnees voor digitale identiteit. Aangezien die aanvullende functies verder gaan dan deze verordening, komen zij niet in aanmerking voor de in deze verordening vastgestelde bepalingen inzake grensoverschrijdende afhankelijkheid van Europese portemonnees voor digitale identiteit.

(10) Teneinde een hoog niveau van gegevensbescherming, beveiliging en betrouwbaarheid te bereiken, moet in deze verordening een geharmoniseerd kader worden vastgesteld met de gemeenschappelijke specificaties en vereisten die van toepassing zijn op de Europese portemonnees voor digitale identiteit. Of de Europese portemonnees voor digitale identiteit in overeenstemming zijn met die vereisten moet worden gecertificeerd door conformiteits-beoordelingsinstanties die door de lidstaten zijn aangewezen. De certificering moet met name berusten op de betrokken Europese regelingen voor cyberbeveiligingscertificering, of delen daarvan, die zijn vastgesteld bij Verordening (EU) 2019/881[6], voor zover zij betrekking hebben op de cyberbeveiligingsvereisten die van toepassing zijn op Europese portemonnees voor digitale identiteit. Door te steunen op Europese regelingen voor cyberbeveiligingscertificering moet in de beveiliging van de Europese portemonnees voor digitale identiteit, ongeacht waar zij in de Unie worden uitgegeven, een geharmoniseerd niveau van vertrouwen gestalte krijgen. De cyberbeveiligingscertificering van de Europese portemonnees voor digitale identiteit moet voortbouwen op de rol van de nationale autoriteiten voor cyberbeveiligingscertificering, om erop toe te zien dat de door de conformiteitsbeoordelingsinstanties binnen hun rechtsgebied afgegeven certificaten de betrokken Europese cyberbeveiligingsregelingen naleven en om die naleving te monitoren. Evenzo moet bij certificering profijt worden getrokken uit normen en technische specificaties zoals gespecificeerd in Verordening (EU) 2019/881. Dergelijke specificaties kunnen worden gebruikt als documenten over de huidige stand van de techniek, zoals gespecificeerd in de betrokken regelingen voor cyberbeveiligingscertificering uit hoofde van Verordening (EU) 2019/881. Wanneer de certificering van betrokken diensten of processen ter beveiliging van de portemonnee niet valt onder de betrokken Europese regelingen voor cyberbeveiligings-certificering die zijn vastgesteld op grond van Verordening (EU) 2019/881, moeten passende regelingen worden opgezet overeenkomstig titel III van Verordening (EU) 2019/881. Er moet een gemeenschappelijke en geharmoniseerde regeling voor de certificering van Europese portemonnees voor digitale identiteit worden vastgesteld om te beoordelen of zij voldoen aan de in deze verordening vastgestelde gemeenschappelijke specificaties en vereisten, met uitzondering van die met betrekking tot cyberbeveiliging en gegevensbescherming, met name die welke betrekking hebben op functionele en operationele aspecten. Met betrekking tot die certificering moeten, om een hoog niveau van vertrouwen en transparantie te waarborgen, mechanismen en procedures worden vastgesteld om intercollegiaal leren en samenwerking tussen de lidstaten te bevorderen bij het monitoren en evalueren van de certificeringsinstanties en de certificaten en certificeringsverslagen die zij afgeven. Een dergelijk mechanisme voor intercollegiaal leren moet Verordening (EU) n2016/679 en Verordening (EU) 2019/881 onverlet laten. Certificering van de portemonnee in het kader van Verordening (EU) 2016/679 is een vrijwillig instrument dat onder meer kan worden gebruikt om aan te tonen dat wordt voldaan aan de vereisten van Verordening (EU) 2016/679, zoals die van toepassing zijn op Europese portemonnees voor digitale identiteit en de verstrekking ervan aan Europese burgers.

---

[6] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

(10a) Burgers en ingezetenen moeten kunnen instappen op de Europese portemonnee voor digitale identiteit door gebruik te maken van elektronische identificatiemiddelen die zijn uitgegeven met betrouwbaarheidsniveau "hoog". Op elektronische identificatiemiddelen met betrouwbaarheidsniveau "hoog" mag uitsluitend een beroep worden gedaan indien de geharmoniseerde technische en operationele specificaties met betrouwbaarheidsniveau "aanzienlijk" in combinatie met andere aanvullende middelen voor identiteitsverificatie het mogelijk zullen maken te voldoen aan de eisen van deze verordening met betrekking tot betrouwbaarheidsniveau "hoog". Die aanvullende middelen of maatregelen moeten betrouwbaar en gemakkelijk te gebruiken zijn voor de gebruikers en kunnen worden gebaseerd op de mogelijkheid om gebruik te maken van instapprocedures op afstand, gekwalificeerde certificaten ondersteund door gekwalificeerde handtekeningen, gekwalificeerde elektronische attestering van attributen of een combinatie daarvan. Om ervoor te zorgen dat de Europese portemonnees voor digitale identiteit voldoende ingang vinden, moeten bij uitvoeringshandelingen geharmoniseerde technische en operationele specificaties worden vastgesteld waarmee gebruikers met behulp van elektronische identificatiemiddelen kunnen instappen, met inbegrip van die welke worden afgegeven met betrouwbaarheidsniveau "aanzienlijk".

(10b) Het doel van deze verordening is de gebruiker te voorzien van een volledig mobiele, veilige en gebruiksvriendelijke Europese portemonnee voor digitale identiteit. Totdat gecertificeerde fraudebestendige oplossingen beschikbaar zijn, zoals beveiligde elementen in de apparaten van de gebruikers, kunnen de Europese portemonnees voor digitale identiteit voor de bescherming van het cryptografisch materiaal en andere gevoelige gegevens bij wijze van overgangsmaatregel gebruikmaken van gecertificeerde externe beveiligde elementen of van aangemelde nationale oplossingen met betrouwbaarheidsniveau "hoog" om aan te tonen dat met betrekking tot het betrouwbaarheidsniveau van de portemonnee aan de eisen ter zake van de verordening wordt voldaan. Het gebruik van de bovengenoemde overgangsmaatregel moet worden beperkt tot praktijkvoorbeelden waarvoor betrouwbaarheidsniveau "hoog" vereist is, bijvoorbeeld bij het instappen van gebruikers in de portemonnee en authenticatie bij diensten die betrouwbaarheidsniveau "hoog" vereisen. Bij de authenticatie van diensten met betrouwbaarheidsniveau "aanzienlijk", mag het voor Europese portemonnees voor digitale identiteit geen verplichting zijn bovengenoemde overgangsmaatregel te gebruiken. Deze verordening moet de nationale voorwaarden voor de afgifte en het gebruik van een gecertificeerd extern beveiligd element onverlet laten indien deze overgangsmaatregel daarop berust.

(11) Europese portemonnees voor digitale identiteit moeten het hoogste beschermings- en beveiligingsniveau voor de voor authenticatie gebruikte persoonsgegevens waarborgen, ongeacht of die gegevens lokaal of in de cloud worden opgeslagen, met inachtneming van de verschillende risiconiveaus. De verwerking van biometrische gegevens als authenticatie-factor van sterke gebruikersauthenticatie is een van de identificatiemethoden die een hoog niveau van vertrouwen bieden, met name in combinatie met andere authenticatie-elementen. Aangezien biometrische gegevens een uniek kenmerk van een persoon vormen, mogen die uitsluitend op grond van de uitzonderingen van artikel 9, lid 2, van Verordening (EU) 2016/679 worden verwerkt en zijn passende waarborgen vereist die in verhouding moeten staan tot het risico dat die verwerking kan inhouden voor de rechten en vrijheden van natuurlijke personen.

(11a) De werking van de Europese portemonnees voor digitale identiteit moet transparant zijn en de verwerking van persoonsgegevens moet kunnen worden geverifieerd. Daartoe worden de lidstaten aangemoedigd om de broncode van softwarecomponenten van Europese portemonnees voor digitale identiteit vrij te geven, voor zover die componenten verband houden met de verwerking van persoonsgegevens en gegevens van rechtspersonen. Het vrijgeven van die broncode stelt de samenleving, waaronder gebruikers en ontwikkelaars, in staat de werking ervan te begrijpen. Mogelijk kan dit ook het vertrouwen van gebruikers in het ecosysteem van de portemonnee vergroten en bijdragen tot de beveiliging van portemonnees, omdat iedereen dan kwetsbaarheden en fouten in de code kan melden. Dat zal leveranciers ertoe aanzetten een zeer hoogbeveiligd product te leveren en in stand te houden. Daarnaast worden de lidstaten aangemoedigd om waar mogelijk de broncode beschikbaar te stellen in het kader van een openbronlicentie. Een openbronlicentie stelt de samenleving, met inbegrip van gebruikers en ontwikkelaars, in staat de broncode te wijzigen en te hergebruiken.

(12) Om het Europese kader voor digitale identiteit toekomstbestendig en open voor innovatie en technologische ontwikkelingen te houden, moeten de lidstaten worden aangemoedigd om gezamenlijke testomgevingen op te zetten om innovatieve oplossingen in een gecontroleerde en beveiligde omgeving te testen, in het bijzonder om de functionaliteit, de bescherming van persoonsgegevens, de beveiliging en de interoperabiliteit van de oplossingen te verbeteren en om technische referenties en wettelijke vereisten in toekomstige updates op te nemen. Het Europese midden- en kleinbedrijf, startups en individuele innovatoren en onderzoekers moeten worden gestimuleerd om aan deze omgeving deel te nemen.

(13) Bij Verordening (EU) 2019/1157[7] is de beveiliging van identiteitskaarten in augustus 2021 verhoogd door middel van strengere beveiligingskenmerken. De lidstaten moeten overwegen of het haalbaar is die op grond van stelsels voor elektronische identificatie aan te melden om de grensoverschrijdende beschikbaarheid van elektronische identificatiemiddelen te verruimen.

(14) De aanmeldingsprocedure van stelsels voor elektronische identificatie moet worden vereenvoudigd en versneld om de toegang tot gemakkelijke, betrouwbare, veilige en innovatieve authenticatie- en identificatiemethoden te bevorderen en, waar van belang, particuliere identiteitsverstrekkers te stimuleren om stelsels voor elektronische identificatie aan de autoriteiten van de lidstaten aan te bieden met het oog op aanmelding als nationaal stelsel voor elektronische identificatie conform Verordening (EU) nr. 910/2014.

(15) Een stroomlijning van de huidige procedures voor aanmelding en collegiale toetsing voorkomt heterogene benaderingen bij de beoordeling van verschillende aangemelde stelsels voor elektronische identificatie en zorgt voor vertrouwen tussen de lidstaten. Nieuwe en vereenvoudigde mechanismen moeten de samenwerking tussen de lidstaten op het gebied van beveiliging en interoperabiliteit van hun aangemelde stelsels voor elektronische identificatie bevorderen.

(16) De lidstaten moeten met de nieuwe en flexibele instrumenten zorgen voor de naleving van deze verordening en de bijbehorende uitvoeringshandelingen. De lidstaten moeten op grond van deze verordening gebruik kunnen maken van verslagen en beoordelingen van geaccrediteerde conformiteitsbeoordelingsinstanties, zoals overeenkomstig Verordening (EU) 2019/881 op Unieniveau op te zetten certificeringsregelingen, ter ondersteuning van hun verklaringen over de afstemming van de regelingen of delen daarvan op de voorwaarden van de eIDAS-verordening met betrekking tot de interoperabiliteit en de beveiliging van de aangemelde stelsels voor elektronische identificatie.

---

[7] Verordening (EU) 2019/1157 van het Europees Parlement en de Raad van 20 juni 2019 betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten afgegeven aan burgers van de Unie en hun familieleden die hun recht van vrij verkeer uitoefenen (PB L 188 van 12.7.2019, blz. 67).

(17a) Het gebruik van unieke en permanente identificatiecodes die door de lidstaten zijn afgegeven of door de Europese portemonnee voor digitale identiteit worden gegenereerd, samen met het gebruik van persoonsidentificatiegegevens, is van essentieel belang om ervoor te zorgen dat de identiteit van de gebruiker, met name in de overheidssector en op grond van nationale of Uniewetgeving, kan worden geverifieerd. Deze verordening moet ervoor zorgen dat de Europese portemonnee voor digitale identiteit een mechanisme kan bieden om het matchen van bestanden mogelijk te maken, onder meer door gebruik te maken van gekwalificeerde elektronische attesteringen van attributen, en dat unieke en permanente identificatiecodes in de persoonsidentificatiedatareeks kunnen worden opgenomen. Een unieke en permanente identificatiecode kan bestaan uit afzonderlijke of meervoudige identificatiegegevens die sectorspecifiek kunnen zijn, zolang hij dient om de gebruiker in de hele Unie op unieke wijze te identificeren. De Europese portemonnee voor digitale identiteit moet ook voorzien in een mechanisme van specifieke identificatiecodes die vertrouwende partijen kunnen gebruiken indien het gebruik van een unieke en permanente identificatiecode op grond van het nationale recht of het Unierecht vereist is. In ieder geval moet het mechanisme voor het matchen van bestanden en het gebruik van unieke en permanente identificatiecodes ervoor zorgen dat de gebruiker wordt beschermd tegen misbruik van persoonsgegevens overeenkomstig deze verordening en het toepasselijke Unierecht, met name Verordening (EU) 2016/679, onder meer tegen het risico van profilering en tracering in verband met het gebruik van de Europese portemonnee voor digitale identiteit.

(17aa) Het is van essentieel belang rekening te houden met de behoeften van gebruikers en zo de vraag naar Europese portemonnees voor digitale identiteit te stimuleren. Er moeten zinvolle praktijkvoorbeelden en onlinediensten komen die steunen op de beschikbare Europese portemonnees voor digitale identiteit. Met het oog op het gebruiksgemak en om de grensoverschrijdende beschikbaarheid van dergelijke diensten te waarborgen, is het belangrijk maatregelen te nemen om bij het ontwerp, de ontwikkeling en de uitvoering van onlinediensten een gelijke aanpak in alle lidstaten te faciliteren. Niet-bindende richtsnoeren voor het ontwerp, de ontwikkeling en de uitvoering van onlinediensten op basis van Europese portemonnees voor digitale identiteit kunnen een nuttig instrument worden om dit doel te bereiken. Deze richtsnoeren moeten worden opgesteld met inachtneming van het interoperabiliteitskader van de Unie. De lidstaten moeten bij de aanneming daarvan een leidende rol spelen.

(18) Overeenkomstig Richtlijn (EU) 2019/882[8] moeten personen met een handicap in staat zijn de Europese portemonnees voor digitale identiteit, vertrouwensdiensten en producten voor de eindgebruiker die bij het verlenen van deze diensten gebruikt worden, op gelijke voet als andere gebruikers te gebruiken.

(19) Deze verordening mag geen betrekking hebben op aspecten die verband houden met de totstandkoming en de geldigheid van contracten of andere juridische verbintenissen waaraan in het nationale recht of het Unierecht vormvereisten worden gesteld. Daarenboven dient zij de nationale vormvereisten voor openbare registers, met name handelsregisters en kadasters, onverlet te laten.

(20) De levering en het gebruik van vertrouwensdiensten worden steeds belangrijker voor de internationale handel en samenwerking. Internationale partners van de EU zetten op Verordening (EU) nr. 910/2014 geïnspireerde vertrouwenskaders op. Om de erkenning van dergelijke diensten en de aanbieders ervan te faciliteren, kunnen in uitvoeringswetgeving derhalve de voorwaarden worden vastgesteld op grond waarvan de vertrouwenskaders van derde landen als gelijkwaardig aan het vertrouwenskader voor gekwalificeerde vertrouwensdiensten en aanbieders daarvan in de zin van deze verordening kunnen worden beschouwd, in aanvulling op de mogelijkheid van wederzijdse erkenning van in de Unie en in derde landen gevestigde vertrouwensdiensten en aanbieders overeenkomstig artikel 218 VWEU. Bij het vaststellen van de voorwaarden waaronder vertrouwenskaders van derde landen als gelijkwaardig aan het vertrouwenskader voor gekwalificeerde vertrouwensdiensten en aanbieders in deze verordening kunnen worden beschouwd, moet ook gelden dat aan desbetreffende bepalingen van Richtlijn XXXX/XXXX, (NIS2-richtlijn) en Verordening (EU) 2016/679 moet zijn voldaan, alsook dat vertrouwenslijsten moeten worden gebruikt als essentiële elementen om vertrouwen op te bouwen.

---

[8] Richtlijn (EU) 2019/882 van het Europees Parlement en de Raad van 17 april 2019 betreffende de toegankelijkheidsvoorschriften voor producten en diensten (PB L 151 van 7.6.2019, blz. 70).

(21) Deze verordening moet voortbouwen op handelingen van de Unie tot waarborging van betwistbare en eerlijke markten in de digitale sector. Zij bouwt met name voort op Verordening (EU) 2022/1925, die regels bepaalt voor als poortwachter aangewezen aanbieders van kernplatformdiensten en, onder meer, verbiedt dat poortwachters zakelijke gebruikers verplichten een identificatiedienst van de poortwachter te gebruiken, aan te bieden of daarmee te interageren in het kader van diensten die worden aangeboden door zakelijke gebruikers die gebruikmaken van de kernplatformdiensten van die poortwachter. Krachtens artikel 6, lid 7, van Verordening (EU) 2022/1925 moet de poortwachter het voor zakelijke gebruikers en aanbieders van ondersteunende diensten mogelijk maken toegang te krijgen tot en te interageren met dezelfde functies van het besturingssysteem, van de hardware en van de software die beschikbaar zijn of worden gebruikt bij het verlenen van ondersteunende diensten door de poortwachter. Overeenkomstig artikel 2, punt 15, van de wet inzake digitale markten zijn identificatiediensten een type ondersteunende dienst. Zakelijke gebruikers en aanbieders van ondersteunende diensten moeten daarom toegang kunnen krijgen tot die hardware- en softwarefuncties, zoals beveiligde elementen in smartphones, en daarmee kunnen interageren via de Europese portemonnees voor digitale identiteit of door de lidstaten aangemelde elektronische identificatiemiddelen.

