**Europees Parlement**
2019-2024

**AANGENOMEN TEKSTEN**

# P9_TA(2024)0117

## Europees kader voor een digitale identiteit

**Wetgevingsresolutie van het Europees Parlement van 29 februari 2024 over het 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 (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))**

**(Gewone wetgevingsprocedure: eerste lezing)**

*Het Europees Parlement*,

– gezien het voorstel van de Commissie aan het Europees Parlement en de Raad (COM(2021)0281),

– gezien artikel 294, lid 2, en artikel 114 van het Verdrag betreffende de werking van de Europese Unie, op grond waarvan het voorstel door de Commissie bij het Parlement is ingediend (C9-0200/2021),

– gezien artikel 294, lid 3, van het Verdrag betreffende de werking van de Europese Unie,

– gezien het advies van het Europees Economisch en Sociaal Comité van 20 oktober 2021[1],

– gezien het advies van het Comité van de Regio's van 13 oktober 2021[2],

– gezien het overeenkomstig artikel 74, lid 4, van zijn Reglement door de bevoegde commissie goedgekeurde voorlopig akkoord en de door de vertegenwoordiger van de Raad bij brief van 6 december 2023 gedane toezegging om het standpunt van het Europees Parlement overeenkomstig artikel 294, lid 4, van het Verdrag betreffende de werking van de Europese Unie goed te keuren,

– gezien artikel 59 van zijn Reglement,

– gezien de adviezen van de Commissie interne markt en consumentenbescherming, de Commissie juridische zaken en de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken,

---

1 PB C 105 van 4.3.2022, blz. 81.
2 PB C 61 van 4.2.2022, blz. 42.

– gezien het verslag van de Commissie industrie, onderzoek en energie (A9-0038/2023),

1. stelt onderstaand standpunt in eerste lezing vast;

2. neemt kennis van de verklaring de Commissie die als bijlage bij deze resolutie is gevoegd;

3. verzoekt de Commissie om hernieuwde voorlegging aan het Parlement indien zij haar voorstel vervangt, ingrijpend wijzigt of voornemens is het ingrijpend te wijzigen;

4. verzoekt zijn Voorzitter het standpunt van het Parlement te doen toekomen aan de Raad en aan de Commissie alsmede aan de nationale parlementen.

**P9_TC1-COD(2021)0136**

**Standpunt van het Europees Parlement in eerste lezing vastgesteld op 29 februari 2024 met het oog op de vaststelling van Verordening (EU) 2024/... van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor 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],

Gezien het advies van het Comité van de Regio's[2],

Handelend volgens de gewone wetgevingsprocedure[3],

---

1 PB C 105 van 4.3.2022, blz. 81.

2 PB C 61 van 4.2.2022, blz. 42.

3 Standpunt van het Europees Parlement van 29 februari 2024.

Overwegende hetgeen volgt:

(1) In de mededeling van de Commissie van 19 februari 2020 met als titel “De digitale toekomst van Europa vormgeven” wordt een herziening van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad[4] aangekondigd om de doeltreffendheid ervan te verbeteren, de voordelen ervan voor de private sector uit te breiden en betrouwbare digitale identiteiten voor alle Europeanen te bevorderen.

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

[4] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

***(3)*** ***In het beleidsprogramma voor het digitale decennium tot 2030, dat is vastgesteld bij Besluit (EU) 2022/2481 van het Europees Parlement en de Raad[5], zijn de doelstellingen en digitale streefcijfers van een Uniekader vastgelegd die tegen 2030 moeten leiden tot een brede uitrol van een betrouwbare, vrijwillige, door de gebruiker gecontroleerde digitale identiteit die Uniebreed wordt erkend en die het voor iedere gebruiker mogelijk maakt controle te hebben over zijn gegevens in online interacties.***

***(4)*** ***In de door het Europees Parlement, de Raad en de Commissie afgekondigde "Europese verklaring over digitale rechten en beginselen voor het digitale decennium"[6] (de "verklaring") wordt benadrukt dat iedereen het recht heeft op toegang tot digitale technologieën, producten en diensten die door hun ontwerp veilig, beveiligd en privacy-beschermend zijn. Dit houdt in dat moet worden gewaarborgd dat alle inwoners van de Unie een toegankelijke, beveiligde en betrouwbare digitale identiteit krijgen die hen in staat stelt toegang te krijgen tot een breed scala aan online- en offlinediensten, waarbij bescherming wordt geboden tegen cyberbeveiligingsrisico's en cybercriminaliteit, met inbegrip van inbreuken op gegevens en identiteitsdiefstal of -manipulatie. In de verklaring wordt ook gesteld dat iedereen recht heeft op bescherming van zijn of haar persoonsgegevens. Dat recht houdt ook controle in over hoe gegevens worden gebruikt en met wie zij worden gedeeld.***

---

**5** Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030 (PB L 323 van 19.12.2022, blz. 4).

**6** PB C 23 van 23.1.2023, blz. 1.

***(5) Burgers en ingezetenen van de Unie moeten recht hebben op een digitale identiteit waarover alleen zijzelf zeggenschap hebben en die hen in staat stelt hun rechten uit te oefenen in de digitale omgeving en deel te nemen aan de digitale economie. Hiertoe moet een Europees kader voor digitale identiteit worden vastgesteld dat burgers en ingezetenen van de Unie in staat stelt toegang te krijgen tot publieke en private online- en offlinediensten in de hele Unie.***

***(6) Een geharmoniseerd kader voor digitale identiteit moet bijdragen tot de totstandbrenging van een meer digitaal geïntegreerde Unie, door de digitale barrières tussen de lidstaten weg te nemen en ervoor te zorgen dat burgers en ingezetenen van de Unie de voordelen van digitalisering kunnen genieten, en tegelijkertijd de transparantie en de bescherming van hun rechten vergroten.***

(7) Een meer geharmoniseerde benadering van elektronische identificatie moet de risico's en de kosten van de huidige versnippering door uiteenlopende nationale oplossingen ***of, in sommige lidstaten, het ontbreken van oplossingen voor elektronische identificatie*** verkleinen. ***Die aanpak*** moet de interne markt versterken door burgers en ingezetenen van de Unie, zoals gedefinieerd in het nationaal recht, en ondernemingen ***in staat te stellen*** zich op een ***veilige, betrouwbare, gebruikersvriendelijke,*** gemakkelijke, ***toegankelijke en geharmoniseerde*** manier in de hele Unie online ***en offline*** te identificeren ***en hun identiteit te authenticeren***. ***De Europese portemonnee voor digitale identiteit moet natuurlijke en rechtspersonen in de hele Unie een geharmoniseerd elektronisch identificatiemiddel bieden dat authenticatie en het delen van aan hun identiteit gekoppelde gegevens mogelijk maakt.*** Iedereen moet veilig toegang kunnen hebben tot publieke en private diensten en kunnen vertrouwen op een verbeterd ecosysteem voor vertrouwensdiensten en op geverifieerde identiteitsbewijzen en ***elektronische*** attesteringen van attributen, zoals ***academische kwalificaties, waaronder universitaire diploma's, of andere onderwijs- of beroepstitels***. Het Europees kader voor digitale identiteit ***is bedoeld om*** een verschuiving ***teweeg te brengen*** van het gebruik van uitsluitend nationale digitale-identiteitsoplossingen naar de levering van elektronische attesteringen van attributen die ***overal in de Unie*** geldig zijn ***en wettelijk worden erkend***. Aanbieders van elektronische attesteringen van attributen moeten profijt trekken uit duidelijke en uniforme regels***, terwijl*** overheidsdiensten moeten kunnen vertrouwen op elektronische documenten in een bepaald format.

*(8) Verschillende lidstaten hebben elektronische identificatiemiddelen ingevoerd – en gebruiken deze ook – die door dienstverleners in de Unie worden aanvaard. Daarnaast is er geïnvesteerd in zowel nationale als grensoverschrijdende oplossingen op basis van Verordening (EU) nr. 910/2014, ook wat betreft de interoperabiliteit van aangemelde stelsels voor elektronische identificatie op grond van die verordening. Om complementariteit te waarborgen en ervoor te zorgen dat Europese portemonnees voor digitale identiteit snel voldoende worden gebruikt bij de huidige gebruikers van aangemelde elektronische identificatiemiddelen, en om de gevolgen voor bestaande dienstverleners tot een minimum te beperken, wordt verwacht dat de Europese portemonnees voor digitale identiteit profijt zullen trekken van de ervaring met bestaande elektronische identificatiemiddelen en van de op Unie- en nationaal niveau uitgerolde infrastructuur van aangemelde stelsels voor elektronische identificatie.*

*(9) Verordening (EU) 2016/679 van het Europees Parlement en de Raad[7] en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad[8] zijn van toepassing op alle activiteiten betreffende de verwerking van persoonsgegevens uit hoofde van Verordening (EU) nr. 910/2014. De oplossingen van het interoperabiliteitskader waarin deze verordening voorziet, voldoen ook aan die regels. De gegevensbeschermingswetgeving van de Unie voorziet in gegevensbeschermingsbeginselen, zoals de beginselen van minimale gegevensverwerking en doelbinding, en in verplichtingen, zoals gegevensbescherming door ontwerp en door standaardinstellingen.*

---

7 *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).*

8 *Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).*

(10) Ter ondersteuning van het concurrentievermogen van Uniebedrijven moeten aanbieders van ***zowel*** online***- als offline***diensten kunnen vertrouwen op digitale-identiteitsoplossingen die Uniebreed worden erkend, ongeacht de lidstaat waar die ***oplossingen*** worden verleend, en dus profiteren van een geharmoniseerde ***Unie***benadering van vertrouwen, beveiliging en interoperabiliteit. ***Zowel*** gebruikers ***als*** dienstverleners moeten er ▌ baat bij kunnen hebben dat de rechtskracht van elektronische attesteringen van attributen in de hele Unie gelijk is. ***Een geharmoniseerd kader voor digitale identiteit is bedoeld om economische waarde te ontsluiten door de toegang tot goederen en diensten gemakkelijker te maken en door de operationele kosten die verband houden met elektronische-identificatie- en authenticatieprocedures aanzienlijk te verlagen, bijvoorbeeld bij de aanmelding van nieuwe klanten, en door de kans op cybercriminaliteit zoals identiteitsdiefstal, gegevensdiefstal en onlinefraude te beperken, en bevordert derhalve efficiëntie en de veilige digitale transformatie in micro-, kleine en middelgrote ondernemingen in de Unie.***

***(11) Europese portemonnees voor digitale identiteit moeten de toepassing van het eenmaligheidsbeginsel vergemakkelijken en bijgevolg de administratieve lasten voor burgers en ingezetenen van de Unie en bedrijven in de hele Unie verminderen en hun grensoverschrijdende mobiliteit ondersteunen, en de ontwikkeling van interoperabele e-overheidsdiensten in de hele Unie bevorderen.***

(12) ***Verordening*** (EU) 2016/679, ***Verordening (EU) 2018/1725*** van het Europees Parlement en de Raad[9] ***en Richtlijn 2002/58/EG*** zijn 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 ***die zij bij het verlenen*** van andere diensten ***hebben verkregen,*** combineren met persoonsgegevens ***die worden verwerkt voor de verlening van*** diensten die binnen het toepassingsgebied van deze verordening vallen. ***Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnees voor digitale identiteit moeten logisch worden gescheiden van andere door de aanbieder van de Europese portemonnee voor digitale identiteit opgeslagen gegevens. Deze verordening mag niet beletten dat aanbieders 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 Europese portemonnees voor digitale identiteit en andere gegevens die in het bezit zijn van de aanbieder. Onverminderd Verordening (EU) 2016/679 specificeert deze verordening de toepassing van de beginselen van doelbinding, minimale gegevensverwerking en gegevensbescherming door ontwerp en door standaardinstellingen.***

---

[9] ***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).