(22) Om de aan aanbieders van vertrouwensdiensten opgelegde cyberbeveiligingsvoorschriften te stroomlijnen en deze aanbieders en hun respectieve bevoegde autoriteiten van het bij Richtlijn XXXX/XXXX (NIS2-richtlijn) opgerichte wettelijke kader te laten profiteren, moeten vertrouwensdiensten passende technische en organisatorische maatregelen nemen overeenkomstig Richtlijn XXXX/XXXX (NIS2-richtlijn), zoals maatregelen tegen systeemfalen, menselijke fouten, kwaadwillige acties of natuurverschijnselen, voor het beheren van de risico's voor de veiligheid van netwerk- en informatiesystemen die die aanbieders gebruiken om hun diensten te verlenen, en voor het melden van significante incidenten en cyberdreigingen overeenkomstig Richtlijn XXXX/XXXX (NIS2-richtlijn). Wat het melden van incidenten betreft, moeten aanbieders van vertrouwensdiensten melding maken van alle incidenten die aanzienlijke gevolgen hebben voor de verlening van hun diensten, zoals diefstal of verlies van apparatuur, schade aan netwerkbekabeling of incidenten in het kader van persoonsidentificatie. De vereisten inzake het risicobeheer en de verslagleggingsverplichtingen op het gebied van cyberbeveiliging overeenkomstig Richtlijn XXXX/XXXX [NIS2-richtlijn] moeten als aanvullend op de overeenkomstig deze verordening aan aanbieders van vertrouwensdiensten opgelegde voorschriften worden beschouwd. Indien van toepassing, moeten de overeenkomstig Richtlijn XXXX/XXXX (NIS2-richtlijn) aangeduide bevoegde autoriteiten de gevestigde nationale praktijken of richtsnoeren met betrekking tot de uitvoering van beveiligings- en verslagleggingsvereisten en het toezicht op de naleving van dergelijke vereisten overeenkomstig Verordening (EU) nr. 910/2014 blijven toepassen. Verplichtingen overeenkomstig deze verordening laten de verplichting tot het melden van inbreuken op persoonsgegevens overeenkomstig Verordening (EU) 2016/679 onverlet.

(23) Er moet de nodige aandacht worden besteed aan de doeltreffende samenwerking tussen de NIS- en de eIDAS-autoriteiten. Indien het toezichthoudende orgaan uit hoofde van deze verordening een andere is dan de overeenkomstig Richtlijn XXXX/XXXX [NIS2] aangeduide bevoegde autoriteit, moeten die instanties nauw samenwerken, door tijdig relevante informatie uit te wisselen om doeltreffend toezicht op aanbieders van vertrouwensdiensten te houden en te waarborgen dat zij deze verordening en Richtlijn XXXX/XXXX [NIS2] naleven. De toezichthoudende organen uit hoofde van deze verordening moeten de bevoegde autoriteit uit hoofde van Richtlijn XXXX/XXXX [NIS2] kunnen verzoeken de relevante informatie te verstrekken die ze nodig hebben om een gekwalificeerde status toe te kennen en om toezichtmaatregelen te nemen om na te gaan of aanbieders van vertrouwensdiensten de voorwaarden van NIS 2 naleven, of om te eisen dat zij een niet-naleving verhelpen.

(24) Het is van essentieel belang dat wordt voorzien in een rechtskader ter facilitering van de grensoverschrijdende erkenning van bestaande nationale juridische regelingen met betrekking tot diensten voor elektronisch aangetekende bezorging. Dat kader zou voor aanbieders van vertrouwensdiensten in de Unie ook nieuwe afzetmogelijkheden kunnen openen voor het aanbieden van nieuwe pan-Europese diensten voor elektronisch aangetekende bezorging. Om ervoor te zorgen dat de gegevens die met behulp van gekwalificeerde dienst voor elektronisch aangetekende bezorging aan de juiste geadresseerde worden geleverd, moeten die diensten de identificatie van de geadresseerde met volledige zekerheid waarborgen, terwijl voor de identificatie van de afzender een hoog niveau van vertrouwen zal volstaan. De lidstaten moeten aanbieders van gekwalificeerde diensten voor elektronisch aangetekende bezorging aansporen om hun diensten interoperabel te maken met gekwalificeerde diensten voor elektronisch aangetekende bezorging van andere gekwalificeerde vertrouwensdiensten, zodat tussen twee of meer aanbieders van gekwalificeerde vertrouwensdiensten gegevens voor elektronisch aangetekende bezorging gemakkelijk kunnen worden uitgewisseld en eerlijke praktijken in de interne markt worden bevorderd.

(25) Meestal kunnen burgers en andere ingezetenen niet veilig en met een hoog niveau van gegevensbescherming grensoverschrijdend digitaal informatie uitwisselen met betrekking tot hun identiteit, zoals adres, leeftijd en beroepskwalificaties, rijbewijzen en andere vergunningen en betalingsgegevens.

(26) Het moet mogelijk zijn betrouwbare digitale attributen uit te geven en te verwerken, en bij te dragen tot een lagere regeldruk, en burgers en andere ingezetenen die attributen in hun privé- en openbare transacties te laten gebruiken. Burgers en andere ingezetenen moeten bijvoorbeeld kunnen aantonen dat zij beschikken over een geldig rijbewijs dat door een instantie in een lidstaat is afgegeven, wat de bevoegde autoriteiten in andere lidstaten kan worden geverifieerd en vertrouwd, en ze moeten hun socialezekerheidsgegevens of toekomstige digitale reisdocumenten grensoverschrijdend kunnen gebruiken.

(27) Entiteiten die geattesteerde attributen zoals diploma's, vergunningen of geboorteakten verzamelen, aanmaken en afgeven, moeten aanbieders van elektronische attestering van attributen kunnen worden. Vertrouwende partijen moeten elektronische attesteringen van attributen als gelijkwaardig aan papieren attesteringen kunnen gebruiken. Daarom mag het rechtsgevolg van een elektronische attestering van attributen niet worden ontzegd op grond van het feit dat die elektronisch is of niet aan de eisen voor gekwalificeerde een elektronische attestering van attributen voldoet. Daartoe moeten algemene eisen worden vastgesteld om te waarborgen dat een gekwalificeerde elektronische attestering van attributen dezelfde rechtsgevolgen heeft als wettelijk uitgegeven attesteringen op papier. Die eisen moeten evenwel van toepassing zijn onverminderd het Unierecht of het nationale recht waarin aanvullende sectorspecifieke vormvereisten met onderliggende rechtsgevolgen worden gesteld, en met name onverminderd de grensoverschrijdende erkenning van gekwalificeerde elektronische attesteringen van attributen, indien van toepassing.

(28) Voor een ruime beschikbaarheid en bruikbaarheid van Europese portemonnees voor digitale identiteit is aanvaarding door particuliere dienstverleners vereist. Particuliere vertrouwende partijen die diensten verlenen op het gebied van vervoer, energie, bankwezen, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie, moeten het gebruik van Europese portemonnees voor digitale identiteit aanvaarden voor de verlening van diensten waarvoor op grond van nationale of Uniewetgeving of contractuele verbintenis sterke gebruikers-authenticatie vereist is. Om het gebruik van de Europese portemonnee voor digitale identiteit te vergemakkelijken en de aanvaarding ervan te bevorderen, moeten breed gedragen industriële normen en specificaties in acht worden genomen. Indien zeer grote onlineplatforms in de zin van artikel 25, lid 1, van Verordening [referentie verordening inzake digitale diensten] verlangen dat gebruikers zich authenticeren om toegang tot onlinediensten te krijgen, moet die platforms worden opgelegd het gebruik van Europese portemonnees voor digitale identiteit op vrijwillig verzoek van de gebruiker te aanvaarden. Gebruikers moeten niet worden verplicht de portemonnee te gebruiken om toegang tot particuliere diensten te krijgen, maar als gebruikers dat willen, moeten zeer grote onlineplatforms de Europese portemonnee voor digitale identiteit daarvoor aanvaarden, met inachtneming van het beginsel van minimale gegevensverwerking. Vanwege het belang van zeer grote onlineplatforms op grond van hun bereik, met name wat het aantal afnemers van hun diensten en economische transacties betreft, is dit noodzakelijk om gebruikers beter tegen fraude te beschermen en een hoog niveau van gegevensbescherming te waarborgen. Er moeten zelfregulerende gedragscodes op Unieniveau (gedragscodes) worden ontwikkeld om bij te dragen tot de brede beschikbaarheid en bruikbaarheid van elektronische identificatiemiddelen, inclusief Europese portemonnees voor digitale identiteit, binnen het toepassingsgebied van deze verordening. De gedragscodes moeten zorgen voor een brede aanvaarding van elektronische identificatiemiddelen, ook voor Europese portemonnees voor digitale identiteit van dienstverleners die niet als zeer grote platforms worden aangemerkt en die zich voor gebruikersauthenticatie bedienen van elektronische identificatiediensten van derden. De gedragscodes moeten binnen 12 maanden na de vaststelling van deze verordening worden ontwikkeld. De Europese Commissie moet 24 maanden na de uitrol van deze diensten de doeltreffendheid ervan in termen van beschikbaarheid en bruikbaarheid voor de gebruiker van de Europese portemonnee voor digitale identiteit evalueren.

(29) Selectieve openstelling is een concept dat de gegevenseigenaar in staat stelt slechts bepaalde delen van een grote datareeks open te stellen, zodat de ontvangende entiteit uitsluitend benodigde informatie ontvangt, bijvoorbeeld wanneer een gebruiker voor een vertrouwende partij uitsluitend de data openstelt die nodig zijn voor het verlenen van de door de gebruiker gevraagde dienst. Het moet technisch mogelijk zijn dat de Europese portemonnee voor digitale identiteit de attributen selectief openstelt voor vertrouwende partijen. Die selectief opengestelde attributen, ook indien die oorspronkelijk onderdeel waren van meervoudige onderscheiden elektronische attesteringen, kunnen vervolgens worden gecombineerd en aan vertrouwende partijen worden aangeboden. Dit kenmerk moet een basiskenmerk in het ontwerp worden en aldus het gebruiksgemak en de bescherming van persoonsgegevens – waaronder minimale gegevensverwerking – versterken.

(30) Attributen die de aanbieders van gekwalificeerde vertrouwensdiensten verlenen als onderdeel van de gekwalificeerde attestering van attributen moeten aan de hand van authentieke bronnen worden geverifieerd, hetzij rechtstreeks door de aanbieder van gekwalificeerde vertrouwensdiensten, hetzij via aangewezen intermediairs die overeenkomstig nationaal recht of Unierecht op nationaal niveau zijn erkend met het oog op de beveiligde uitwisseling van geattesteerde attributen tussen aanbieders van identiteits-diensten of van attestering van attribuutsdiensten enerzijds en vertrouwende partijen anderzijds. De lidstaten moeten op nationaal niveau passende mechanismen instellen om ervoor te zorgen dat verleners van gekwalificeerde vertrouwensdiensten die gekwalificeerde elektronische attesteringen van attributen afgeven, na toestemming van de persoon aan wie de attestering wordt afgegeven, aan de hand van authentieke bronnen de authenticiteit van de attributen kunnen verifiëren. Passende mechanismen kunnen het gebruik van specifieke intermediairs of technisch oplossingen omvatten die in overeenstemming zijn met de nationale wetgeving betreffende de toegang tot authentieke bronnen. De aanwezigheid van een mechanisme waarmee attributen aan de hand van authentieke bronnen kunnen worden geverifieerd moet ervoor zorgen dat aanbieders van gekwalificeerd vertrouwensdiensten die gekwalificeerde elektronische attesteringen van attributen afgeven, gemakkelijker de verplichtingen uit hoofde van deze verordening zullen naleven. In bijlage VI staat een lijst van categorieën van attributen waarvoor de lidstaten maatregelen moeten nemen opdat gekwalificeerde aanbieders van elektronische attesteringen van attributen, door middel van elektronische middelen en op verzoek van de gebruiker hun authenticiteit aan de hand van de betrokken authentieke bron kunnen verifiëren. Welke specifieke attributen onder deze categorieën moeten vallen, moet door de lidstaten worden overeengekomen.

(31) Veilige elektronische identificatie en de verlening van attesteringen van attributen moeten extra flexibiliteit en oplossingen voor de financiëledienstensector bieden om klanten te kunnen identificeren en specifieke attributen te kunnen uitwisselen waaraan moet worden voldaan, zoals cliëntenonderzoeksvereisten uit hoofde van de antiwitwasverordening [referentie toevoegen na vaststelling van het voorstel], of uit de wetgeving ter bescherming van investeerders voortvloeiende geschiktheidseisen, ofwel ter ondersteuning van strenge cliëntauthenticatievereisten voor online-identificatie om op accounts in te loggen en transacties op het gebied van betalingsdiensten te initiëren.

(31a) Ter wille van de consistentie in de certificeringspraktijken in de EU, moet de Commissie richtsnoeren uitbrengen over de certificering en hercertificering van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en van gekwalificeerde middelen voor het aanmaken van elektronische zegels, onder meer wat betreft hun geldigheid en geldigheidsduur. Deze verordening belet lidstaten niet om openbare of particuliere organen die over gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen beschikken, toe te staan om tijdelijk de geldigheid van een certificering te verlengen indien hercertificering van hetzelfde middel om andere redenen dan een inbreuk of een veiligheidsincident niet binnen de wettelijk vastgestelde termijn mogelijk is.

(32) Diensten voor de authenticatie van websites bieden gebruikers een hoge mate van zekerheid dat het om de website van een werkelijk bestaande, legitieme entiteit gaat, ongeacht het platform dat daarvoor wordt gebruikt. Die diensten dragen bij tot toenemend vertrouwen in online zaken doen, en tot minder onlinefraude. Websites die gebruikmaken van diensten voor authenticatie van websites moeten dat op vrijwillige basis kunnen doen. Om van authenticatie van websites een middel te maken om het vertrouwen te bevorderen, de gebruikers betere ervaringen te bezorgen en de groei in de interne markt te bevorderen, moet deze verordening evenwel in minimumverplichtingen voorzien inzake beveiliging en aansprakelijkheid voor aanbieders van diensten voor authenticatie van websites en de door hen verleende diensten. Daartoe moeten aanbieders van webbrowsers zorgen voor ondersteuning van en interoperabiliteit met gekwalificeerde certificaten voor websiteauthenticatie overeenkomstig Verordening (EU) nr. 910/2014. Zij moeten gekwalificeerde certificaten voor websiteauthenticatie erkennen en ervoor zorgen dat de gecertificeerde identiteitsgegevens zichtbaar zijn voor de eindgebruiker in de browseromgeving, op basis van de overeenkomstig deze verordening vastgestelde specificaties. Het feit dat een gekwalificeerd certificaat voor websiteauthenticatie erkend wordt als een door een gekwalificeerde aanbieder van vertrouwensdiensten afgegeven gekwalificeerd certificaat, moet ervoor zorgen dat de identiteitsgegevens in het certificaat overeenkomstig deze verordening kunnen worden geauthenticeerd en geverifieerd. Dit mag aanbieders van webbrowsers niet beletten om ernstige nalevingstekortkomingen met betrekking tot inbreuken op beveiliging en integriteitsverlies voor individuele certificaten aan te pakken en aldus bij te dragen aan de onlinebeveiliging van eindgebruikers. Om burgers nog meer te beschermen en het gebruik van gekwalificeerde certificaten voor websiteauthenticatie verder te bevorderen, moeten overheidsinstanties in de lidstaten overwegen om die certificaten in hun websites op te nemen.

(33) Veel lidstaten hebben nationale vereisten ingevoerd voor diensten die beveiligde en betrouwbare digitale archivering aanbieden om elektronische gegevens en bijbehorende vertrouwensdiensten voor de lange termijn te kunnen bewaren. Om de rechtszekerheid, het vertrouwen en de harmonisatie tussen de lidstaten te waarborgen, moet een rechtskader voor gekwalificeerde elektronische archiveringsdiensten worden opgesteld, geïnspireerd op het in deze verordening opgenomen kader voor de andere vertrouwensdiensten. Dat kader moet aanbieders van vertrouwensdiensten en gebruikers een doelmatig instrument bieden met functionele vereisten voor elektronische archiveringsdiensten en met duidelijke rechtsgevolgen wanneer van een gekwalificeerde elektronische archiveringsdienst wordt gebruikgemaakt. Die bepalingen moeten van toepassing zijn op zowel documenten die in elektronisch vorm het licht zien, als papieren documenten die gescand en gedigitaliseerd worden. Indien vereist, moeten deze bepalingen het mogelijk maken dat de bewaarde elektronische gegevens naar andere media of in andere formaten worden overdragen om hun houdbaarheid en leesbaarheid tot na de technische geldigheidsperiode te verlengen, waarbij verlies van gegevens of wijzigingen daarin zoveel mogelijk moeten worden beperkt. Indien de aan de digitale archiveringsdienst overgedragen gegevens een of meer gekwalificeerde elektronische handtekeningen of zegels bevatten, moet de dienst gebruikmaken van procedures en technieken waarmee de betrouwbaarheid van de handtekeningen of zegels gedurende de bewaringstermijn van die gegevens wordt verlengd, eventueel door zich te bedienen van andere bij deze verordening opgezette gekwalificeerde elektronische vertrouwensdiensten. Voor het aanmaken van bewijsmateriaal in gevallen waarin elektronische handtekeningen, elektronische zegels of elektronische tijdstempels worden gebruikt, moet een beroep worden gedaan op gekwalificeerde elektronische vertrouwensdiensten. Voor zover elektronische archiveringsdiensten niet bij deze verordening zijn geharmoniseerd, kunnen de lidstaten in overeenstemming met het Unierecht nationale bepalingen in verband met deze diensten invoeren of handhaven, zoals specifieke bepalingen waarbij sommige afwijkingen worden toegestaan voor in een organisatie geïntegreerde diensten die uitsluitend voor de interne archivering van die organisatie worden gebruikt. Deze verordening mag geen onderscheid maken tussen documenten die in elektronisch vorm het licht zien en gedigitaliseerd documenten.