*(13) Europese portemonnees voor digitale identiteit moeten een in het ontwerp ingebouwd gemeenschappelijk dashboard hebben om een hogere mate van transparantie en privacy te waarborgen en ervoor te zorgen dat gebruikers meer controle hebben over hun persoonsgegevens. Die functie moet een gemakkelijke, gebruiksvriendelijke interface bieden met een overzicht van alle vertrouwende partijen waarmee de gebruiker gegevens deelt, met inbegrip van attributen, en het soort gegevens dat met elke vertrouwende partij wordt gedeeld. Ook moet de functie gebruikers de mogelijkheid bieden alle transacties die met de Europese portemonnee voor digitale identiteit zijn uitgevoerd te raadplegen, waarbij ten minste de volgende gegevens beschikbaar moeten zijn: het tijdstip en de datum van de transactie, de identificatie van de wederpartij, de gevraagde persoonsgegevens en de gedeelde gegevens. Die informatie moet worden opgeslagen, zelfs als de transactie niet werd voltooid. Het mag niet mogelijk zijn de authenticiteit van de informatie in de transactiegeschiedenis te verwerpen. Een dergelijke functie moet standaard ingeschakeld zijn. De functie moet gebruikers in staat stellen gemakkelijk een verzoek te doen om persoonsgegevens onmiddellijk te laten wissen door een vertrouwende partij overeenkomstig artikel 17 van Verordening (EU) 2016/679 en gemakkelijk de vertrouwende partij bij de bevoegde nationale gegevensbeschermingsautoriteit aan te geven indien een vermeend onrechtmatig of verdacht verzoek om persoonsgegevens rechtstreeks via het Europese portemonnee voor digitale identiteit wordt ontvangen.*

*(14) De lidstaten moeten verschillende technologieën voor privacybescherming, zoals "zero-knowledge proof", in de Europese portemonnee voor digitale identiteit integreren. Met die cryptografische methoden moet een vertrouwende partij kunnen vaststellen dat een bepaalde verklaring die is gebaseerd op de identificatiegegevens en de attestering van attributen van de persoon, waarheidsgetrouw is, zonder de gegevens te onthullen waarop de verklaring is gebaseerd, zodat de privacy van de gebruiker wordt beschermd.*

(15) ***Deze verordening zet*** geharmoniseerde voorwaarden uiteen voor het opzetten van een kader voor door de lidstaten ***aan te bieden*** Europese portemonnees voor digitale identiteit. Alle ***burgers*** en ▌ ingezetenen van de Unie zoals gedefinieerd in het nationaal recht ***moeten in staat worden gesteld om*** gegevens over hun identiteit ***veilig op te vragen, te selecteren, te combineren, op te slaan, te wissen, te*** delen ***en aan te bieden, en op een gebruikersvriendelijke en gemakkelijke manier te verzoeken hun persoonsgegevens te wissen,*** waarbij de gebruiker volledige controle heeft***, terwijl persoonsgegevens ook selectief kunnen worden verstrekt***. ***Deze verordening weerspiegelt de gedeelde Europese waarden, eerbiedigt de grondrechten en omvat juridische waarborgen en aansprakelijkheid, en beschermt aldus onze democratische samenlevingen en de burgers en ingezetenen van de Unie.*** De op die doelstellingen gerichte technologieën moeten worden ontwikkeld met het oog op het hoogste niveau van beveiliging, ***privacy*****,** gebruiksgemak***, toegankelijkheid,*** brede inzetbaarheid ***en naadloze interoperabiliteit***. De lidstaten moeten voor al hun burgers en ingezetenen gelijke toegang tot elektronische identificatie waarborgen. ***De lidstaten mogen noch direct, noch indirect de toegang tot publieke of private diensten beperken voor natuurlijke of rechtspersonen die ervoor kiezen geen gebruik te maken van Europese portemonnees voor digitale identiteit, en moeten passende alternatieve oplossingen beschikbaar stellen.***

***(16) De lidstaten moeten gebruikmaken van de mogelijkheden die deze verordening biedt om, onder hun verantwoordelijkheid, Europese portemonnees voor digitale identiteit aan te bieden voor gebruik door de natuurlijke personen en rechtspersonen die op hun grondgebied verblijven. Om de lidstaten flexibiliteit te bieden en de nieuwste technologie ten volle te benutten, moet deze verordening ervoor zorgen dat Europese portemonnees voor digitale identiteit rechtstreeks kunnen worden aangeboden door een lidstaat, krachtens een mandaat van een lidstaat, of onafhankelijk van een lidstaat, maar erkend door die lidstaat.***

*(17)* ***Met het oog op registratie moeten vertrouwende partijen de informatie verstrekken die nodig is voor hun elektronische identificatie en authenticatie bij Europese portemonnees voor digitale identiteit. Wanneer vertrouwende partijen verklaren dat zij voornemens zijn de Europese portemonnee voor digitale identiteit te gebruiken, moeten zij informatie verstrekken over de eventuele gegevens die zij zullen opvragen om hun diensten te verlenen en over de reden voor het verzoek. Door vertrouwende partijen te registreren, kunnen lidstaten gemakkelijker de rechtmatigheid van de activiteiten van de vertrouwende partijen overeenkomstig het Unierecht controleren. De in deze verordening vastgestelde registratie-verplichting mag geen afbreuk doen aan de verplichtingen uit hoofde van ander Unie- of nationaal recht, zoals de krachtens Verordening (EU) 2016/679 aan de betrokkenen te verstrekken informatie. Vertrouwende partijen moeten voldoen aan de waarborgen van de artikelen 35 en 36 van die verordening, met name door gegevensbeschermingseffectbeoordelingen uit te voeren en voorafgaand aan de gegevensverwerking de bevoegde gegevensbeschermingsautoriteiten te raadplegen wanneer uit gegevensbeschermingseffectbeoordelingen blijkt dat de verwerking een hoog risico met zich zou meebrengen. Dergelijke waarborgen moeten de rechtmatige verwerking van persoonsgegevens door vertrouwende partijen ondersteunen, met name met betrekking tot bijzondere categorieën van gegevens, zoals gezondheidsgegevens.***

***De registratie van vertrouwende partijen is bedoeld om de transparantie en het vertrouwen in het gebruik van Europese portemonnees voor digitale identiteit te vergroten. De registratie moet kosteneffectief zijn en in verhouding staan tot de daaraan verbonden risico's, opdat dienstverleners zich daadwerkelijk registreren. In dat verband moet de registratie kunnen plaatsvinden op basis van geautomatiseerde procedures, waarbij bijvoorbeeld de lidstaten op bestaande registers kunnen vertrouwen en deze kunnen gebruiken, en mag er geen voorafgaande authorisatieprocedure zijn. Het registratieproces moet een verscheidenheid aan gebruikssituaties mogelijk maken die kunnen verschillen wat betreft de werkwijze, online of in offlinemodus, of de verplichting tot authenticatie van apparaten voor koppeling aan de Europese portemonnee voor digitale identiteit. De registratie is uitsluitend bedoeld voor vertrouwende partijen die diensten verlenen door middel van digitale interactie.***

***(18)*** ***Het beschermen van burgers en ingezetenen van de Unie tegen ongeoorloofd of frauduleus gebruik van Europese portemonnees voor digitale identiteit is van groot belang om het vertrouwen in en het brede gebruik van Europese portemonnees voor digitale identiteit te waarborgen. Gebruikers moeten doeltreffend worden beschermd tegen misbruik. Met name wanneer een nationale rechterlijke instantie in het kader van een andere procedure feiten vaststelt die de basis vormen voor frauduleus of anderszins illegaal gebruik van een Europese portemonnee voor digitale identiteit, moeten de toezichthoudende organen die bevoegd zijn toezicht te houden op afgevers van Europese portemonnees voor digitale identiteit, na kennisgeving de nodige maatregelen nemen om ervoor te zorgen dat de registratie van de vertrouwende partij en de opname van vertrouwende partijen in het authenticatiemechanisme worden ingetrokken of opgeschort totdat de kennisgevende autoriteit bevestigt dat de vastgestelde onregelmatigheden zijn verholpen.***

▌

(19) Alle ***Europese portemonnees voor digitale identiteit*** moeten gebruikers in staat stellen om zich online en in offlinemodus grensoverschrijdend te identificeren en te authenticeren om toegang tot een breed scala publieke en private diensten te krijgen. Onverminderd de prerogatieven van de lidstaten betreffende de identificatie van hun burgers en ingezetenen, kunnen ***Europese portemonnees voor digitale identiteit*** ook tegemoetkomen aan de institutionele behoeften van overheidsinstanties, internationale organisaties en de instellingen, organen en instanties van de Unie. Authenticatie in offlinemodus is van belang in veel sectoren, zoals de gezondheidssector waar diensten vaak via persoonlijke interactie worden verleend, en waarvoor e-recepten op QR-codes of soortgelijke technologieën moet kunnen worden vertrouwd om de authenticiteit te verifiëren. Op basis van het betrouwbaarheidsniveau "hoog" ***met betrekking tot stelsels voor elektronische identificatie*** moeten ***de Europese portemonnees voor digitale identiteit*** kunnen gebruikmaken van het potentieel van fraudebestendige oplossingen, zoals beveiligde elementen, opdat de beveiligingsvoorschriften van deze verordening worden nageleefd. Met Europese portemonnees voor digitale identiteit moeten gebruikers ook in de hele Unie aanvaarde gekwalificeerde elektronische handtekeningen en zegels kunnen aanmaken en gebruiken. ***Natuurlijke personen die eenmaal in een Europese portemonnee voor digitale identiteit zijn ingestapt, moeten deze standaard en kosteloos kunnen gebruiken om met gekwalificeerde elektronische handtekeningen te kunnen ondertekenen, zonder dat zij daarvoor aanvullende administratieve procedures hoeven te doorlopen. Gebruikers moeten ook beweringen over of attributen van zichzelf kunnen ondertekenen of verzegelen.***

Met het oog op vereenvoudiging en kostenbesparingen voor personen en bedrijven in de hele ***Unie***, onder meer door de mogelijkheid van vertegenwoordigingsbevoegdheden en e-mandaten, moeten de lidstaten ***Europese portemonnees voor digitale identiteit aanbieden*** die berusten op gemeenschappelijke normen en technische specificaties om naadloze interoperabiliteit te waarborgen en ***de IT-beveiliging in toereikende mate te verhogen, de bestendigheid tegen cyberaanvallen te versterken en zo de potentiële risico's van de voortschrijdende digitalisering voor burgers en ingezetenen van de Unie en ondernemingen aanzienlijk te beperken***. Alleen de bevoegde instanties van de lidstaten kunnen een hoog ***niveau*** 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 moet ***bij het aanbieden van*** Europese portemonnees voor digitale identiteit ***worden gebruikgemaakt*** van de wettelijke identiteit van burgers of ingezetenen van de Unie of rechtspersonen. ***Het gebruik van de wettelijke identiteit mag niet beletten dat gebruikers van de Europese portemonnees voor digitale identiteit onder een pseudoniem toegang hebben tot diensten waar de wettelijke identiteit geen wettelijk vereiste voor authenticatie is. Het vertrouwen in Europese portemonnees voor digitale identiteit*** zou nog hoger worden als de verstrekkende ***en beherende*** partijen verplicht zijn passende technische en organisatorische maatregelen te treffen om ***het hoogste*** beveiligingsniveau te waarborgen dat in overeenstemming is met de risico's voor de rechten en vrijheden van natuurlijke personen, conform Verordening (EU) 2016/679.