(33a) Nationale archieven en geheugeninstellingen zijn, als organisaties die zich in het openbaar belang wijden aan het behoud van het documentair erfgoed, normaliter bij nationale wet met hun opdracht belast en bieden niet noodzakelijk vertrouwensdiensten in de zin van deze verordening. Voor zover deze instellingen dit soort diensten niet aanbieden, laat deze verordening hun werkzaamheden onverlet.

(34) Elektronisch registers zijn een opeenvolging van elektronische gegevensbestanden die de integriteit en de nauwkeurigheid van de chronologische volgorde daarvan waarborgen. Het doel van elektronisch registers bestaat erin een chronologische opeenvolging van gegevensbestanden vast te leggen die verhindert dat digitale activa worden gekopieerd en aan meerdere ontvangers worden verkocht. Elektronisch registers kunnen bijvoorbeeld worden gebruikt voor digitale bestanden betreffende eigendom op het gebied van de wereldhandel, de financiering van toeleveringsketens, de digitalisering van intellectuele-eigendomsrechten of goederen zoals elektriciteit. In combinatie met andere technologieën kunnen zij mede oplossingen bieden voor efficiëntere en transformatieve overheidsdiensten zoals elektronisch stemmen, grensoverschrijdende douanesamenwerking, grens-overschrijdende samenwerking tussen academische instellingen, of eigendomsregistratie van vastgoed bij gedecentraliseerde grondkadasters. Gekwalificeerde elektronisch registers scheppen een rechtsvermoeden voor de unieke en accurate chronologische volgorde en integriteit van de gegevensbestanden in het register. De specifieke attributen van elektronisch registers, namelijk de chronologische volgorde van gegevensbestanden, onderscheiden elektronisch registers van andere vertrouwensdiensten zoals elektronische tijdstempels en diensten voor elektronisch aangetekende bezorging. Immers, een tijdstempel of een digitaal document, of de overdracht ervan door middel van diensten voor elektronisch aangetekende bezorging, kunnen zonder verdere technische of organisatorische maatregelen onvoldoende verhinderen dat dezelfde digitale activa worden gekopieerd en meerdere malen aan verschillende partijen worden verkocht. Het aanmaken en actualiseren van een elektronisch register hangt af van het type register (centraal of decentraal).

(35) Om versnippering van de interne markt te voorkomen, moet een pan-Europees rechtskader worden vastgesteld aan de hand waarvan vertrouwensdiensten die gegevens in gekwalificeerde elektronische registers opslaan, grensoverschrijdend kunnen worden erkend. Vertrouwensdiensten van elektronisch registers moeten tot taak krijgen zich van de chronologische volgorde van de gegevensbestanden in het register te vergewissen. Deze verordening laat elke wettelijke verplichting die gebruikers krachtens het recht van de Unie of het nationale recht moeten naleven, onverlet. Praktijkvoorbeelden waarbij persoonsgegevens worden verwerkt, bijvoorbeeld, moeten voldoen aan Verordening (EU) 2016/679. Praktijkvoorbeelden die betrekking hebben op cryptoactiva, moeten verenigbaar zijn met alle toepasselijke financiële regels, met inbegrip van de richtlijn markten voor financiële instrumenten[9], de richtlijn betalingsdiensten[10], de richtlijn e-geld[11] en de toekomstige verordening betreffende markten in cryptoactiva alsook met de regelgeving betreffende de bestrijding van witwassen, die zou kunnen worden opgenomen in de verordening inzake geldovermakingen[12], en die aanbieders van cryptoactivadiensten zou kunnen verplichten om de identiteit van gebruikers van elektronische registers te verifiëren om te kunnen voldoen aan de internationale antiwitwasnormen.

---

9 Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).

10 Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35).

11 Richtlijn 2009/110/EG van het Europees Parlement en de Raad van 16 september 2009 betreffende de toegang tot, de uitoefening van en het prudentieel toezicht op de werkzaamheden van instellingen voor elektronisch geld, tot wijziging van de Richtlijnen 2005/60/EG en 2006/48/EG en tot intrekking van Richtlijn 2000/46/EG (PB L 267 van 10.10.2009, blz. 7).

12 Zie het voorstel van de Commissie van 20.7.2021 tot herschikking van Verordening (EU) 2015/847 van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie (COM(2021) 422 final).

(36) Om versnippering en obstakels ten gevolge van uiteenlopende normen en technische beperkingen te voorkomen, en om, door middel van een gecoördineerd proces, de toekomstige uitvoering van het Europese kader voor digitale identiteit niet in gevaar te brengen, moeten de Commissie, de lidstaten en de particuliere sector nauw en gestructureerd samenwerken. Daartoe moeten de lidstaten samenwerken binnen het kader van Aanbeveling XXX/XXXX van de Commissie [EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit][13] om een toolbox voor een Europees kader voor digitale identiteit op te stellen. De toolbox moet beschikken over een alomvattende technische architectuur en een referentiekader, gemeenschappelijke normen en technische referenties en richtsnoeren en beschrijvingen van beste praktijken, die ten minste alle aspecten van de functionaliteiten en de interoperabiliteit van de Europese portemonnee voor digitale identiteit, inclusief elektronische handtekeningen, omvatten, en van de gekwalificeerde vertrouwensdienst voor de attestering van attributen, zoals in deze verordening uiteengezet. In dit verband moeten de lidstaten ook overeenstemming bereiken over gemeenschappelijke elementen van een bedrijfsmodel en een vergoedingsstructuur van de Europese portemonnee voor digitale identiteit, zodat met name kleine en middelgrote ondernemingen in een grensoverschrijdende context eenvoudiger kunnen deelnemen. De inhoud van de toolbox moet worden ontwikkeld in samenhang met en een afspiegeling zijn van het resultaat van de discussie over en het proces van goedkeuring van het Europese kader voor digitale identiteit.

(36a) De lidstaten moeten regels vaststellen over sancties voor inbreuken zoals rechtstreekse of onrechtstreekse praktijken die leiden tot verwarring tussen niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten, of tot misbruik van het vertrouwensmerk van de EU door aanbieders van niet-gekwalificeerde vertrouwensdiensten. Het vertrouwensmerk van de EU mag niet worden gebruik in omstandigheden die rechtstreeks of onrechtstreeks de indruk kunnen wekken dat niet-gekwalificeerde vertrouwensdiensten van een aanbieder gekwalificeerd zijn.

---

13 [voeg referentie in na vaststelling]

(36b) Deze verordening moet een geharmoniseerd niveau inzake kwaliteit, betrouwbaarheid en beveiliging van gekwalificeerde vertrouwensdiensten waarborgen, ongeacht de plek waar de werkzaamheden worden verricht. Het moet een aanbieder van gekwalificeerde vertrouwensdiensten toegestaan zijn eigen werkzaamheden in verband met het aanbieden van een gekwalificeerde vertrouwensdienst buiten de Unie uit te besteden, indien die dienst kan waarborgen dat toezichtsactiviteiten en audits kunnen worden gehandhaafd alsof de werkzaamheden in de Unie plaatsvinden. Indien de naleving van de verordening niet volledig gewaarborgd is, moeten de toezichthoudende organen evenredige en gerechtvaardigde maatregelen kunnen nemen, waaronder de intrekking van de kwalificatiestatus van de geboden vertrouwensdienst.

(36c) Om de rechtszekerheid te waarborgen wat betreft de geldigheid van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten, is het van essentieel belang de componenten van een geavanceerde gekwalificeerde elektronische handtekening op basis van gekwalificeerde certificaten te specificeren; die moeten worden beoordeeld door de vertrouwende partij die de validering van die handtekening uitvoert.

(36d) Aanbieders van vertrouwensdiensten moeten cryptografische algoritmen gebruiken die sporen met de beste praktijken en een betrouwbare toepassing van deze algoritmes weerspiegelen, teneinde de veiligheid en de betrouwbaarheid van hun vertrouwensdiensten te garanderen.

(36e) Deze verordening moet een aanbieder van gekwalificeerde vertrouwensdiensten verplichten om op basis van diverse in de EU geharmoniseerde methoden, de identiteit te verifiëren van een natuurlijke persoon of rechtspersoon aan wie het gekwalificeerde certificaat wordt afgegeven. Die methode kan inhouden dat hij zich bedient van elektronisch identificatiemiddelen die voldoen aan betrouwbaarheidsniveau "aanzienlijk", in combinatie met aanvullende geharmoniseerde procedures op afstand die met een hoog niveau van vertrouwen de identificatie van de persoon garanderen.

(36f) Verstrekkers van Europese portemonnees voor digitale identiteit en van aangemelde elektronische identificatiemiddelen die handelen in een commerciële of professionele hoedanigheid en gebruikmaken van kernplatformdiensten die worden aangeboden door poortwachters met het oog op of tijdens het verlenen van diensten aan eindgebruikers, moeten worden beschouwd als zakelijke gebruikers in de zin van artikel 2, punt 21, van Verordening (EU) 2022/1925. De poortwachters moeten daarom worden verplicht om kosteloos te zorgen voor effectieve interoperabiliteit met en, ten behoeve van interoperabiliteit, toegang tot dezelfde besturingssystemen, hardware en software als die welke beschikbaar zijn of worden gebruikt bij het aanbieden van hun eigen complementaire en ondersteunende diensten en hardware. Dit moet verstrekkers van Europese portemonnees voor digitale identiteit en van aangemelde elektronische identificatiemiddelen in staat stellen via interfaces of soortgelijke oplossingen even doeltreffend aan te sluiten op de betrokken functionaliteiten als op de diensten of hardware van de poortwachters zelf.

(36g) Om deze verordening in overeenstemming te houden met de huidige ontwikkelingen en aan te sluiten bij de praktijken van de interne markt, moeten de door de Commissie vastgestelde uitvoeringshandelingen regelmatig worden geëvalueerd en zo nodig worden geactualiseerd. Bij het beoordelen van de noodzaak van deze actualiseringen moet rekening worden gehouden met nieuwe technologieën, praktijken, normen of technische specificaties die op de markt hun intrede hebben gedaan.

(37) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1525 van het Europees Parlement en de Raad[14].

(38) Verordening (EU) 910/2014 moet daarom dienovereenkomstig worden gewijzigd,

---

[14] Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Verordening (EU) 910/2014 wordt als volgt gewijzigd:

1) artikel 1 wordt vervangen door:

"Deze verordening is gericht op het goede functioneren van de interne markt, en op het bieden van een adequaat niveau van beveiliging van elektronische identificatiemiddelen en vertrouwensdiensten. Daartoe wordt bij deze verordening het volgende vastgesteld:

a bis) de voorwaarden waaronder de lidstaten elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen aanbieden en erkennen die onder een aangemeld stelsel voor elektronische identificatie van een andere lidstaat vallen,

a ter) de voorwaarden waaronder de lidstaten Europese portemonnees voor digitale identiteit verstrekken en erkennen;

b) regels voor vertrouwensdiensten, met name voor elektronische transacties,

c) een juridisch kader voor elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, diensten voor elektronisch aangetekende bezorging, certificatendiensten voor websiteauthenticatie, elektronische validering van elektronische handtekeningen, elektronische zegels en de certificaten daarvoor, elektronische validering van certificaten voor website-authenticatie, elektronische bewaring van elektronische handtekeningen, elektronische zegels en de certificaten daarvoor, elektronische archivering, elektronische attestering van attributen, het beheer van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand, en elektronische registers.";

2) artikel 2 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Deze verordening is van toepassing op stelsels voor elektronische identificatie die zijn aangemeld door een lidstaat, op door de lidstaten verstrekte Europese portemonnees voor digitale identiteit en op verleners van vertrouwensdiensten die in de Unie zijn gevestigd.";

b) lid 3 wordt vervangen door:

"3. Deze verordening doet geen afbreuk aan nationaal of Unierecht dat betrekking heeft op de totstandkoming en geldigheid van contracten of andere wettelijke of procedurele vormverplichtingen dan wel sectorspecifieke vormvereisten.";

3) artikel 3 wordt als volgt gewijzigd:

(X) punt 1 wordt vervangen door:

"1. "elektronische identificatie": het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een natuurlijke persoon of rechtspersoon vertegenwoordigt, op unieke wijze aanduiden;";

a) punt 2 wordt vervangen door:

"2. "elektronisch identificatiemiddel": een materiële en/of immateriële eenheid, inclusief Europese portemonnees voor digitale identiteit, die persoons-identificatiegegevens bevat en voor authenticatie bij een onlinedienst of, in voorkomend geval, een offlinedienst wordt gebruikt;";

aa) punt 3 wordt vervangen door:

"3. "persoonsidentificatiegegevens": een overeenkomstig het Unierecht of het nationale recht uitgegeven reeks gegevens, aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of van een natuurlijke persoon die een natuurlijke persoon of rechtspersoon vertegenwoordigt, kan worden vastgesteld;";

b) punt 4 wordt vervangen door:

"4. "stelsel voor elektronische identificatie": een stelsel voor elektronische identificatie waarbinnen elektronische identificatiemiddelen worden uitgegeven aan natuurlijke personen, rechtspersonen of natuurlijke personen die natuurlijke personen of rechtspersonen vertegenwoordigen;";

ba) punt 5 wordt vervangen door:

"5. "authenticatie": een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt;";

bb) het volgende punt wordt ingevoegd:

"5 bis. "gebruiker": een natuurlijke of rechtspersoon, of een natuurlijke persoon die een natuurlijke persoon of rechtspersoon vertegenwoordigt, en die gebruikmaakt van overeenkomstig deze verordening verleende vertrouwensdiensten of verstrekte elektronische identificatiemiddelen;";

c) punt 14 wordt vervangen door:

"14. "certificaat voor elektronische handtekeningen": een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt;";

d) punt 16 wordt vervangen door:

"16. "vertrouwensdienst": een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:

a) het uitgeven van certificaten voor elektronische handtekeningen, certificaten voor elektronische zegels, certificaten voor websiteauthenticatie of certificaten voor het verlenen van andere vertrouwensdiensten;

a bis) het valideren van certificaten voor elektronische handtekeningen, certificaten voor elektronische zegels, certificaten voor websiteauthenticatie of certificaten voor het verlenen van andere vertrouwensdiensten;

b) het aanmaken van elektronische handtekeningen of elektronische zegels;

c) het valideren van elektronische handtekeningen of elektronische zegels;

d) het bewaren van elektronische handtekeningen, elektronische zegels, certificaten voor elektronische handtekeningen of certificaten voor elektronische zegels;

e) het beheer van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen op afstand of gekwalificeerde middelen voor het aanmaken van elektronische zegels op afstand;

f) het uitgeven van elektronische attesteringen van attributen;

f bis) het valideren van elektronische attesteringen van attributen;

g) het aanmaken van elektronische tijdstempels;

g bis) het valideren van elektronische tijdstempels;

g ter) het verlenen van diensten voor elektronisch aangetekende bezorging;

g quater) het valideren van gegevens die via diensten voor elektronisch aangetekende bezorging zijn verzonden en het bewijs daarvoor;

h) het elektronisch archiveren van elektronische gegevens; of

i) het opslaan van elektronische gegevens in elektronische registers.";

da) punt 18 wordt vervangen door:

"18. "conformiteitsbeoordelingsinstantie": een instantie als omschreven in artikel 2, punt 13, van Verordening (EG) nr. 765/2008, die in overeenstemming met die verordening is geaccrediteerd om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten, of om Europese portemonnees voor digitale identiteit of elektronische identificatiemiddelen te certificeren;";

e) punt 21 wordt vervangen door:

"21. "product": software of hardware, of relevante componenten van hardware en/of software, die bedoeld zijn om te worden gebruikt voor de verlening van elektronische identificatie- en vertrouwensdiensten;";

f) de volgende punten worden ingevoegd:

"23 bis. "gekwalificeerd middel voor het aanmaken van elektronische handtekeningen op afstand": een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen dat overeenkomstig artikel 29 bis namens een ondertekenaar wordt beheerd door een gekwalificeerde verlener van vertrouwensdiensten;

23 ter. "gekwalificeerd middel voor het aanmaken van elektronische zegels op afstand": een gekwalificeerd middel voor het aanmaken van elektronische zegels dat overeenkomstig artikel 39 bis namens een zegelaanmaker wordt beheerd door een gekwalificeerde verlener van vertrouwensdiensten;";

g) punt 29 wordt vervangen door:

"29. "certificaat voor elektronische zegels": een elektronische attestering die valideringsgegevens van elektronische zegels aan een rechtspersoon verbindt en de naam van die rechtspersoon bevestigt;";

h) punt 41 wordt vervangen door:

"41. "validering": proces waarmee wordt nagegaan of, en bevestigd dat gegevens in elektronische vorm volgens de vereisten van deze verordening geldig zijn;";

i) de volgende punten worden toegevoegd:

"42. "Europese portemonnee voor digitale identiteit": een elektronisch identificatiemiddel dat gebruikers in staat stelt identiteitsgegevens, waaronder persoonsidentificatiegegevens, en elektronische attesteringen van attributen met betrekking tot hun identiteit op te slaan en op te vragen, op verzoek aan vertrouwende partijen te verstrekken, en voor online en, indien passend, offline authenticatie voor een dienst overeenkomstig artikel 6 bis te gebruiken, en dat ondertekening middels gekwalificeerde elektronische handtekeningen en verzegeling middels gekwalificeerde elektronische zegels mogelijk maakt;";

43. "attribuut": aanduiding van de eigenschap, kwaliteit, rechten of toestemming van een natuurlijke persoon of rechtspersoon of van een voorwerp;

44. "elektronische attestering van attributen": een attestering in elektronisch formaat aan de hand waarvan attributen kunnen worden geauthenticeerd;

45. "gekwalificeerde elektronische attestering van attributen": een elektronische attestering van attributen die is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage V;

45 bis. "elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron": een elektronische attestering van attributen uitgegeven door een openbare instantie die verantwoordelijk is voor een authentieke bron of door een openbare instantie die door de lidstaat is aangewezen voor het uitgeven van dergelijke attesteringen van attributen namens de openbare instanties die verantwoordelijk zijn voor authentieke bronnen overeenkomstig artikel 45 quinquies bis en die voldoen aan de eisen van bijlage VII;

46. "authentieke bron": een register of systeem, onder de verantwoordelijkheid van een openbare instantie of particuliere entiteit, dat attributen omtrent een natuurlijke persoon of rechtspersoon bevat en verstrekt, en als een primaire bron van die informatie wordt beschouwd of krachtens Unierecht of nationaal recht, met inbegrip van de bestuursrechtelijke praktijken, als authentiek wordt erkend;

47. "elektronische archivering": een dienst die de ontvangst, opslag, opvraging en verwijdering van elektronische gegevens verzorgt om de duurzaamheid en leesbaarheid ervan te garanderen alsook de integriteit, de vertrouwelijkheid en het bewijs van de oorsprong ervan gedurende de volledige bewaartermijn te vrijwaren;

48. "gekwalificeerde elektronische archiveringsdienst": een elektronische archiveringsdienst die voldoet aan de eisen die zijn vastgelegd in artikel 45 octies bis;

49. "EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit": een verifieerbare eenvoudige, herkenbare en duidelijke indicatie dat een Europese portemonnee voor digitale identiteit is verstrekt overeenkomstig deze verordening;

50. "sterke gebruikersauthenticatie": een authenticatie op basis van ten minste twee authenticatiefactoren uit verschillende categorieën, hetzij kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker bezit) of een inherente eigenschap (iets wat de gebruiker is) die los van elkaar staan, zodat een inbreuk op een ervan de betrouwbaarheid van de andere niet in gevaar brengt, en die zo zijn ontworpen dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd;

53. "elektronisch register": een opeenvolging van elektronische gegevensbestanden die de integriteit en de nauwkeurigheid van de chronologische volgorde daarvan waarborgt;

53 bis. "gekwalificeerd elektronisch register": een elektronisch register dat voldoet aan de eisen die zijn vastgelegd in artikel 45 decies;

54. "persoonsgegevens": alle informatie als gedefinieerd in artikel 4, punt 1, van Verordening (EU) 2016/679;

55. "matching van bestanden": een proces waarbij persoonsidentificatiegegevens, persoonsidentificatiemiddelen, gekwalificeerde elektronische attestering van attributen of attesteringen van attributen uitgegeven door of namens een publiekrechtelijk orgaan dat verantwoordelijk is voor een authentieke bron, met een bestaande account van dezelfde persoon worden gematcht of gekoppeld;

55 bis. "unieke en permanente identificatiecode": een identificatiecode die uit één of meer nationale of sectorale identificatiegegevens kan bestaan, met één gebruiker verbonden is en permanent is;

55 ter. "gegevensbestand": elektronische gegevens die samen met daaraan gerelateerde metagegevens (of attributen) zijn opgeslagen ter ondersteuning van de verwerking van de gegevens.

55 quater. "offlinegebruik van Europese portemonnees voor digitale identiteit": interactie tussen een gebruiker en een vertrouwende partij op een fysieke locatie, waarbij de portemonnee geen toegang tot systemen op afstand via elektronische communicatienetwerken hoeft te hebben ten behoeve van de interactie.";

"*Artikel 5*

Pseudoniemen in elektronische transacties

Onverminderd het rechtsgevolg dat aan het gebruik van pseudoniemen op grond van nationaal recht wordt toegekend, wordt het gebruik ervan in elektronische transacties niet verboden.";

5) in hoofdstuk II wordt vóór artikel 6 bis wordt het volgende opschrift ingevoegd:

"AFDELING I

Europese portemonnee voor digitale identiteit";

7) de volgende artikelen worden ingevoegd:

"*Artikel 6 bis*

Europese portemonnees voor digitale identiteit

1. Opdat alle natuurlijke personen en rechtspersonen in de Unie veilige, betrouwbare en naadloze grensoverschrijdende toegang tot publieke en particuliere diensten krijgen, zorgen alle lidstaten ervoor dat binnen 24 maanden na de inwerkingtreding van de in lid 11 en in artikel 6 quater, lid 4, bedoelde uitvoeringshandelingen een Europese portemonnee voor digitale identiteit wordt verstrekt.

2. Europese portemonnees voor digitale identiteit worden verstrekt:

   a) door een lidstaat;

   b) krachtens een mandaat van een lidstaat; of

   c) onafhankelijk van een lidstaat, maar erkend door een lidstaat.

3. Een Europese portemonnee voor digitale identiteit is een elektronisch identificatiemiddel waarmee gebruikers op een transparante en door hen traceerbare wijze:

   a) veilig elektronische attesteringen van attributen en persoonsidentificatie-gegevens kunnen aanvragen, selecteren, combineren, opslaan, verwijderen en aanbieden aan vertrouwende partijen, en zich online en, indien passend, offline kunnen authenticeren, zodat zij openbare en particuliere onlinediensten kunnen gebruiken, waarbij ervoor wordt gezorgd dat een selectieve openstelling van gegevens mogelijk is;

   b) middels gekwalificeerde elektronische handtekeningen kunnen ondertekenen en middels gekwalificeerde elektronische zegels kunnen verzegelen.

4. Europese portemonnees voor digitale identiteit moeten in het bijzonder:

a) een gemeenschappelijke reeks interfaces bieden:

1) voor het uitgeven van persoonsidentificatiegegevens, gekwalificeerde en niet-gekwalificeerde elektronische attesteringen van attributen of gekwalificeerde en niet-gekwalificeerde certificaten aan de Europese portemonnee voor digitale identiteit;

2) voor vertrouwende partijen om persoonsidentificatiegegevens en elektronische attesteringen van attributen aan te vragen;

3) om online en, indien passend, ook offline persoonsidentificatiegegevens of elektronische attestering van attributen aan vertrouwende partijen aan te bieden;

4) voor de gebruiker om met de Europese portemonnee voor digitale identiteit te kunnen communiceren en een "EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit" te kunnen weergeven;

b) verleners van vertrouwensdiensten van elektronische attesteringen van attributen geen informatie verstrekken over het gebruik van die attributen nadat deze zijn uitgegeven;

b bis) ervoor zorgen dat de identiteit van vertrouwende partijen kan worden gevalideerd door de toepassing van authenticatiemechanismen overeenkomstig artikel 6 ter;

c) aan de voorwaarden van artikel 8 voldoen wat het betrouwbaarheidsniveau "hoog" betreft, dat van overeenkomstige toepassing is op het beheer en het gebruik van persoonsidentificatiegegevens in de hele portemonnee, met inbegrip van elektronische identificatie en authenticatie;

e) waarborgen dat de in artikel 12, lid 4, punt d), bedoelde persoonsidentificatiegegevens de met de portemonnee verbonden natuurlijke persoon, rechtspersoon of natuurlijke persoon die de natuurlijke persoon of rechtspersoon vertegenwoordigt, op unieke wijze en permanent aanduiden.

4 bis. De lidstaten voorzien in procedures om de gebruiker in staat te stellen mogelijk verlies of misbruik van zijn portemonnee te melden en om intrekking ervan te verzoeken.

5. De lidstaten voorzien in valideringsmechanismen voor de Europese portemonnees voor digitale identiteit, zodat:

a) de authenticiteit en de geldigheid ervan kunnen worden geverifieerd;

d) de gebruiker vertrouwende partijen kan authenticeren overeenkomstig artikel 6 ter;

6. De Europese portemonnees voor digitale identiteit worden uitgegeven op grond van een aangemeld stelsel voor elektronische identificatie met een "hoog" betrouwbaarheidsniveau.

6 bis. Het uitgeven, gebruiken voor authenticatie en intrekken van Europese portemonnees voor digitale identiteit is gratis voor natuurlijke personen.

6 ter. Onverminderd artikel 6 quinquies ter kunnen de lidstaten overeenkomstig het nationale recht in extra functies van de Europese portemonnees voor digitale identiteit voorzien, waaronder interoperabiliteit met bestaande nationale eID-middelen.

7. De gebruikers hebben volledige controle over het gebruik van de Europese portemonnee voor digitale identiteit en van de gegevens in hun Europese portemonnee voor digitale identiteit. De afgever van de Europese portemonnee voor digitale identiteit verzamelt geen informatie over het gebruik van de portemonnee die niet noodzakelijk is voor de levering van de portemonneediensten, noch combineert hij persoonsidentificatiegegevens en andere persoonsgegevens die zijn opgeslagen of betrekking hebben op het gebruik van de Europese portemonnee voor digitale identiteit met persoonsgegevens van andere door deze afgever of derden aangeboden diensten als die niet noodzakelijk zijn voor de levering van de portemonneediensten, tenzij de gebruiker daar uitdrukkelijk om heeft gevraagd. Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnees voor digitale identiteit worden logisch gescheiden van andere door de afgever van Europese portemonnees voor digitale identiteit opgeslagen gegevens. Indien de Europese portemonnee voor digitale identiteit wordt verstrekt door particuliere partijen overeenkomstig lid 2, punten b) en c), is artikel 45 septies, lid 4, van overeenkomstige toepassing.

7 bis. De lidstaten stellen de Commissie onverwijld in kennis van informatie over:

a) de instantie die verantwoordelijk is voor het opstellen en bijhouden van de lijst van aangemelde vertrouwende partijen die de Europese portemonnees voor digitale identiteit gebruiken, overeenkomstig artikel 6 ter, lid 2;

b) de instanties die verantwoordelijk zijn voor de verstrekking van de Europese portemonnees voor digitale identiteit, overeenkomstig artikel 6 bis, lid 1;

c) de instanties die ervoor moeten zorgen dat de persoonsidentificatiegegevens worden verbonden met de portemonnee, overeenkomstig artikel 6 bis, lid 4, punt e);

De kennisgeving bevat ook informatie over het mechanisme voor de validering van de in artikel 12, lid 4, bedoelde persoonsidentificatiegegevens en van de identiteit van de vertrouwende partijen.

De Commissie maakt via een beveiligd kanaal de in dit lid bedoelde informatie in elektronisch ondertekende of verzegelde en voor automatische verwerking geschikte vorm publiek beschikbaar.

8. Artikel 11 is van overeenkomstige toepassing op de Europese portemonnee voor digitale identiteit.

9. Artikel 24, lid 2, punten b), e), g), en h), is van overeenkomstige toepassing op de afgever van Europese portemonnees voor digitale identiteit.

10. De Europese portemonnee voor digitale identiteit wordt toegankelijk gemaakt voor personen met een handicap overeenkomstig de toegankelijkheidsvoorschriften van Richtlijn (EU) 2019/882.

11. Binnen zes maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de Europese portemonnee voor digitale identiteit technische en operationele specificaties en referentienormen inzake de in de leden 3, 4, 5 en 7 bis bedoelde voorschriften vast. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

11 bis. De Commissie stelt technische en operationele specificaties alsook referentienormen vast met het oog op het vergemakkelijken van de instap in de Europese portemonnee voor digitale identiteit voor gebruikers die gebruikmaken van hetzij elektronische identificatiemiddelen van betrouwbaarheidsniveau "hoog" hetzij elektronische identificatiemiddelen van betrouwbaarheidsniveau "aanzienlijk" in combinatie met extra instapprocedures op afstand die samen aan de eisen van het betrouwbaarheidsniveau "hoog" voldoen. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 6 ter

Vertrouwende partijen voor Europese portemonnees voor digitale identiteit

1. Indien vertrouwende partijen die particuliere of openbare diensten verlenen, voornemens zijn om overeenkomstig deze verordening afgegeven Europese portemonnees voor digitale identiteit te gebruiken, geven zij daarvan kennis aan de lidstaat waar de vertrouwende partijen zijn gevestigd.

1 bis. De kennisgevingsprocedure is kosteneffectief en evenredig met het risico en zorgt ervoor dat vertrouwende partijen ten minste de informatie verstrekken die nodig is om zich te authenticeren voor Europese portemonnees voor digitale identiteit. Dit omvat ten minste de lidstaat waar zij zijn gevestigd en de naam van de vertrouwende partij en, indien van toepassing, haar registratienummer zoals vermeld in de officiële registers.

1 ter. De kennisgevingsvereiste doet geen afbreuk aan andere kennisgevings- en registratievereisten overeenkomstig het Unierecht of het nationale recht, zoals die welke van toepassing zijn op bijzondere categorieën persoonsgegevens, waarvoor aanvullende authorisatievereisten nodig kunnen zijn.

1 quater. De lidstaten kunnen vertrouwende partijen vrijstellen van de kennisgevings-vereiste indien het Unierecht of het nationale recht niet voorziet in specifieke kennisgevings- of registratievereisten om toegang te krijgen tot informatie die via de Europese portemonnee voor digitale identiteit wordt verstrekt. Het is mogelijk dat de vrijgestelde vertrouwende partijen zich niet hoeven te authenticeren bij de Europese portemonnee voor digitale identiteit.

1 quinquies. Overeenkomstig dit artikel aangemelde vertrouwende partijen stellen de lidstaat onverwijld in kennis van eventuele latere wijzigingen in de oorspronkelijk verstrekte informatie.

2. Vertrouwende partijen zien toe op de toepassing van de in artikel 6 bis, lid 4, punt b bis), bedoelde authenticatiemechanismen.

3. Vertrouwende partijen zijn verantwoordelijk voor de uitvoering van de procedure voor de authenticatie van personen en de validering van de elektronische attestering van attributen uit Europese portemonnees voor digitale identiteit die overeenkomstig artikel 6 bis, lid 4, punt a), 2), zijn verkregen via de gemeenschappelijke interface.

4. Binnen zes maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de Europese portemonnees voor digitale identiteit in de zin van artikel 6 bis, lid 11, technische en operationele specificaties voor de in de leden 1, 1 bis en 1 quinquies bedoelde voorschriften vast. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 6 quater

Certificering van de Europese portemonnees voor digitale identiteit

1. De conformiteit van Europese portemonnees voor digitale identiteit met de eisen van artikel 6 bis, leden 3, 4 en 5, met de eis inzake logische scheiding van artikel 6 bis, lid 7, en indien van toepassing met de eisen van artikel 6 bis, lid 11 bis, wordt gecertificeerd door conformiteitsbeoordelingsinstanties die zijn geaccrediteerd overeenkomstig artikel 60 van de cyberbeveiligingsverordening en overeenkomstig de regelingen, specificaties, normen en procedures waarnaar wordt verwezen overeenkomstig lid 4, punten a), a bis) en a bis bis), en die zijn aangewezen door de lidstaten. De certificering duurt niet langer dan vijf jaar, op voorwaarde dat de kwetsbaarheden regelmatig gedurende twee jaar worden beoordeeld. Indien kwetsbaarheden worden vastgesteld en niet binnen drie maanden worden verholpen, wordt de certificering geannuleerd.

2. Wat betreft de naleving van de gegevensbeschermingsvoorschriften van artikel 6 bis, lid 7, kan de certificering uit hoofde van lid 1 worden aangevuld met een certificering overeenkomstig artikel 42 van Verordening (EU) 2016/679.

3. De conformiteit van de Europese portemonnees voor digitale identiteit, of delen daarvan, met de eisen van artikel 6 bis, leden 3, 4, 5 en 7, en indien van toepassing 11 bis, die betrekking hebben op cyberbeveiliging, worden door de in lid 1 bedoelde conformiteitsbeoordelingsinstanties gecertificeerd volgens relevante regelingen voor cyberbeveiligingscertificering overeenkomstig Verordening (EU) 2019/881, waarnaar wordt verwezen overeenkomstig lid 4, punten a) en a bis).

3 bis. De in de artikelen 7 en 9 bedoelde eisen zijn niet van toepassing op gecertificeerde Europese portemonnees voor digitale identiteit.