*(20)* ***Alle natuurlijke personen moeten kosteloos kunnen gebruikmaken van een gekwalificeerde elektronische handtekening voor niet-professionele doeleinden. De lidstaten moeten gerechtvaardigde, met de vastgestelde risico's evenredige maatregelen kunnen nemen om te voorkomen dat natuurlijke personen kosteloos gebruikmaken van gekwalificeerde elektronische handtekeningen voor professionele doeleinden.***

*(21)* ***Om de invoering en het gebruik van Europese portemonnees voor digitale identiteit te vergemakkelijken is het nuttig dat deze naadloos worden geïntegreerd in het ecosysteem van publieke en private digitale diensten dat reeds op nationaal, lokaal of regionaal niveau bestaat. Om dat doel te bereiken, moeten de lidstaten wettelijke en organisatorische maatregelen kunnen nemen om instellingen die Europese portemonnees voor digitale identiteit aanbieden meer flexibiliteit te bieden en meer functionaliteiten van Europese portemonnees voor digitale identiteit mogelijk te maken dan de in deze verordening vastgelegde functionaliteiten, onder meer door een betere interoperabiliteit met bestaande nationale elektronische identificatiemiddelen. De extra functionaliteiten mogen geenszins ten koste gaan van het aanbod van de kernfuncties van Europese portemonnees voor digitale identiteit, zoals vastgelegd in deze verordening, en mogen evenmin tot doel hebben bestaande nationale oplossingen aan te prijzen ten koste van Europese portemonnees voor digitale identiteit. Aangezien de extra functionaliteiten verder gaan dan deze verordening, vallen zij niet onder de in deze verordening vastgestelde bepalingen inzake grensoverschrijdend vertrouwen in elkaars Europese portemonnees voor digitale identiteit.***

***(22) Europese portemonnees voor digitale identiteit moeten een functionaliteit bevatten om door gebruikers gekozen en beheerde pseudoniemen te genereren, waarmee gebruikers zich kunnen authenticeren bij toegang tot onlinediensten.***

(23) Met het oog op een hoog niveau van beveiliging en betrouwbaarheid worden in deze verordening de vereisten voor de Europese portemonnees voor digitale identiteit vastgesteld. Of de Europese portemonnees voor digitale identiteit in overeenstemming zijn met deze vereisten, moet worden gecertificeerd door geaccrediteerde ***conformiteitsbeoordeling***sinstanties die door de lidstaten zijn aangewezen.

***(24) Om uiteenlopende benaderingen te voorkomen en de uitvoering van de vereisten van deze verordening te harmoniseren, moet de Europese Commissie, teneinde Europese portemonnees voor digitale identiteit te certificeren, uitvoeringshandelingen vaststellen om een lijst met referentienormen vast te stellen en, waar nodig, specificaties en procedures vast te stellen met als doel om die vereisten nader te omschrijven met technische specificaties. Voor zover de certificering van de conformiteit van de Europese portemonnees voor digitale identiteit met de desbetreffende cyberbeveiligingsvereisten niet wordt gedekt door de bestaande regelingen voor cyberbeveiligingscertificering die in deze verordening worden genoemd, en wat betreft andere dan cyberbeveiligingsvereisten die van toepassing zijn op Europese portemonnees voor digitale identiteit, moeten de lidstaten nationale certificeringsregelingen vaststellen overeenkomstig de geharmoniseerde vereisten die in en krachtens deze verordening zijn vastgesteld. De lidstaten moeten hun ontwerpen van nationale certificeringsregelingen toesturen aan de Europese samenwerkingsgroep voor digitale identiteit, die adviezen en aanbevelingen moet kunnen afgeven.***

***(25) De certificering van conformiteit met de in deze verordening vastgestelde cyberbeveiligingsvereisten moet, indien beschikbaar, steunen op de desbetreffende Europese regelingen voor cyberbeveiligingscertificering die zijn vastgesteld op grond van Verordening (EU) 2019/881 van het Europees Parlement en de Raad[10], waarin een vrijwillig Europees kader voor cyberbeveiligingscertificering voor ICT-producten, -processen en -diensten is vastgesteld.***

***(26) Om veiligheidsrisico's voortdurend te beoordelen en te beperken, moeten de gecertificeerde Europese portemonnees voor digitale identiteit regelmatig worden onderworpen aan kwetsbaarheidsbeoordelingen die erop gericht zijn de kwetsbaarheden in de gecertificeerde product-, proces- en dienstengerelateerde onderdelen van de Europese portemonnee voor digitale identiteit op te sporen.***

***(27) Door gebruikers en bedrijven te beschermen tegen cyberbeveiligingsrisico's, moeten de essentiële cyberbeveiligingsvereisten van deze verordening ook bijdragen aan een betere bescherming van de persoonsgegevens en privacy van personen. Synergieën op het gebied van zowel normalisatie als certificering op het gebied van cyberbeveiliging moeten in aanmerking worden genomen in het kader van de samenwerking tussen de Commissie, de Europese normalisatieorganisaties, het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), het Europees Comité voor gegevensbescherming, opgericht bij Verordening (EU) 2016/679, en de nationale toezichthoudende autoriteiten voor gegevensbescherming.***

---

**10** 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).

*(28)* ***Het instappen van burgers en ingezetenen van de Unie in de Europese portemonnee voor digitale identiteit moet worden gestimuleerd door gebruik te maken van op betrouwbaarheidsniveau "hoog" afgegeven elektronische identificatiemiddelen. Op op betrouwbaarheidsniveau "substantieel" afgegeven elektronische identificatiemiddelen mag uitsluitend een beroep worden gedaan indien de geharmoniseerde technische specificaties en procedures waarbij gebruik wordt gemaakt van op betrouwbaarheidsniveau "substantieel" afgegeven elektronische identificatiemiddelen in combinatie met andere aanvullende middelen voor identiteitsverificatie het mogelijk maken te voldoen aan de eisen van deze verordening met betrekking tot betrouwbaarheidsniveau "hoog". Dergelijke aanvullende middelen moeten betrouwbaar en gemakkelijk te gebruiken zijn en kunnen worden gebaseerd op de mogelijkheid om gebruik te maken van instapprocedures op afstand, gekwalificeerde certificaten ondersteund door gekwalificeerde elektronische handtekeningen, gekwalificeerde elektronische attestering van attributen of een combinatie daarvan. Om ervoor te zorgen dat de Europese portemonnees voor digitale identiteit voldoende breed gebruikt worden, moeten bij uitvoeringshandelingen geharmoniseerde technische specificaties en procedures worden vastgesteld waarmee gebruikers kunnen instappen met behulp van elektronische identificatiemiddelen, met inbegrip van die welke op betrouwbaarheidsniveau "substantieel" worden afgegeven.***

***(29) Het doel van deze verordening is de gebruiker te voorzien van een volledig mobiele, veilige en gebruiksvriendelijke Europese portemonnee voor digitale identiteit. In afwachting van gecertificeerde niet-manipuleerbare oplossingen, zoals beveiligde elementen in de apparaten van de gebruikers, moeten de Europese portemonnees voor digitale identiteit voor de bescherming van het cryptografisch materiaal en andere gevoelige gegevens bij wijze van overgangsmaatregel kunnen gebruikmaken van gecertificeerde externe beveiligde elementen of van aangemelde elektronische identificatiemiddelen op betrouwbaarheidsniveau "hoog" om aan te tonen dat met betrekking tot het betrouwbaarheidsniveau van de Europese portemonnee voor digitale identiteit aan de toepasselijke eisen van deze verordening wordt voldaan. Deze verordening mag geen afbreuk doen aan de nationale voorwaarden met betrekking tot de afgifte en gebruik van een gecertificeerd extern beveiligd element indien de overgangsmaatregel daarop berust.***

(30) Europese portemonnees voor digitale identiteit moeten het hoogste ***gegevens-beschermings- en*** beveiligingsniveau ***voor elektronische identificatie en authenticatie bij toegang tot publieke en private diensten*** waarborgen, ongeacht of de gegevens lokaal of in de cloud worden opgeslagen; de verschillende risiconiveaus moeten daarbij terdege in acht worden genomen. ▌

***(31) Europese portemonnees voor digitale identiteit moeten "secure-by-design" zijn en geavanceerde beveiligingskenmerken gebruiken om bescherming te bieden tegen identiteits- en andere gegevensdiefstal, Denial of Service, en andere cyberdreigingen. Die beveiliging moet geavanceerde versleutelings- en opslagmethoden omvatten die alleen toegankelijk zijn voor en alleen ontcijferbaar zijn door de gebruiker, en moeten gebaseerd zijn op eind-tot-eindversleutelde communicatie met andere Europese portemonnees voor digitale identiteit en vertrouwende partijen. Daarnaast moeten Europese portemonnees voor digitale identiteit veilige, uitdrukkelijke en actieve bevestiging van de gebruiker vereisen voor de verrichtingen die via de Europese portemonnee voor digitale identiteit worden uitgevoerd.***

*(32)* ***Het kosteloze gebruik van Europese portemonnees voor digitale identiteit mag niet resulteren in het verwerken van gegevens die verder gaat dan gegevens die noodzakelijk zijn voor het verlenen van diensten in verband met Europese portemonnees voor digitale identiteit. Deze verordening mag niet toestaan dat de aanbieder van de Europese portemonnee voor digitale identiteit persoonsgegevens die zijn opgeslagen in of voortkomen uit het gebruik van de Europese portemonnee voor digitale identiteit verwerkt voor andere doeleinden dan het verlenen van diensten in verband met de Europese portemonnee voor digitale identiteit. Ter waarborging van de privacy moeten aanbieders van Europese portemonnees voor digitale identiteit onzichtbaarheid garanderen door geen gegevens te verzamelen over en geen inzicht te krijgen in de transacties van de gebruikers van de Europese portemonnee voor digitale identiteit. Dergelijke onzichtbaarheid houdt in dat de aanbieders de details van de door de gebruiker verrichte transacties niet mogen kunnen zien. In specifieke gevallen kunnen aanbieders van Europese portemonnees voor digitale identiteit, op basis van de uitdrukkelijke voorafgaande toestemming van de gebruiker in elk van die specifieke gevallen en met volledige inachtneming van Verordening (EU) 2016/679, echter wel toegang krijgen tot de informatie die noodzakelijk is voor het verlenen van een concrete dienst in verband met Europese portemonnees voor digitale identiteit.***

*(33) De transparantie van Europese portemonnees voor digitale identiteit en de verantwoordingsplicht van de aanbieders daarvan zijn fundamenteel om maatschappelijk vertrouwen op te bouwen en de aanvaarding van het kader in de hand te werken. De werking van de Europese portemonnees voor digitale identiteit moet derhalve transparant zijn en moet het in het bijzonder mogelijk maken de verwerking van persoonsgegevens te verifiëren. Daartoe moeten de lidstaten de broncode van de softwarecomponenten van de gebruikerstoepassing van Europese portemonnees voor digitale identiteit openbaar maken, ook van die welke verband houden met de verwerking van persoonsgegevens en gegevens van rechtspersonen. Met de openbaarmaking van deze broncode onder een opensourcelicentie moet de maatschappij, met inbegrip van gebruikers en ontwikkelaars, de werking ervan kunnen begrijpen en de code kunnen controleren en evalueren. Dit zou ook het vertrouwen van gebruikers in het ecosysteem van Europese portemonnees voor digitale identiteit vergroten en bijdragen aan de beveiliging ervan, omdat iedereen dan kwetsbaarheden en fouten in de code kan melden. Dit zou aanbieders in het algemeen moeten stimuleren om een zeer sterk beveiligd product te leveren en in stand te houden. Er zijn echter bepaalde gevallen waarin de lidstaten de openbaarmaking van de broncode van de gebruikte softwarebibliotheken, het communicatiekanaal of andere elementen die niet op het apparaat van de gebruiker worden gehost kunnen beperken, om terdege gemotiveerde redenen, met name ter wille van de openbare veiligheid.*