4. Binnen zes maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen het volgende vast:

a) een lijst van regelingen voor cyberbeveiligingscertificering overeenkomstig Verordening (EU) 2019/881, vereist voor de certificering van de Europese portemonnees voor digitale identiteit bedoeld in lid 3;

a bis) specificaties, procedures en referentienormen voor het gebruik ervan in het kader van de relevante regelingen voor cyberbeveiligingscertificering als bedoeld in punt a);

a bis bis) een lijst van specificaties, procedures en referentienormen tot vaststelling van gemeenschappelijke certificeringseisen die niet vallen onder de relevante regelingen voor cyberbeveiligingscertificering overeenkomstig Verordening (EU) 2019/881 met het oog op de in lid 1 bedoelde certificering om aan te tonen dat een Europese portemonnee voor digitale identiteit aan de eisen van lid 1 voldoet;

b) technische, procedurele, organisatorische en operationele specificaties voor de aanwijzing van conformiteitsbeoordelingsinstanties als bedoeld in lid 1 en, voor wat de krachtens punt a bis bis) vastgestelde certificeringsvoorschriften betreft, voor de monitoring en herziening van de certificeringsregelingen en de bijbehorende evaluatiemethoden die deze instanties gebruiken en de certificaten en certificeringsverslagen die zij afgeven;

5. De lidstaten verstrekken aan de Commissie de namen en adressen van de in lid 1 bedoelde openbare of private organen. De Commissie stelt deze informatie beschikbaar aan de lidstaten.

6. De in lid 4 bedoelde uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 6 quinquies

Bekendmaking van een lijst van gecertificeerde Europese portemonnees voor digitale identiteit

1. De lidstaten verstrekken de Commissie onverwijld informatie over de overeenkomstig artikel 6 bis verstrekte en door de in artikel 6 quater, lid 1, bedoelde organen gecertificeerde Europese portemonnees voor digitale identiteit. Zij stellen de Commissie er onverwijld van in kennis als de certificering wordt geannuleerd.

2. De Commissie stelt op basis van de ontvangen informatie een machineleesbare lijst op van gecertificeerde Europese portemonnees voor digitale identiteit op en publiceert en actualiseert deze lijst.

3. Binnen zes maanden na de inwerkingtreding van deze verordening legt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de Europese portemonnees voor digitale identiteit in de zin van artikel 6 bis, lid 11, de formaten en procedures voor de toepassing van de leden 1 en 2 vast. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 6 quinquies bis

Inbreuk op de beveiliging van de Europese portemonnees voor digitale identiteit

1. Indien Europese portemonnees voor digitale identiteit die overeenkomstig artikel 6 bis zijn verstrekt of de in artikel 6 bis, lid 5, punt a), d) of e), bedoelde valideringsmechanismen zijn geschonden of ten dele zijn aangetast, waardoor de betrouwbaarheid ervan of de betrouwbaarheid van andere Europese portemonnees voor digitale identiteit in gevaar komt, schort de afgever van de betrokken portemonnees onverwijld de afgifte en het gebruik van de Europese portemonnee voor digitale identiteit op. De lidstaat waar de betrokken portemonnees zijn verstrekt, stelt de lidstaten en de Commissie daarvan onverwijld in kennis. De afgever van de betrokken portemonnees of de lidstaat brengt de vertrouwende partijen en de gebruikers dienovereenkomstig op de hoogte.

2. Wanneer de in lid 1 bedoelde schending of aantasting verholpen is, herstelt de afgever van de portemonnee de afgifte en het gebruik van de Europese portemonnee voor digitale identiteit. De lidstaat waar de betrokken portemonnees zijn verstrekt, stelt de lidstaten en de Commissie onverwijld daarvan in kennis. De afgever van de betrokken portemonnees of de lidstaat stelt de vertrouwende partijen en de gebruikers onverwijld daarvan in kennis.

3. Indien de in lid 1 bedoelde schending of aantasting niet binnen drie maanden na de opschorting is verholpen, trekt de betrokken lidstaat de betreffende Europese portemonnee voor digitale identiteit terug en stelt hij de andere lidstaten en de Commissie daarvan in kennis. Indien de ernst van de inbreuk dat rechtvaardigt, wordt de Europese portemonnee voor digitale identiteit onverwijld teruggetrokken.

4. De Commissie maakt de overeenkomstige wijzigingen aan de in artikel 6 quinquies bedoelde lijst onverwijld bekend in het Publicatieblad van de Europese Unie.

5. Binnen zes maanden na de inwerkingtreding van deze verordening specificeert de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de Europese portemonnees voor digitale identiteit in de zin van artikel 6 bis, lid 11, de in de leden 1, 2 en 3 bedoelde nadere maatregelen. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 6 quinquies ter

Grensoverschrijdend gebruik van Europese portemonnees voor digitale identiteit

1. Indien de lidstaten elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereisen om toegang tot een door een openbare instantie aangeboden onlinedienst te krijgen, aanvaarden ze ook Europese portemonnees voor digitale identiteit die overeenkomstig deze verordening voor authenticatie van de gebruiker zijn verstrekt.

2. Indien particuliere vertrouwende partijen die diensten verlenen, met uitzondering van micro-ondernemingen en kleine ondernemingen als gedefinieerd in Aanbeveling 2003/361/EG van de Commissie, krachtens nationaal of Unierecht, sterke gebruikersauthenticatie voor online-identificatie moeten gebruiken, of indien sterke gebruikersauthenticatie vereist is op grond van een contractuele verbintenis, waaronder op het gebied van vervoer, energie, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie, aanvaarden particuliere vertrouwende partijen, uiterlijk twaalf maanden na de datum van verstrekking van de Europese portemonnees voor digitale identiteit overeenkomstig artikel 6 bis, lid 1, zij het uitsluitend op vrijwillig verzoek van de gebruiker, ook het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig deze verordening zijn verstrekt voor de minimaal benodigde gegevens voor de specifieke onlinedienst waarvoor authenticatie van de gebruiker vereist is.

3. Indien zeer grote onlineplatforms, als gedefinieerd in artikel 25, lid 1, van Verordening [referentie verordening inzake digitale diensten] verlangen dat gebruikers zich authenticeren om toegang tot onlinediensten te krijgen, aanvaarden ze ook het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig deze verordening zijn verstrekt voor authenticatie van de gebruiker, zij het uitsluitend op vrijwillig verzoek van de gebruiker en met inachtneming van de minimaal benodigde gegevens voor de specifieke onlinedienst waarvoor authenticatie vereist is.

4. De Commissie stimuleert en faciliteert in samenwerking met de lidstaten dat gedragscodes worden ontwikkeld om bij te dragen aan de brede beschikbaarheid en bruikbaarheid van Europese portemonnees voor digitale identiteit binnen het toepassingsgebied van deze verordening. Deze gedragscodes vergemakkelijken brede aanvaarding van elektronische identificatiemiddelen, inclusief de Europese portemonnee voor digitale identiteit, binnen het toepassingsgebied van deze verordening, met name door dienstverleners die voor gebruikersauthenticatie gebruikmaken van elektronische identificatiediensten van derden. De Commissie faciliteert de ontwikkeling van dergelijke gedragscodes in nauwe samenwerking met alle belanghebbenden, en stimuleert dienstverleners om de ontwikkeling van de gedragscodes binnen 12 maanden na de vaststelling van deze verordening te voltooien en die binnen 18 maanden na de vaststelling van de verordening daadwerkelijk te implementeren.

5. De Commissie beoordeelt binnen 24 maanden na de invoering van de Europese portemonnee voor digitale identiteit of, op basis van bewijsmateriaal inzake de vraag naar en de beschikbaarheid en de bruikbaarheid van de Europese portemonnee voor digitale identiteit, aan extra particuliere aanbieders van onlinediensten zal worden opgelegd om, uitsluitend op vrijwillig verzoek van de gebruiker, het gebruik van de Europese portemonnee voor digitale identiteit te aanvaarden. De beoordelingscriteria hebben betrekking op de omvang van de gebruikersbasis, de grensoverschrijdende aanwezigheid van dienstverleners, technologische ontwikkelingen, de ontwikkeling van gebruikspatronen en de vraag van de consument.";

8) vóór artikel 7 wordt het volgende opschrift ingevoegd:

"AFDELING II

STELSELS VOOR ELEKTRONISCHE IDENTIFICATIE";

9) de inleidende zin van artikel 7 wordt vervangen door:

"Overeenkomstig artikel 9, lid 1, melden de lidstaten die zulks nog niet hebben gedaan, binnen 24 maanden na de inwerkingtreding van de in artikel 6 bis, lid 11, en artikel 6 quater, lid 4, bedoelde uitvoeringshandelingen ten minste één stelsel voor elektronische identificatie met inbegrip van ten minste één identificatiemiddel van betrouwbaarheidsniveau "hoog" aan. Een stelsel voor elektronische identificatie komt in aanmerking voor aanmelding overeenkomstig artikel 9, lid 1, indien aan alle onderstaande voorwaarden is voldaan:";

10) in artikel 9 worden de leden 2 en 3 vervangen door:

"2. De Commissie maakt in het Publicatieblad van de Europese Unie een lijst bekend van de stelsels voor elektronische identificatie die overeenkomstig lid 1 zijn aangemeld alsmede de hiermee verband houdende basisinformatie.

3. De Commissie maakt binnen één maand na de datum van ontvangst van die aanmelding de wijzigingen van de in lid 2 bedoelde lijst in het Publicatieblad van de Europese Unie bekend.";

12) het volgende artikel wordt ingevoegd:

"*Artikel 11 bis*

Matching van bestanden

1. Indien er voor authenticatie aangemelde elektronische identificatiemiddelen of Europese portemonnees voor digitale identiteit worden gebruikt, waarborgen de lidstaten, wanneer zij als vertrouwende partijen optreden, matching van bestanden.

2. Voor het verstrekken van Europese portemonnees voor digitale identiteit nemen de lidstaten in de minimale reeks persoonsidentificatiegegevens bedoeld in artikel 12, lid 4, punt d), ten minste één unieke en permanente identificatiecode op overeenkomstig het Unierecht en het nationale recht, om de gebruiker op hun verzoek te identificeren in die gevallen waarin gebruikersidentificatie wettelijk voorgeschreven is.

2 bis. De lidstaten voorzien in technische en organisatorische maatregelen om een hoog niveau van bescherming te waarborgen van persoonsgegevens die worden gebruikt om bestanden te matchen en om profilering van gebruikers te voorkomen.

2 bis bis. De lidstaten kunnen in overeenstemming met het nationale recht bepalen dat de gebruiker van de Europese portemonnee voor digitale identiteit kan verlangen dat een unieke en permanente identificatiecode die in de minimumreeks persoonsidentificatiegegevens is opgenomen en overeenkomstig artikel 6 bis, lid 4, punt e), met de portemonnee is verbonden, wordt vervangen door een andere unieke en permanente identificatiecode die wordt afgegeven door de lidstaat.

3. Binnen zes maanden na de inwerkingtreding van deze verordening specificeert de Commissie de in lid 1 bedoelde maatregelen door middel van een uitvoeringshandeling. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

3 bis. Binnen zes maanden na de inwerkingtreding van deze verordening beschrijft de Commissie de in de leden 2 en 2 bis bis bedoelde maatregelen nader door middel van een uitvoeringshandeling. Deze uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

13) artikel 12 wordt als volgt gewijzigd:

Samenwerking en interoperabiliteit

a) in lid 3 wordt punt d) geschrapt;

b) in lid 4 wordt punt d) vervangen door:

"d) een verwijzing naar een minimale reeks persoonsidentificatiegegevens die nodig is om een natuurlijke persoon, rechtspersoon of natuurlijke persoon die natuurlijke personen of rechtspersonen vertegenwoordigt, aan te duiden;";

ba) aan lid 5 wordt het volgende punt toegevoegd:

"c) een vergelijkbare benadering ten aanzien van onlinediensten waarvoor het gebruik van overeenkomstig deze verordening verstrekte Europese portemonnees voor digitale identiteit wordt aanvaard.";

c) in lid 6 wordt punt a) vervangen door:

"a) de uitwisseling van informatie, ervaring en goede werkwijzen wat betreft stelsels voor elektronische identificatie en in het bijzonder wat betreft de technische vereisten inzake interoperabiliteit, matching van bestanden en betrouwbaarheidsniveaus;";

ca) aan lid 6 wordt het volgende punt toegevoegd:

"e) de uitwisseling van informatie, ervaring en goede werkwijzen en de verstrekking van richtsnoeren over de wijze waarop onlinediensten kunnen worden ontworpen, ontwikkeld en geïmplementeerd met het oog op het gebruik van de Europese digitale portemonnees.";

14) de volgende artikelen worden ingevoegd:

"*Artikel 12 bis*

Certificering van stelsels voor elektronische identificatie

1. De conformiteit van aan te melden stelsels voor elektronische identificatie met de eisen van deze verordening wordt gecertificeerd om aan te tonen dat die stelsels of delen daarvan voldoen aan de vereisten van artikel 8, lid 2, met betrekking tot de betrouwbaarheidsniveaus van stelsels voor elektronische identificatie in het kader van een relevante regeling voor cyberbeveiligingscertificering uit hoofde van Verordening (EU) 2019/881 of delen daarvan, voor zover het cyberbeveiligings-certificaat of delen daarvan voldoen aan de vereisten van artikel 8, lid 2, met betrekking tot de betrouwbaarheidsniveaus van stelsels voor elektronische identificatie. De certificering duurt niet langer dan vijf jaar, op voorwaarde dat de kwetsbaarheden regelmatig gedurende twee jaar worden beoordeeld. Indien kwetsbaarheden worden vastgesteld en niet binnen drie maanden worden verholpen, wordt de certificering geannuleerd.

   De certificering wordt overeenkomstig Verordening (EG) nr. 765/2008 verricht door geaccrediteerde openbare of private conformiteitsbeoordelingsinstanties die door de lidstaten zijn aangewezen.

2. De collegiale toetsing van de in artikel 12, lid 6, punt c), bedoelde stelsels voor elektronische identificatie geldt niet voor stelsels voor elektronische identificatie of delen daarvan die overeenkomstig lid 1 zijn gecertificeerd.

2 bis. Niettegenstaande lid 2 van dit artikel kunnen lidstaten een aanmeldende lidstaat om aanvullende informatie verzoeken over stelsels voor elektronische identificatie of delen daarvan die overeenkomstig lid 2 van dit artikel zijn gecertificeerd.

3. De lidstaten verstrekken aan de Commissie de namen en adressen van de in lid 1 bedoelde openbare of private instanties. De Commissie stelt deze informatie beschikbaar aan de lidstaten.

Artikel 12 ter

Toegang tot hardware- en softwarekenmerken

Afgevers van Europese portemonnees voor digitale identiteit van aangemelde elektronische identificatiemiddelen die handelen in een commerciële of professionele hoedanigheid en gebruikmaken van kernplatformdiensten als gedefinieerd in artikel 2, lid 2, van Verordening (EU) 2022/1925 met het oog op of tijdens het verlenen van diensten in verband met Europese portemonnees voor digitale identiteit en elektronische identificatiemiddelen aan eindgebruikers, zijn zakelijke gebruikers in de zin van artikel 2, punt 21, van Verordening (EU) 2022/1925.";

17) in artikel 13 wordt lid 1 vervangen door:

"1. Onverminderd lid 2 zijn verleners van vertrouwensdiensten aansprakelijk voor schade die opzettelijk of uit onachtzaamheid wordt veroorzaakt aan natuurlijke of rechtspersonen vanwege een niet-naleving van de verplichtingen krachtens deze verordening.

De bewijslast voor het aantonen van opzet of nalatigheid van een niet gekwalificeerde verlener van vertrouwensdiensten ligt bij de natuurlijke persoon of de rechtspersoon die zich op de in de eerste alinea bedoelde schade beroept.

De opzet of nalatigheid van een gekwalificeerde verlener van vertrouwensdiensten wordt vermoed tenzij die gekwalificeerde verlener van vertrouwensdiensten bewijst dat in de eerste alinea bedoelde schade is ontstaan zonder dat er sprake was van opzet of nalatigheid van die gekwalificeerde verlener van vertrouwensdiensten.";

18) artikel 14 wordt vervangen door:

"*Artikel 14*

Internationale aspecten

1. Vertrouwensdiensten verstrekt door in een derde land gevestigde verleners van vertrouwensdiensten of door een internationale organisatie worden rechtens erkend als gelijkwaardig aan gekwalificeerde vertrouwensdiensten verstrekt door gekwalificeerde, in de Unie gevestigde verleners van vertrouwensdiensten, indien de vertrouwensdiensten die afkomstig zijn uit het derde land of van de internationale organisatie worden erkend op grond van een uitvoeringsbesluit of van een overeenkomst tussen de Unie en het derde land of de internationale organisatie overeenkomstig artikel 218 van het Verdrag.

2. De in lid 1 bedoelde uitvoeringsbesluiten en overeenkomsten regelen dat de eisen die gelden voor gekwalificeerde verleners van vertrouwensdiensten die in de Unie zijn gevestigd en voor de gekwalificeerde vertrouwensdiensten die zij verlenen, worden nageleefd door de verleners van vertrouwensdiensten in het derde land of de internationale organisaties en bij de vertrouwensdiensten die zij verlenen. Derde landen en internationale organisaties moeten met name een vertrouwenslijst van erkende verleners van vertrouwensdiensten opstellen, bijhouden en bekendmaken.

   De in lid 1 bedoelde overeenkomsten regelen dat de gekwalificeerde vertrouwensdiensten die worden verleend door in de Unie gevestigde gekwalificeerde verleners van vertrouwensdiensten, worden erkend als wettelijk gelijkwaardig aan vertrouwensdiensten van verleners van vertrouwensdiensten in het derde land of de internationale organisatie waarmee de overeenkomst is gesloten.