***(34)*** ***De gebruikers moeten het exclusieve recht en de exclusieve keuze hebben om Europese portemonnees voor digitale identiteit te gebruiken en om met het gebruik ervan te stoppen. De lidstaten moeten eenvoudige en veilige procedures uitwerken zodat de gebruikers kunnen verzoeken de geldigheid van een Europese portemonnee voor digitale identiteit onmiddellijk in te trekken. Bij overlijden van de gebruiker of bij stopzetting van de activiteiten van een rechtspersoon, moet een mechanisme worden opgezet waarlangs de bevoegde instantie die de nalatenschap van de natuurlijke persoon of de activa van de rechtspersoon afhandelt, kan verzoeken om de onmiddellijke herroeping van de Europese portemonnee voor digitale identiteit.***

***(35)*** ***Om ervoor te zorgen dat de Europese portemonnees voor digitale identiteit voldoende breed worden gebruikt en een breder gebruik van digitale identiteiten te bevorderen, moeten de lidstaten niet alleen duidelijk maken wat de voordelen zijn van de betreffende diensten, maar moeten zij ook in samenwerking met de private sector, onderzoekers en academici opleidingsprogramma's ontwikkelen om de digitale vaardigheden van burgers en ingezetenen te versterken, met name gericht op kwetsbare groepen zoals mensen met een handicap en ouderen. De lidstaten moeten door middel van communicatiecampagnes ook het bewustzijn vergroten over de voordelen en risico's van de Europese portemonnees voor digitale identiteit.***

(36) Om het Europees kader voor digitale identiteit toekomstbestendig en open voor innovatie en technologische ontwikkelingen te houden, ***worden*** de lidstaten ***gezamenlijk*** aangemoedigd om 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. ***Kleine en middelgrote ondernemingen, start-ups en individuele innovatoren en onderzoekers, maar ook andere belanghebbenden uit de betrokken sectoren*** moeten worden gestimuleerd om aan die omgeving deel te nemen. ***Zulke initiatieven moeten ertoe bijdragen dat de aan de burgers en ingezetenen van de Unie te verstrekken Europese portemonnees voor digitale identiteit aan de regelgeving voldoen en technisch robuust zijn, zodat wordt voorkomen dat er oplossingen worden ontwikkeld die niet aan het Unierecht inzake gegevensbescherming voldoen of die beveiligingskwetsbaarheden vertonen***.

(37) Bij Verordening (EU) 2019/1157 van het Europees Parlement en de Raad[11] wordt de beveiliging van identiteitskaarten uiterlijk in augustus 2021 verhoogd door middel van strengere beveiligingskenmerken. De lidstaten moeten overwegen of het haalbaar is deze op grond van stelsels voor elektronische identificatie aan te melden, met het doel de grensoverschrijdende beschikbaarheid van elektronische identificatiemiddelen te verruimen.

---

**11** 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).

(38) De aanmeldingsprocedure van stelsels voor elektronische identificatie moet worden vereenvoudigd en versneld om toegang tot gemakkelijke, betrouwbare, veilige en innovatieve authenticatie- en identificatiemethoden te bevorderen en, waar van belang, private 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.

(39) 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 zijn bedoeld om de samenwerking tussen de lidstaten op het gebied van beveiliging en interoperabiliteit van hun aangemelde stelsels voor elektronische identificatie te bevorderen.

(40) De lidstaten moeten met de nieuwe en flexibele instrumenten toezien op de naleving van deze verordening en van de op grond daarvan vastgestelde uitvoeringshandelingen. De lidstaten moeten op grond van deze verordening gebruik kunnen maken van verslagen en beoordelingen van geaccrediteerde conformiteitsbeoordelingsinstanties, ***zoals bedoeld in het kader van*** de 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 Verordening (EU) nr. 910/2014.

(41) Aanbieders van ***publieke*** diensten gebruiken de ▌ persoonsidentificatiegegevens die beschikbaar zijn uit elektronische identificatie***middelen*** overeenkomstig Verordening (EU) nr. 910/2014 ***om de elektronische identiteit van de gebruikers van andere lidstaten te matchen met de persoonsidentificatiegegevens die worden verstrekt aan de*** gebruikers ***in de*** lidstaat waar ***het grensoverschrijdende*** identiteits***matchingsproces wordt uitgevoerd***. Ondanks het gebruik van de in het kader van de aangemelde stelsels voor elektronische identificatie verstrekte ***minimale*** reeks gegevens, ***is, wanneer lidstaten als vertrouwende partijen optreden, in veel gevallen voor een nauwkeurige identiteitsmatching*** evenwel extra informatie over de gebruiker ***nodig*** en moeten er op nationaal niveau specifieke ***aanvullende*** unieke identificatieprocedures ***worden uitgevoerd***. Met het oog op een ruimere bruikbaarheid van elektronische identificatiemiddelen, ***een betere verstrekking van online-overheidsdiensten en meer rechtszekerheid met betrekking tot de elektronische identiteit van de gebruikers***, moet Verordening (EU) nr. 910/2014 ▌ ***de lidstaten verplichten specifieke onlinemaatregelen te nemen om eenduidige identiteitsmatching te waarborgen wanneer gebruikers toegang willen verkrijgen tot grensoverschrijdende online-overheidsdiensten***.