3. De in lid 1 bedoelde uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

19) artikel 15 wordt vervangen door:

"*Artikel 15*

Toegankelijkheid voor personen met een handicap

Vertrouwensdiensten en voor de levering van die diensten gebruikte eindgebruikersproducten worden toegankelijk gemaakt voor personen met een handicap overeenkomstig de toegankelijkheidsvoorschriften van Richtlijn (EU) 2019/882 betreffende de toegankelijkheidsvoorschriften voor producten en diensten.";

20) artikel 17 wordt als volgt gewijzigd:

a) lid 4 wordt als volgt gewijzigd:

1) in lid 4 wordt punt c) vervangen door:

"c) de relevante nationale bevoegde organen van de betrokken lidstaten die overeenkomstig Richtlijn (EU) XXXX/XXXX [NIS2] zijn aangewezen, op de hoogte brengen van significante beveiligings-inbreuken of integriteitsverlies waarvan zij bij de uitvoering van hun taken kennis krijgen. Indien de significante beveiligingsinbreuken of het integriteitsverlies andere lidstaten betreft, stelt het toezicht-houdend orgaan het overeenkomstig Richtlijn (EU) XXXX/XXXX (NIS2) aangewezen centrale contactpunt van de betrokken lidstaat en de overeenkomstig artikel 17 van deze verordening in de overige betrokken lidstaten aangewezen toezichthoudende organen daarvan in kennis; Het in kennis hoogte gestelde toezichthoudende orgaan informeert het publiek, of eist dat de verlener van vertrouwens-diensten dat doet, indien het van oordeel is dat bekendmaking van de beveiligingsinbreuk of het integriteitsverlies in het algemeen belang is.";

2) punt f) wordt vervangen door:

"f) samenwerken met de overeenkomstig Verordening (EU) 2016/679 opgerichte bevoegde toezichthoudende autoriteiten en in het bijzonder deze instanties onverwijld informeren indien er regels inzake de bescherming van persoonsgegevens lijken te zijn overtreden, en over beveiligingsinbreuken die inbreuken op persoonsgegevens lijken te vormen;";

b) lid 6 wordt vervangen door:

"6. Elk toezichthoudend orgaan legt de Commissie jaarlijks uiterlijk op 31 maart een verslag voor over zijn hoofdactiviteiten in het voorgaande kalenderjaar.";

c) lid 8 wordt vervangen door:

"8. Binnen twaalf maanden na de inwerkingtreding van deze verordening neemt de Commissie richtsnoeren aan voor de uitoefening door de toezicht-houdende organen van de in lid 4 bedoelde taken en bepaalt zij door middel van volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgestelde uitvoeringshandelingen de formaten en procedures voor het in lid 6 bedoelde verslag vast.";

21) artikel 18 wordt als volgt gewijzigd:

a) de titel van artikel 18 wordt vervangen door:

"Wederzijdse bijstand en samenwerking";

b) lid 1 wordt vervangen door:

"1. Toezichthoudende organen werken samen met het oog op de uitwisseling van goede praktijken en informatie met betrekking tot het verlenen van vertrouwensdiensten.";

c) de volgende leden 4 en 5 worden toegevoegd:

"4. Toezichthoudende organen en nationale bevoegde instanties op grond van Richtlijn (EU) XXXX/XXXX van het Europees Parlement en de Raad [NIS2] werken samen en verlenen elkaar bijstand om te waarborgen dat verleners van vertrouwensdiensten voldoen aan de vereisten van deze verordening en van Richtlijn (EU) XXXX/XXXX [NIS2]. De toezichthoudende organen verzoeken nationale bevoegde autoriteiten op grond van Richtlijn (EU) XXXX/XXXX [NIS2] om toezichtmaatregelen uit te voeren om na te gaan of de verleners van vertrouwensdiensten voldoen aan de vereisten van Richtlijn XXXX/XXXX [NIS2]; om van de verleners van vertrouwensdiensten te eisen dat zij niet-naleving van die vereisten verhelpen; om de resultaten van toezichtactiviteiten in verband met verleners van vertrouwensdiensten tijdig te verstrekken; en om de toezichthoudende organen in kennis te stellen van overeenkomstig Richtlijn XXXX/XXXX [NIS2] gemelde incidenten.

5. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen de noodzakelijke procedureregels vast om de samenwerking tussen de in lid 1 bedoelde toezichthoudende organen te faciliteren. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

21a) het volgende artikel wordt ingevoegd:

"Artikel 19 bis

Eisen aan niet-gekwalificeerde verleners van vertrouwensdiensten

1. Een niet-gekwalificeerde verlener van vertrouwensdiensten die niet-gekwalificeerde vertrouwensdiensten verleent:

a) heeft passend beleid en treft overeenkomstige maatregelen om juridische, zakelijke, operationele en andere directe of indirecte risico's met betrekking tot de levering van de niet-gekwalificeerde vertrouwensdienst te beheersen. Onverminderd artikel 18 van Richtlijn (EU) XXXX/XXXX [NIS2] omvatten die maatregelen ten minste het volgende:

i) maatregelen inzake de registratie en instapprocedures voor een dienst;

ii) maatregelen inzake procedurele of administratieve controles;

iii) maatregelen inzake het beheer en de uitvoering van diensten.

b) stelt het toezichthoudend orgaan, de identificeerbare getroffen personen, het publiek indien dit van algemeen belang is en, indien van toepassing, andere relevante bevoegde organen, onverwijld en in elk geval uiterlijk 24 uur nadat hij er kennis van heeft genomen, in kennis van inbreuken of verstoringen in de verlening van de dienst of de uitvoering van de maatregelen bedoeld in punt a), i), ii) en iii), die een aanzienlijk effect hebben op de verleende vertrouwensdienst of op de daarin bijgehouden persoonsgegevens.

2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen de technische kenmerken van de in lid 1, punt a), bedoelde maatregelen vast. Die uitvoerings-handelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

22) artikel 20 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Gekwalificeerde verleners van vertrouwensdiensten worden minstens eens in de 24 maanden op hun kosten aan een audit door een conformiteits-beoordelingsinstantie onderworpen. Het doel van deze audit is te bevestigen dat de gekwalificeerde verleners van vertrouwensdiensten en de gekwalificeerde vertrouwensdiensten die door hen worden verleend, voldoen aan de in deze verordening en de in artikel 18 van Richtlijn (EU) XXXX/XXXX [NIS2] vastgestelde eisen. Gekwalificeerde verleners van vertrouwensdiensten dienen het conformiteitsbeoordelingsverslag binnen drie werkdagen na ontvangst in bij het toezichthoudend orgaan.";

aa) het volgende lid wordt ingevoegd:

"1 bis. De lidstaten kunnen erin voorzien dat gekwalificeerde verleners van vertrouwensdiensten het toezichthoudend orgaan vooraf in kennis stellen van geplande audits en de deelname daaraan van het toezichthoudend orgaan als waarnemer op verzoek toestaan.";

b) in lid 2 wordt de laatste zin vervangen door:

"Indien er sprake blijkt te zijn van een inbreuk op de regels voor de bescherming van persoonsgegevens brengt het toezichthoudend orgaan de bevoegde toezichthoudende autoriteiten op grond van Verordening (EU) 2016/679 onverwijld op de hoogte.";

c) de leden 3 en 4 worden vervangen door:

"3. Indien de gekwalificeerde verlener van vertrouwensdiensten de vereisten van deze verordening niet naleeft, eist het toezichthoudend orgaan dat deze de niet-naleving rechtzet, binnen een bepaalde tijdspanne, indien van toepassing.

Bij ontstentenis van een rechtzetting, indien van toepassing binnen een door het toezichthoudend orgaan bepaalde tijdspanne, kan het toezichthoudend orgaan, gelet op in het bijzonder de mate, de duur en de gevolgen van die niet-naleving, de status "gekwalificeerd" van die verlener of van de door hem verleende betrokken dienst intrekken.

3 bis. Indien het toezichthoudend orgaan er door de nationale bevoegde autoriteiten uit hoofde van Richtlijn (EU) XXXX/XXXX [NIS2] van in kennis wordt gesteld dat de gekwalificeerde verlener van vertrouwensdiensten geen van de in artikel 18 van Richtlijn (EU) XXXX/XXXX [NIS2] vastgestelde vereisten naleeft, kan het toezichthoudend orgaan, gelet op in het bijzonder de mate, de duur en de gevolgen van die niet-naleving, de status "gekwalificeerd" van die verlener of van de door hem verleende betrokken dienst intrekken.

3 ter. Indien het toezichthoudend orgaan er door de toezichthoudende autoriteiten uit hoofde van Verordening (EU) 2016/679 van in kennis wordt gesteld dat de gekwalificeerde verlener van vertrouwensdiensten geen van de vereisten van Verordening (EU) 2016/679 naleeft, kan het toezichthoudend orgaan, gelet op in het bijzonder de mate, de duur en de gevolgen van die niet-naleving, de status "gekwalificeerd" van die verlener of van de door hem verleende betrokken dienst intrekken.

3 quater. Het toezichthoudend orgaan stelt de gekwalificeerde verlener van vertrouwensdiensten in kennis van het feit dat zijn status van gekwalificeerde of de status van gekwalificeerde van de betrokken dienst is ingetrokken. Het toezichthoudend orgaan brengt het in artikel 22, lid 3, bedoelde orgaan daarvan op de hoogte met als doel de actualisering van de in artikel 22, lid 1, bedoelde vertrouwenslijsten, evenals de in Richtlijn XXXX [NIS2] bedoelde nationale bevoegde autoriteit.

4. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers van normen vast voor:

a) de accreditering van de conformiteitsbeoordelingsinstanties en voor het conformiteitsbeoordelingsverslag bedoeld in lid 1;

b) de auditvereisten volgens welke de conformiteitsbeoordelingsinstanties hun conformiteitsbeoordeling van de gekwalificeerde verleners van vertrouwensdiensten, bedoeld in lid 1, uitvoeren;

c) de conformiteitsbeoordelingsregelingen volgens welke de conformiteitsbeoordelingsinstanties de conformiteitsbeoordeling van de gekwalificeerde verleners van vertrouwensdiensten uitvoeren en het in lid 1 bedoelde verslag leveren.

Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

23) artikel 21 wordt als volgt gewijzigd:

"1. Indien verleners van vertrouwensdiensten het voornemen hebben gekwalificeerde vertrouwensdiensten te gaan verlenen, dienen zij bij het toezichthoudend orgaan een kennisgeving van hun voornemen in, evenals een door een conformiteitsbeoordelingsinstantie afgegeven conformiteits-beoordelingsverslag waarin wordt bevestigd dat is voldaan aan de vereisten van deze verordening en van artikel 18 van Richtlijn (EU) XXXX/XXXX [NIS2].

a) lid 2 wordt vervangen door:

"2. Het toezichthoudend orgaan verifieert of de verlener van vertrouwens-diensten en de door hem verleende vertrouwensdiensten overeenkomstig de in deze verordening vastgestelde eisen zijn, en in het bijzonder conform de eisen die worden gesteld aan gekwalificeerde verleners van vertrouwens-diensten en aan de gekwalificeerde vertrouwensdiensten die zij verlenen.

Om te controleren of de verlener van vertrouwensdiensten de eisen van artikel 18 van Richtlijn XXXX [NIS2] naleeft, verzoekt het toezichthoudend orgaan de bevoegde autoriteiten bedoeld in Richtlijn (EU) XXXX [NIS2] om toezichtmaatregelen ter zake uit te voeren en onverwijld en uiterlijk twee maanden na de ontvangst van dit verzoek door de in Richtlijn XXXX [NIS2] bedoelde bevoegde entiteiten informatie over de uitkomst te verstrekken. Indien de verificatie niet binnen twee maanden na de kennisgeving is afgerond, brengen de in Richtlijn XXXX [NIS2] bedoelde bevoegde autoriteiten het toezichthoudend orgaan op de hoogte van de redenen voor de vertraging en van de termijn waarbinnen de verificatie zal zijn afgerond.

Indien het toezichthoudend orgaan tot het oordeel komt dat de verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming zijn met de eisen van deze verordening, kent het toezichthoudend orgaan de status "gekwalificeerd" toe aan de verlener van vertrouwensdiensten en aan de door hem verleende vertrouwensdiensten en stelt het toezichthoudend orgaan het in artikel 22, lid 3, bedoelde orgaan hiervan in kennis, zodat de in artikel 22, lid 1, bedoelde vertrouwenslijsten bijgewerkt worden, en wel binnen drie maanden na kennisgeving overeenkomstig lid 1.

Indien de verificatie niet binnen drie maanden na de kennisgeving is afgerond, brengt het toezichthoudend orgaan de verlener van vertrouwensdiensten op de hoogte van de redenen voor de vertraging en van de termijn waarbinnen de verificatie afgerond zal zijn.";

b) lid 4 wordt vervangen door:

"4. Voor de toepassing van de leden 1 en 2 bepaalt de Commissie binnen twaalf maanden na de inwerkingtreding van deze verordening door middel van uitvoeringshandelingen de formaten en procedures voor de aanmelding en de verificatie. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

25) artikel 24 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Wanneer een gekwalificeerde verlener van vertrouwensdiensten een gekwalificeerd certificaat of een gekwalificeerde elektronische attestering van attributen afgeeft, moet hij de identiteit en in voorkomend geval de specifieke attributen verifiëren van de natuurlijke persoon of de rechtspersoon aan wie het gekwalificeerde certificaat of de gekwalificeerde elektronische attestering van attributen zal worden afgegeven.

De in de eerste alinea bedoelde informatie wordt door de gekwalificeerde verlener van vertrouwensdiensten geverifieerd, hetzij rechtstreeks, hetzij door een beroep te doen op een derde partij, op een van de volgende wijzen:

a) door middel van de Europese portemonnee voor digitale identiteit of een aangemelde elektronische identificatiemiddelen die voldoen aan de vereisten van artikel 8 wat betreft het betrouwbaarheidsniveau "hoog";

b) door middel van gekwalificeerde elektronische attesteringen van attributen of een certificaat van een gekwalificeerde elektronische handtekening of van een gekwalificeerd elektronisch zegel, afgegeven overeenkomstig punt a), c) of d);

c) door middel van andere identificatiemethoden ter waarborging van de identificatie van de persoon met een hoge niveau van vertrouwen, waarvan de overeenstemming wordt bevestigd door een conformiteitsbeoordelingsorgaan;

d) door de fysieke aanwezigheid van de natuurlijke persoon of van een gemachtigde vertegenwoordiger van de rechtspersoon volgens passende procedures en overeenkomstig nationaal recht.";

b) het volgende lid 1 bis wordt ingevoegd:

"1 bis. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen minimale technische specificaties, normen en procedures vast met betrekking tot de verificatie van de identiteit en de attributen overeenkomstig lid 1, punt c). Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

c) lid 2 wordt als volgt gewijzigd:

0) punt a) wordt als volgt gewijzigd:

"a) informeert het toezichthoudende orgaan ten minste één maand voor de doorvoering van een wijziging in de verlening van zijn gekwalificeerde vertrouwensdiensten of ten minste drie maanden in geval van een voornemen om deze activiteiten te staken. Het toezichthoudend orgaan kan om aanvullende informatie of het resultaat van een conformiteitsbeoordeling verzoeken alvorens toestemming te geven om de voorgenomen wijzigingen in de gekwalificeerde vertrouwensdiensten door te voeren. Indien de verificatie niet binnen drie maanden na de kennisgeving is afgerond, brengt het toezichthoudend orgaan de verlener van vertrouwens-diensten op de hoogte van de redenen voor de vertraging en van de termijn waarbinnen de verificatie zal zijn afgerond.";

1) de punten d) en e) worden vervangen door:

"d) verstrekt individueel aan personen die gebruik wensen te maken van een gekwalificeerde vertrouwensdienst duidelijke, volledige en gemakkelijk toegankelijke informatie in een voor het publiek toegankelijke plaats over de precieze voorwaarden betreffende het gebruik van die dienst, met inbegrip van eventuele beperkingen op het gebruik ervan, alvorens een contractuele verbintenis aan te gaan;

e) maakt gebruik van betrouwbare systemen en producten die beschermd zijn tegen wijziging en die de technische veiligheid en betrouwbaarheid waarborgen van de processen die zij ondersteunen, alsook van geschikte cryptografische algoritmen, sleutellengten en hashfuncties in de systemen, producten en processen die zij ondersteunen;";

2) de volgende nieuwe punten worden ingevoegd:

"f bis) heeft passend beleid en treft overeenkomstige maatregelen om juridische, zakelijke, operationele en andere directe of indirecte risico's met betrekking tot de levering van de gekwalificeerde vertrouwensdienst te beheersen. Onverminderd artikel 18 van Richtlijn (EU) XXXX/XXXX [NIS2] omvatten die maatregelen ten minste het volgende:

i) maatregelen inzake de registratie en instapprocedures voor een dienst;

ii) maatregelen inzake procedurele of administratieve controles;

iii) maatregelen inzake het beheer en de uitvoering van diensten.

f ter) stelt het toezichthoudend orgaan, de identificeerbare getroffen personen, andere relevante bevoegde organen indien van toepassing en, op verzoek van het toezichthoudend orgaan, het publiek indien dit van algemeen belang is, onverwijld en in elk geval uiterlijk 24 uur na het incident in kennis van inbreuken of verstoringen in de verlening van de dienst of de uitvoering van de maatregelen bedoeld in punt f bis, i), ii) en iii), die een aanzienlijk effect hebben op de verleende vertrouwensdienst of op de daarin bijgehouden persoonsgegevens.";

3) de punten g) en h) worden vervangen door:

"g) neemt passende maatregelen tegen vervalsing, diefstal of verduistering van gegevens, of het onrechtmatig wissen, wijzigen of ontoegankelijk maken van gegevens;

h) legt zo lang als nodig, nadat de gekwalificeerde verlener van vertrouwensdiensten zijn activiteiten heeft gestaakt, alle relevante informatie vast met betrekking tot de gegevens die de gekwalificeerde verlener van vertrouwensdiensten heeft afgegeven en ontvangen, en houdt deze informatie toegankelijk, om ten behoeve van gerechtelijke procedures bewijzen te kunnen leveren en om de continuïteit van de dienst te waarborgen. Dit vastleggen mag elektronisch plaatsvinden;";

4) punt j) wordt geschrapt;

d) het volgende lid wordt ingevoegd:

"4 bis. De leden 3 en 4 zijn van overeenkomstige toepassing op de intrekking van gekwalificeerde elektronische attesteringen van attributen.";

e) lid 5 wordt vervangen door:

"5. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties, procedures en referentienummers voor normen inzake de in lid 2 bedoelde eisen vast. Indien die technische specificaties, procedures en normen worden nageleefd, wordt aangenomen dat er overeenstemming is met de in dit artikel bepaalde eisen. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

f) het volgende lid wordt ingevoegd:

"6. De Commissie is bevoegd uitvoeringshandelingen vast te stellen tot nadere bepaling van de technische kenmerken van de in lid 2, punt f bis), bedoelde maatregelen.";

25a) artikel 26 wordt als volgt gewijzigd:

"2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake geavanceerde elektronische handtekeningen vast. Aan de vereisten voor geavanceerde elektronische handtekeningen wordt geacht te zijn voldaan indien een geavanceerde elektronische handtekening aan deze specificaties en normen voldoet. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeks-procedure vastgesteld.";

25b) artikel 27 wordt als volgt gewijzigd:

lid 4 wordt geschrapt.

26) in artikel 28 wordt lid 6 vervangen door:

"6. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake gekwalificeerde certificaten voor elektronische handtekeningen vast. Indien een gekwalificeerd certificaat voor elektronische handtekeningen aan dergelijke specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage I vastgestelde eisen. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

27) aan artikel 29 wordt het volgende nieuwe lid 1 bis toegevoegd:

"1 bis. Het genereren en beheren van de gegevens voor het aanmaken van elektronische handtekeningen namens de ondertekenaar of het dupliceren van dergelijke gegevens voor back-updoeleinden kan alleen worden uitgevoerd door een gekwalificeerde verlener van vertrouwensdiensten die een gekwalificeerde vertrouwensdienst voor het beheer van een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen op afstand verleent.";

28) het volgende artikel 29 bis wordt ingevoegd:

"*Artikel 29 bis*

Eisen voor een gekwalificeerde dienst voor het beheer van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen op afstand

1. Het beheer van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen op afstand als gekwalificeerde vertrouwensdienst kan alleen worden uitgevoerd door een gekwalificeerde verlener van vertrouwensdiensten die:

a) gegevens voor het aanmaken van elektronische handtekeningen namens de ondertekenaar genereert of beheert;

b) onverminderd punt 1, d), van bijlage II, de gegevens voor het aanmaken van elektronische handtekeningen voor back-updoeleinden kan dupliceren, op voorwaarde dat aan de volgende eisen wordt voldaan:

i. de beveiliging van de gedupliceerde gegevensverzamelingen moet van hetzelfde niveau zijn als de beveiliging van de originele gegevensverzamelingen;

ii. het aantal gedupliceerde gegevensverzamelingen mag niet hoger zijn dan het minimum dat nodig is om de continuïteit van de dienst te waarborgen.

c) aan de voorwaarden uit het certificeringsverslag van het overeenkomstig artikel 30 afgegeven specifieke middel voor het aanmaken van elektronische handtekeningen op afstand voldoet.

2. Voor de toepassing van lid 1 stelt de Commissie binnen twaalf maanden na de inwerkingtreding van deze verordening door middel van uitvoeringshandelingen technische specificaties en referentienummers van normen vast.";

29) in artikel 30 wordt het volgende lid 3 bis ingevoegd:

"3 bis. De in lid 1 bedoelde certificering is niet langer dan vijf jaar geldig, op voorwaarde van een regelmatige tweejaarlijkse kwetsbaarheidsbeoordeling. Indien kwetsbaarheden worden vastgesteld en niet worden verholpen, wordt de certificering geannuleerd.";

30) in artikel 31 wordt lid 3 vervangen door:

"3. Voor de toepassing van lid 1 stelt de Commissie binnen twaalf maanden na de inwerkingtreding van deze verordening door middel van uitvoeringshandelingen de formaten en procedures vast. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

31) artikel 32 wordt als volgt gewijzigd:

a) aan lid 1 wordt de volgende alinea toegevoegd:

"Indien de validering van gekwalificeerde elektronische handtekeningen aan de in lid 3 bedoelde specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in de eerste alinea bedoelde vastgestelde eisen.";

b) lid 3 wordt vervangen door:

"3. Binnen twaalf maanden na de inwerkingtreding van deze verordening bepaalt de Commissie door middel van uitvoeringshandelingen specificaties en referentienummers voor normen inzake de validering van gekwalificeerde elektronische handtekeningen. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

31a) het volgende artikel 32 bis wordt ingevoegd:

"Eisen voor de validering van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten

1. Het valideringsproces voor een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat bevestigt de geldigheid van een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat, op voorwaarde dat:

a) het certificaat dat de handtekening ondersteunt op het tijdstip van ondertekening een gekwalificeerd certificaat voor elektronische handtekeningen was overeenkomstig bijlage I;

b) het gekwalificeerd certificaat werd afgegeven door een gekwalificeerd verlener van vertrouwensdiensten en op het tijdstip van ondertekening geldig was;

c) de gegevens voor het valideren van de handtekening overeenstemmen met de gegevens die aan de vertrouwende partij zijn verstrekt;

d) de unieke reeks gegevens die in het certificaat verwijst naar de ondertekenaar, correct wordt doorgegeven aan de vertrouwende partij;

e) de vertrouwende partij duidelijk wordt gewezen op het eventuele gebruik van een pseudoniem op het tijdstip van ondertekening;

f) de integriteit van de ondertekende gegevens niet is aangetast;

g) op het tijdstip van ondertekening voldaan was aan de in artikel 26, bedoelde eisen. Indien de validering van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten aan de in lid 3 bedoelde specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in de eerste alinea bedoelde vastgestelde eisen.

2. Het systeem dat is gebruikt voor het valideren van de geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat verstrekt het juiste resultaat van het valideringsproces aan de vertrouwende partij en stelt deze in de gelegenheid om veiligheidsproblemen te identificeren.

3. Binnen twaalf maanden na de inwerkingtreding van deze verordening bepaalt de Commissie door middel van uitvoeringshandelingen specificaties en referentienummers voor normen inzake de validering van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

31b) artikel 33 wordt als volgt gewijzigd:

"1. Een gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen kan uitsluitend worden verleend door een gekwalificeerde verlener van vertrouwensdiensten die:";

"2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties, procedures en referentienummers voor normen inzake de in lid 2 bedoelde gekwalificeerde valideringsdienst vast. Indien de dienst voor de validering van gekwalificeerde elektronische handtekeningen aan dergelijke specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

32) artikel 34 wordt vervangen door:

"*Artikel 34*

Gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen

1. Een gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen kan uitsluitend worden verleend door een gekwalificeerde verlener van vertrouwensdiensten die procedures en technologieën hanteert welke het mogelijk maken de betrouwbaarheid van de gekwalificeerde elektronische handtekeningen te verlengen tot na de technologische geldigheidsduur.

2. Indien de voorzieningen voor de gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen aan de in lid 3 bedoelde specificaties en normen voldoen, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen.

3. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake de gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen vast. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

32a) aan artikel 36 wordt een nieuw lid 2 toegevoegd:

"2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake geavanceerde elektronische zegels vast.

Aan de vereisten voor geavanceerde elektronische zegels wordt geacht te zijn voldaan indien een geavanceerde elektronische zegel aan deze specificaties en normen voldoet. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

(33) artikel 37 wordt als volgt gewijzigd:

lid 4 wordt geschrapt;

34) artikel 38 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Gekwalificeerde certificaten voor elektronisch zegels voldoen aan de in bijlage III vastgestelde eisen. Indien een gekwalificeerd certificaat voor elektronisch zegels aan de in lid 6 bedoelde specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage III vastgestelde eisen.";

b) lid 6 wordt vervangen door:

"6. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake gekwalificeerde certificaten voor elektronische zegels vast. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

35) het volgende artikel 39 bis wordt ingevoegd:

"Artikel 39 bis

Eisen voor een gekwalificeerde dienst voor het beheer van gekwalificeerde middelen voor het aanmaken van elektronische zegels op afstand

Artikel 29 bis is van overeenkomstige toepassing op een gekwalificeerde dienst voor het beheer van gekwalificeerde middelen voor het aanmaken van elektronische zegels op afstand.";

35a) het volgende artikel 40 bis wordt ingevoegd:

"*Artikel 40 bis*

Eisen voor de validering van geavanceerde elektronische zegels op basis van gekwalificeerde certificaten

(1) Artikel 32 bis is van overeenkomstige toepassing op de validering van geavanceerde elektronische zegels op basis van gekwalificeerde certificaten.";

36) artikel 42 wordt als volgt gewijzigd:

a) het volgende nieuwe lid 1 bis wordt ingevoegd:

"1 bis. Indien de koppeling van datum en tijdstip aan gegevens en de nauwkeurige tijdsbron aan de in lid 2 bedoelde specificaties en normen voldoen, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen.";

b) lid 2 wordt vervangen door:

"2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake de koppeling van datum en tijdstip aan gegevens en de nauwkeurige tijdsbron vast. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

36a) aan artikel 43 wordt een nieuw lid 3 toegevoegd:

"2 bis. Een gekwalificeerde dienst voor elektronisch aangetekende bezorging in een lidstaat wordt in alle lidstaten als een gekwalificeerde dienst voor elektronisch aangetekende bezorging erkend.";

37) artikel 44 wordt als volgt gewijzigd:

a) het volgende lid 1 bis wordt ingevoegd:

"1 bis. Indien het proces voor het verzenden en ontvangen van gegevens aan de in lid 2 bedoelde specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen.";

b) lid 2 wordt vervangen door:

"2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake processen voor het verzenden en ontvangen van gegevens vast. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

c) de volgende leden 3 en 4 worden ingevoegd:

"3. Verleners van gekwalificeerde diensten voor elektronisch aangetekende bezorging kunnen een akkoord bereiken over de interoperabiliteit van de gekwalificeerde diensten voor elektronisch aangetekende bezorging die zij verlenen. Een dergelijk interoperabiliteitskader voldoet aan de eisen van lid 1. De overeenstemming wordt bevestigd door een conformiteitsbeoordelingsinstantie.

4. De Commissie kan door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen vaststellen teneinde de overdracht van gegevens tussen twee of meer gekwalificeerde verleners van vertrouwensdiensten te faciliteren. De technische specificaties en de inhoud van de normen zijn kosteneffectief en evenredig. De uitvoeringshandeling wordt volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

38) artikel 45 wordt vervangen door:

"*Artikel 45*

Eisen voor gekwalificeerde certificaten voor websiteauthenticatie

"1. Gekwalificeerde certificaten voor websiteauthenticatie voldoen aan de eisen van bijlage IV. De evaluatie van de overeenstemming met de eisen van bijlage IV wordt uitgevoerd overeenkomstig de in lid 4 bedoelde specificaties en normen.

2. De in lid 1 bedoelde gekwalificeerde certificaten voor websiteauthenticatie worden herkend door webbrowsers. Daartoe waarborgen webbrowsers dat de met behulp van alle identificatiemethoden verstrekte identiteitsgegevens gebruiksvriendelijk worden weergegeven. Webbrowsers zorgen voor ondersteuning van en interoperabiliteit met de in lid 1 bedoelde gekwalificeerde certificaten voor websiteauthenticatie, met uitzondering van ondernemingen die overeenkomstig Aanbeveling 2003/361/EG van de Commissie tijdens de eerste vijf jaar als aanbieders van webbrowserdiensten als kleine en micro-ondernemingen worden beschouwd.

4. Binnen twaalf maanden na de inwerkingtreding van deze verordening bepaalt de Commissie door middel van uitvoeringshandelingen de specificaties en referentie-nummers voor normen inzake de in de leden 1 en 2 bedoelde gekwalificeerde certificaten voor websiteauthenticatie. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

39) de volgende afdelingen 9, 10 en 11 worden ingevoegd na artikel 45:

"AFDELING 9

ELEKTRONISCHE ATTESTERING VAN ATTRIBUTEN

Artikel 45 bis

Rechtsgevolgen van elektronische attesteringen van attributen

1. Het rechtsgevolg van een elektronische attestering van attributen en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures worden niet ontzegd louter op grond van het feit dat het elektronisch is of niet aan de eisen voor gekwalificeerde elektronische attesteringen van attributen voldoet.

2. Een gekwalificeerde elektronische attestering van attributen en attesteringen van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, hebben dezelfde rechtsgevolgen als rechtmatig afgegeven attesteringen op papier.

3. Een gekwalificeerde elektronische attestering van attributen, afgegeven in een lidstaat, wordt in alle lidstaten als een gekwalificeerde elektronische attestering van attributen erkend.

4. Een attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, wordt in alle lidstaten erkend als een attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron.

Artikel 45 ter

Elektronische attestering van attributen in publieke diensten

Wanneer een elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereist is op grond van nationaal recht om toegang te krijgen tot een door een openbare instantie aangeboden onlinedienst, vervangen de persoonsidentificatiegegevens in de elektronische attestering van attributen niet de elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie voor elektronische identificatie, tenzij de lidstaat daarvoor uitdrukkelijk toestemming heeft verleend. In een dergelijk geval wordt een gekwalificeerde elektronische attestering van andere lidstaten ook aanvaard.

Artikel 45 quater

Eisen voor gekwalificeerde elektronische attestering van attributen

1. Gekwalificeerde elektronische attesteringen van attributen voldoen aan de in bijlage V vastgestelde eisen.

1 bis. De evaluatie van de overeenstemming met de eisen van bijlage V wordt uitgevoerd overeenkomstig de in lid 4 bedoelde specificaties en normen.

2. Voor gekwalificeerde elektronische attesteringen van attributen gelden geen dwingende eisen naast de in bijlage V vastgestelde eisen.

3. Indien een gekwalificeerde elektronische attestering van attributen na initiële afgifte wordt ingetrokken, verliest zij haar geldigheid vanaf het moment van de intrekking en kan de status ervan in geen geval worden hersteld.

4. Binnen zes maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de in artikel 6 bis, lid 11, bedoelde Europese portemonnees voor digitale identiteit technische specificaties en referentienummers voor normen inzake gekwalificeerde elektronische attesteringen van attributen vast.

Artikel 45 quinquies

Verificatie van attributen aan de hand van authentieke bronnen

1. De lidstaten waarborgen binnen 24 maanden na de inwerkingtreding van de in artikel 6 bis, lid 11, en artikel 6 quater, lid 4, bedoelde uitvoeringshandelingen dat er, ten minste voor de in bijlage VI vermelde attributen, voor zover die attributen authentieke bronnen binnen de publieke sector gebruiken, maatregelen worden genomen zodat gekwalificeerde verleners van elektronische attesteringen van attributen langs elektronische weg deze attributen kunnen verifiëren op verzoek van de gebruiker en overeenkomstig het nationale of Unierecht.

2. Binnen zes maanden na de inwerkingtreding van deze verordening en met inachtneming van de toepasselijke internationale normen legt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de Europese portemonnees voor digitale identiteit in de zin van artikel 6 bis, lid 11, minimale technische specificaties, normen en procedures vast met betrekking tot de catalogus van attributen en regelingen voor de attestering van attributen en verificatie-procedures voor gekwalificeerde elektronische attesteringen van attributen.

Artikel 45 quinquies bis

Eisen voor elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron

1. Een elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, voldoet aan de volgende eisen:

a) de eisen van bijlage VII;

b) het gekwalificeerde certificaat ter ondersteuning van de gekwalificeerde elektronische handtekening of het gekwalificeerde elektronische zegel van de in artikel 3, punt 45 bis) bedoelde openbare instantie die is geïdentificeerd als de in punt b), van bijlage VII bedoelde afgever, bevat een specifieke reeks gecertificeerde attributen in een voor automatische verwerking geschikte vorm:

i) waaruit blijkt dat overeenkomstig nationaal recht of Unierecht is vastgesteld dat de afgevende instantie de verantwoordelijke is voor de authentieke bron op basis waarvan de elektronische attestering van attributen is uitgegeven of de instantie die is aangewezen om namens haar op te treden;

ii) die een reeks gegevens bevatten die ondubbelzinnig naar de in punt i) bedoelde authentieke bron verwijzen; en

iii) waarin het in punt i) bedoelde nationale recht of Unierecht wordt vastgesteld.

2. De lidstaat waar de in artikel 3, punt 45 bis), bedoelde openbare instanties zijn gevestigd, zorgt ervoor dat de openbare instanties die elektronische attesteringen van attributen uitgeven, een betrouwbaarheidsniveau hebben dat gelijkwaardig is aan dat van gekwalificeerde verleners van vertrouwensdiensten overeenkomstig artikel 24.

2 bis. De lidstaten melden de in artikel 3, punt 45 bis, bedoelde openbare instanties aan bij de Commissie. Deze aanmelding omvat een conformiteitsbeoordelingsverslag van een conformiteitsbeoordelingsinstantie waarin wordt bevestigd dat aan de eisen van de leden 1, 2 en 6 van dit artikel is voldaan. De Commissie maakt via een beveiligd kanaal de lijst van de in artikel 3, punt 45 bis), bedoelde openbare instanties in elektronisch ondertekende of verzegelde en voor automatische verwerking geschikte vorm publiek beschikbaar.

3. Indien een elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, eerst is uitgegeven en vervolgens ingetrokken, verliest deze haar geldigheid vanaf het moment van intrekking. Na de intrekking wordt de status "ingetrokken" van een elektronische attestering niet teruggedraaid.

4. Een elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, wordt geacht te voldoen aan de eisen van lid 1 van dit artikel, indien het aan de in lid 5 bedoelde normen voldoet.

5. Binnen zes maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de in artikel 6 bis, lid 11, bedoelde Europese portemonnees voor digitale identiteit technische specificaties en referentienummers voor normen inzake elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron vast.

5 bis. Binnen zes maanden na de inwerkingtreding van deze verordening bepaalt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de in artikel 6 bis, lid 11, bedoelde Europese portemonnees voor digitale identiteit, de formaten, procedures, specificaties en normen voor de toepassing van lid 2 bis.

6. De in artikel 3, punt 45 bis), bedoelde openbare instanties die elektronische attesteringen van attributen uitgeven, bieden een interface met de overeenkomstig artikel 6 bis verstrekte Europese portemonnees voor digitale identiteit.

Artikel 45 sexies

Uitgifte van elektronische attesteringen van attributen aan Europese portemonnees voor digitale identiteit

Verleners van gekwalificeerde elektronische attesteringen van attributen bieden een interface met de overeenkomstig artikel 6 bis verstrekte Europese portemonnees voor digitale identiteit.

Artikel 45 septies

Aanvullende voorschriften voor de levering van diensten voor elektronische attestering van attributen

1. Verleners van gekwalificeerde en niet-gekwalificeerde diensten voor elektronische attestering van attributen mogen persoonsgegevens met betrekking tot de verlening van die diensten niet combineren met persoonsgegevens van andere door hen of hun commerciële partners aangeboden diensten.

2. Persoonsgegevens met betrekking tot de verlening van elektronische attestering van attributen worden logisch gescheiden van andere door de verlener van elektronische attestering van attributen opgeslagen gegevens.

4. Verleners van gekwalificeerde diensten van elektronische attestering van attributen voeren een functionele scheiding in voor het verlenen van dergelijke diensten.

AFDELING 10

ELEKTRONISCHE ARCHIEFDIENSTEN

Artikel 45 octies

Rechtsgevolg van een elektronische archiveringsdienst

1. Het rechtsgevolg en de toelaatbaarheid als bewijsmiddel in gerechtelijke procedures van elektronische gegevens die zijn opgeslagen via een elektronische archiverings-dienst, worden niet ontzegd louter op grond van het feit dat de gegevens elektronisch zijn of niet opgeslagen zijn via een gekwalificeerde elektronische archiveringsdienst.

2. Voor via een gekwalificeerde elektronische archiveringsdienst opgeslagen elektronische gegevens geldt het vermoeden van integriteit van de gegevens en van juistheid van de oorsprong van de gegevens voor de duur van de termijn van bewaring door de verlener van gekwalificeerde vertrouwensdiensten.

3. Een gekwalificeerde elektronische archiveringsdienst in een lidstaat wordt in alle andere lidstaten als een gekwalificeerde elektronische archiveringsdienst erkend.

Artikel 45 octies bis

Eisen voor gekwalificeerde elektronische archiveringsdiensten

1. Gekwalificeerde elektronische archiveringsdiensten voldoen aan de volgende eisen:

   a) zij worden verleend door gekwalificeerde verleners van vertrouwensdiensten;

   b) zij maken gebruik van procedures en technologieën die het mogelijk maken de duurzaamheid en leesbaarheid van de elektronische gegevens te verlengen tot na de technologische geldigheidsduur en ten minste gedurende de wettelijke of contractuele bewaringstermijn, en handhaven daarbij de integriteit en de oorsprong van de gegevens;

c) zij zorgen ervoor dat de elektronische gegevens zodanig worden bewaard dat zij beschermd zijn tegen verlies en wijzigingen, behalve wijzigingen met betrekking tot het medium of het elektronische formaat;

d) zij stellen gemachtigde vertrouwende partijen in staat op geautomatiseerde wijze verslagen te ontvangen waarin wordt bevestigd dat voor elektronische gegevens die zijn opgevraagd uit een gekwalificeerd elektronisch archief het vermoeden van integriteit van de gegevens geldt vanaf het begin van de bewaringstermijn tot het moment van opvraging. Dit verslag wordt op betrouwbare en efficiënte wijze verstrekt en draagt de gekwalificeerde elektronische handtekening of het gekwalificeerde elektronische zegel van de verlener van de gekwalificeerde elektronische archiveringsdienst;

2. Binnen twaalf maanden na de inwerkingtreding van deze verordening stelt de Commissie door middel van uitvoeringshandelingen technische specificaties en referentienummers voor normen inzake gekwalificeerde elektronische archiveringsdiensten vast. Aan de vereisten voor gekwalificeerde elektronische archiveringsdiensten wordt geacht te zijn voldaan indien een gekwalificeerde elektronische archiveringsdienst aan deze specificaties en normen voldoet. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

AFDELING 11

ELEKTRONISCHE REGISTERS

Artikel 45 nonies

Rechtsgevolgen van elektronische registers

1. Het rechtsgevolg van een elektronisch register en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures worden niet ontzegd louter op grond van het feit dat het elektronisch is of niet aan de eisen voor gekwalificeerde elektronische register voldoet.

2. Voor gegevensbestanden in een gekwalificeerd elektronisch register geldt het vermoeden van het unieke karakter en de juistheid van de chronologische volgorde en van de integriteit ervan.

3. Een gekwalificeerd elektronisch register in een lidstaat wordt in alle lidstaten als een gekwalificeerd elektronisch register erkend.

Artikel 45 decies

Eisen voor gekwalificeerde elektronische registers

1. Gekwalificeerde elektronische registers voldoen aan de volgende eisen:

   a) zij worden aangemaakt door een of meer gekwalificeerde verleners van vertrouwensdiensten;

   b) zij stellen de oorsprong van de gegevensbestanden in het register vast;

   c) zij waarborgen de unieke chronologische volgorde van de gegevensbestanden in het register;

   d) zij slaan de gegevens op zodanige wijze op dat elke wijziging achteraf van de gegevens onmiddellijk kan worden opgespoord, en waarborgen de integriteit ervan in de tijd.

2. Indien het elektronische register aan de in lid 3 bedoelde specificaties en normen voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen.

3. De Commissie stelt door middel van uitvoeringshandelingen technische specificaties en referentienummers vast voor normen inzake de aanmaak en werking van een gekwalificeerd elektronisch register. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

40) het volgende artikel 48 bis wordt ingevoegd:

"Artikel 48 bis

Verslagleggingsvereisten

1. De lidstaten waarborgen dat er statistieken worden verzameld over de werking van de Europese portemonnees voor digitale identiteit zodra zij worden verstrekt op hun grondgebied.

2. De overeenkomstig lid 1 verzamelde statistieken omvatten de volgende elementen:

   a) het aantal natuurlijke en rechtspersonen met een geldige Europese portemonnee voor digitale identiteit;

   b) het soort en het aantal diensten die het gebruik van de Europese portemonnee voor digitale identiteit aanvaarden;

   c) samenvattend verslag met gegevens over incidenten die het gebruik van de Europese portemonnee voor digitale identiteit verhinderen.

3. De in lid 2 bedoelde statistieken worden publiekelijk beschikbaar gesteld in een open en gangbaar machineleesbaar formaat.

4. De lidstaten leggen de Commissie jaarlijks uiterlijk op 31 maart een verslag voor over de overeenkomstig lid 2 verzamelde statistieken.";

41) artikel 49 wordt vervangen door:

"*Artikel 49*

Evaluatie

1. De Commissie evalueert de toepassing van deze verordening en brengt daarover binnen 36 maanden na de inwerkingtreding ervan verslag uit bij het Europees Parlement en de Raad. De Commissie evalueert met name het toepassingsgebied van de artikelen 6 en 6 quinquies ter en de vraag of het gepast is het toepassingsgebied van deze verordening dan wel de specifieke bepalingen ervan te wijzigen, rekening houdend met de ervaring met de toepassing van deze verordening, alsook met de vraag van klanten en technologische, marktgebonden en juridische ontwikkelingen. Dat verslag gaat zo nodig vergezeld van een voorstel tot wijziging van deze verordening.

2. Het evaluatieverslag omvat een beoordeling van de beschikbaarheid en de bruikbaarheid van de Europese portemonnees voor digitale identiteit, binnen het toepassingsgebied van deze verordening, en beoordeelt of alle particuliere onlinedienstverleners die voor gebruikersauthenticatie gebruikmaken van elektronische identificatiediensten van derden, is opgelegd om het gebruik van de Europese portemonnees voor digitale identiteit te aanvaarden.

3. Daarnaast dient de Commissie elke vier jaar na het in de eerste alinea bedoelde verslag een verslag over de vooruitgang bij de verwezenlijking van de doelstellingen van deze verordening in bij het Europees Parlement en de Raad.";

42) artikel 51 wordt vervangen door:

"*Artikel 51*

Overgangsmaatregelen

1. Veilige middelen voor het aanmaken van handtekeningen waarvan de overeenstemming bepaald is overeenkomstig artikel 3, lid 4, van Richtlijn 1999/93/EG, worden tot en met 36 maanden na de inwerkingtreding van deze verordening verder beschouwd als gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen in de zin van deze verordening.

2. Aan natuurlijke personen afgegeven gekwalificeerde certificaten overeenkomstig Richtlijn 1999/93/EG worden tot en met 24 maanden na de inwerkingtreding van deze verordening verder beschouwd als gekwalificeerde certificaten voor elektronische handtekeningen in de zin van deze verordening.

2 bis. Het beheer van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand door gekwalificeerde verleners van vertrouwensdiensten die geen gekwalificeerde verleners van vertrouwensdiensten zijn die gekwalificeerde vertrouwensdiensten verlenen voor het beheer van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand overeenkomstig de artikelen 29 bis en 39 bis, worden tot en met 24 maanden na de inwerkingtreding van deze verordening geacht de status "gekwalificeerd" voor de verlening van deze beheerdiensten niet te hoeven verkrijgen.

2 ter. Gekwalificeerde verleners van vertrouwensdiensten aan wie uit hoofde van deze verordening middels methoden voor identiteitsverificatie voor het afgeven van gekwalificeerde certificaten overeenkomstig artikel 24, lid 1, de status "gekwalificeerd" is toegekend vóór [datum van inwerkingtreding van de wijzigingsverordening], leggen het toezichthoudend orgaan zo spoedig mogelijk en uiterlijk 30 maanden na de inwerkingtreding van de wijzigingsverordening een conformiteitsbeoordelingsverslag voor dat bewijst dat aan artikel 24, lid 1, is voldaan. Tot de indiening van dat conformiteitsbeoordelingsverslag en de voltooiing van de beoordeling ervan door het toezichthoudend orgaan kan die gekwalificeerde verlener van vertrouwensdiensten de methoden voor identiteitsverificatie van artikel 24, lid 1, van Verordening (EU) nr. 910/2014 blijven gebruiken.";

43) bijlage I wordt gewijzigd overeenkomstig bijlage I bij deze verordening;

44) bijlage II wordt vervangen door de tekst die is opgenomen in bijlage II bij deze verordening;

45) bijlage III wordt gewijzigd overeenkomstig bijlage III bij deze verordening;

46) bijlage IV wordt gewijzigd overeenkomstig bijlage IV bij deze verordening;

47) een nieuwe bijlage V wordt toegevoegd zoals opgenomen in bijlage V bij deze verordening;

48) een nieuwe bijlage VI wordt aan deze verordening toegevoegd.

Artikel 52

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement	Voor de Raad
De voorzitter	De voorzitter

BIJLAGE I

Bijlage I, punt i), wordt vervangen door:

"i) de informatie, of de locatie van de diensten waar informatie kan worden opgevraagd, over de geldigheidsstatus van het gekwalificeerde certificaat;".

BIJLAGE II

EISEN VOOR GEKWALIFICEERDE MIDDELEN VOOR HET AANMAKEN VAN ELEKTRONISCHE HANDTEKENINGEN

1. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen waarborgen via passende technieken en procedures dat ten minste:

(a) de vertrouwelijkheid van de gegevens die worden gebruikt om elektronische handtekeningen aan te maken redelijkerwijs gewaarborgd is;

(b) de gegevens voor het aanmaken van elektronische handtekeningen in de praktijk slechts één keer kunnen voorkomen;

(c) de gegevens voor het aanmaken van elektronische handtekeningen met redelijke zekerheid niet kunnen worden afgeleid en dat de elektronische handtekening op betrouwbare wijze beschermd is tegen vervalsing met de thans beschikbare technologie;

(d) de gegevens voor het aanmaken van elektronische handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen.

2. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen laten de te ondertekenen gegevens ongewijzigd en beletten niet dat die gegevens vóór ondertekening aan de ondertekenaar worden voorgelegd.

BIJLAGE III

Bijlage III, punt i), wordt vervangen door:

"i) de informatie, of de locatie van de diensten waar informatie kan worden opgevraagd, over de geldigheidsstatus van het gekwalificeerde certificaat;".

BIJLAGE IV

Bijlage IV, punt j), wordt vervangen door:

"j) de informatie, of de locatie van de geldigheidsstatus van certificaatsdiensten waar informatie kan worden opgevraagd, over de geldigheidsstatus van het gekwalificeerde certificaat;".

BIJLAGE V

EISEN VOOR GEKWALIFICEERDE ELEKTRONISCHE ATTESTERING VAN ATTRIBUTEN

Gekwalificeerde elektronische attesteringen van attributen bevatten:

(e) een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat de attestering afgegeven is als een gekwalificeerde elektronische attestering van attributen;

(f) een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde elektronische attesteringen van attributen afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en

– voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers,

– voor een natuurlijk persoon: de naam van de persoon;

(g) een reeks gegevens die ondubbelzinnig verwijzen naar de entiteit waarnaar de geattesteerde attributen verwijzen; als er een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven;

(h) het geattesteerde attribuut of de geattesteerde attributen inclusief, indien van toepassing, de benodigde informatie om de reikwijdte van die attributen te bepalen;

(i) informatie over begin en einde van de geldigheidsduur van de attestering;

(j) de identiteitscode van de attestering, die uniek moet zijn voor de gekwalificeerde verlener van vertrouwensdiensten en, indien van toepassing, de vermelding van de attesteringsregeling waar de attestering van attributen deel van uitmaakt;

(k) de gekwalificeerde elektronische handtekening of het gekwalificeerde elektronische zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;

(l) de locatie waar het certificaat ter ondersteuning van de gekwalificeerde elektronische handtekening of het gekwalificeerde elektronische zegel als bedoeld in punt g), gratis beschikbaar is;

(m) de informatie of de locatie van de diensten waar informatie kan worden opgevraagd over de geldigheidsstatus van de gekwalificeerde attestering.

BIJLAGE VI

MINIMALE LIJST VAN ATTRIBUTEN

Overeenkomstig artikel 45 quinquies waarborgen de lidstaten dat er, indien die attributen gebruikmaken van authentieke bronnen binnen de publieke sector, maatregelen worden genomen zodat gekwalificeerde verleners van elektronische attesteringen van attributen op verzoek van de gebruiker langs elektronische weg aan de hand van de relevante authentieke bron op nationaal niveau of via op nationaal niveau erkende aangewezen intermediairs, overeenkomstig nationaal of Unierecht, de authenticiteit van de volgende attributen kunnen verifiëren:

1. adres;
2. leeftijd;
3. geslacht;
4. burgerlijke staat;
5. gezinssamenstelling;
6. nationaliteit of staatsburgerschap;
7. onderwijskwalificaties, -titels en -diploma's;
8. beroepskwalificaties, -titels en -licenties;
9. openbare vergunningen en licenties;
10. financiële en bedrijfsgegevens.

BIJLAGE VII

EISEN VOOR ELEKTRONISCHE ATTESTERING VAN ATTRIBUTEN UITGEGEVEN DOOR OF NAMENS EEN OPENBARE INSTANTIE DIE VERANTWOORDELIJK IS VOOR EEN AUTHENTIEKE BRON

Een elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, bevat:

a) een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat de attestering is afgegeven als een elektronische attestering van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron;
b) een reeks gegevens die ondubbelzinnig verwijzen naar de openbare instantie die de gekwalificeerde elektronische attestering van attributen afgeeft, met inbegrip van ten minste de lidstaat waar die openbare instantie is gevestigd en de naam, en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers;
c) een reeks gegevens die ondubbelzinnig verwijzen naar de entiteit waarnaar de geattesteerde attributen verwijzen; als er een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven;
d) het geattesteerde attribuut of de geattesteerde attributen inclusief, indien van toepassing, de benodigde informatie om de reikwijdte van die attributen te bepalen;
e) informatie over begin en einde van de geldigheidsduur van de attestering;
f) de identiteitscode van de attestering, die uniek moet zijn voor de afgevende openbare instantie en, indien van toepassing, de vermelding van de attesteringsregeling waar de attestering van attributen deel van uitmaakt;
g) de gekwalificeerde elektronische handtekening of het gekwalificeerde elektronische zegel van de afgevende instantie;
h) de locatie waar het certificaat ter ondersteuning van de gekwalificeerde elektronische handtekening of het gekwalificeerde elektronische zegel als bedoeld in punt g), gratis beschikbaar is;
i) de informatie of de locatie van de diensten waar informatie kan worden opgevraagd over de geldigheidsstatus van de attestering.

_____