***(42)*** ***Bij het ontwikkelen van de Europese portemonnees voor digitale identiteit is het van fundamenteel belang dat de behoeften van de gebruikers in aanmerking worden genomen. Er moeten zinvolle praktijkvoorbeelden en onlinediensten beschikbaar zijn die steunen op de Europese portemonnees voor digitale identiteit. Ten behoeve van het gebruiksgemak en ter waarborging van de grensoverschrijdende beschikbaarheid van dergelijke diensten is het belangrijk dat maatregelen worden genomen 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 dat doel te bereiken. Die richtsnoeren moeten worden opgesteld met inachtneming van het interoperabiliteitskader van de Unie. De lidstaten moeten bij de aanneming van die richtsnoeren een leidende rol spelen.***

(43) ***Overeenkomstig*** Richtlijn (EU) 2019/882 van het Europees Parlement en de Raad[12] 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 die diensten worden gebruikt, op voet van gelijkheid met andere consumenten te gebruiken.

---

**12** 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, ELI: http://data.europa.eu/eli/dir/2019/882/oj).

***(44)*** ***Met het oog op de doeltreffende handhaving van deze verordening moet een minimum worden vastgesteld voor het maximumbedrag van administratieve boetes voor verleners van zowel gekwalificeerde als niet-gekwalificeerde vertrouwensdiensten. De lidstaten moeten maatregelen invoeren waarbij doeltreffende, evenredige en afschrikkende sancties worden opgelegd. Bij het bepalen van de sancties moet rekening worden gehouden met de omvang van de betrokken entiteiten, hun bedrijfsmodel, en de ernst van de inbreuken.***

***(45)*** ***De lidstaten moeten regels vaststellen over sancties voor inbreuken zoals directe of indirecte praktijken die leiden tot verwarring tussen niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten, of tot misbruik van het vertrouwensmerk van de EU door verleners van niet-gekwalificeerde vertrouwensdiensten. Het vertrouwensmerk van de EU mag niet worden gebruikt in omstandigheden die direct of indirect de indruk kunnen wekken dat door die verleners aangeboden niet-gekwalificeerde vertrouwensdiensten gekwalificeerd zijn.***

(46) 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 ***Unie***recht ***of het nationaal*** recht vormvereisten worden gesteld. Daarenboven dient zij de nationale vormvereisten voor publieke registers, met name handelsregisters en kadasters, onverlet te laten.

(47) Het verlenen en gebruiken van vertrouwensdiensten ***en de voordelen die hieruit volgen wat betreft gemak en rechtszekerheid bij grensoverschrijdende transacties, met name wanneer gekwalificeerde vertrouwensdiensten worden gebruikt***, worden steeds belangrijker voor de internationale handel en samenwerking. Internationale partners van de Unie zetten op Verordening (EU) nr. 910/2014 geïnspireerde vertrouwenskaders op. ▌ Om de erkenning van ***gekwalificeerde vertrouwens***diensten en van de verleners daarvan te faciliteren, kan de Commissie uitvoeringshandelingen vaststellen om de voorwaarden te bepalen waaronder vertrouwenskaders van derde landen beschouwd kunnen worden als gelijkwaardig aan het vertrouwenskader voor gekwalificeerde vertrouwensdiensten en verleners daarvan in deze verordening***. Een dergelijke aanpak moet*** een aanvulling vormen op ▌ de mogelijkheid ***van*** wederzijdse erkenning van in de Unie en in derde landen gevestigde vertrouwensdiensten en verleners daarvan overeenkomstig artikel 218 van het Verdrag betreffende de werking van de Europese Unie (VWEU). ***Bij het bepalen van de voorwaarden waaronder vertrouwenskaders van derde landen als gelijkwaardig kunnen worden beschouwd aan het vertrouwenskader voor gekwalificeerde vertrouwensdiensten en verleners daarvan in het kader van Verordening (EU) nr. 910/2014, moet ook gelden dat aan de desbetreffende bepalingen van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[13] en van Verordening (EU) 2016/679 moet worden voldaan, alsmede dat vertrouwenslijsten moeten worden gebruikt als essentiële elementen om vertrouwen op te bouwen.***

▌

---

**13** Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

***(48) Deze verordening moet bevorderlijk zijn voor de keuze en de overstap tussen Europese portemonnees voor digitale identiteit indien een lidstaat meerdere Europese portemonnees voor digitale identiteit heeft goedgekeurd op zijn grondgebied. Om in dergelijke situaties lock-ineffecten te voorkomen, moeten de aanbieders van Europese portemonnees voor digitale identiteit er, indien dat technisch haalbaar is, op verzoek van gebruikers van een Europese portemonnee voor digitale identiteit voor zorgen dat gegevens doeltreffend kunnen worden overgedragen, en mogen zij geen contractuele, economische of technische belemmeringen kunnen opwerpen die een vlotte overstap tussen verschillende Europese portemonnees voor digitale identiteit verhinderen of ontmoedigen.***

***(49)*** ***Met het oog op de goede werking van de Europese portemonnees voor digitale identiteit moeten aanbieders van Europese portemonnees voor digitale identiteit kunnen rekenen op doeltreffende interoperabiliteit en rechtvaardige, redelijke en niet-discriminerende voorwaarden opdat de Europese portemonnees voor digitale identiteit toegang kunnen verkrijgen tot specifieke hardware- en softwarekenmerken van mobiele apparaten. Het kan hierbij met name gaan om componenten zoals antennes voor draadloze korteafstandscommunicatie (Near Field Communication) en beveiligde elementen (waaronder universele chipkaarten, ingebouwde beveiligde elementen, microSD-kaarten en Bluetooth met laag energieverbruik). De toegang tot die componenten kan onder de controle vallen van exploitanten van mobiele netwerken en producenten van apparatuur. Producenten van originele mobiele apparaten of aanbieders van elektronische communicatiediensten mogen de toegang tot die componenten derhalve niet weigeren, indien deze noodzakelijk is om de diensten van Europese portemonnees voor digitale identiteit te verlenen. Daarnaast moeten op ondernemingen die zijn aangewezen als poortwachter voor de overeenkomstig Verordening (EU) 2022/1925 van het Europees Parlement en de Raad[14] door de Commissie vastgestelde kernplatformdiensten, de specifieke bepalingen van die verordening van toepassing blijven, voortbouwend op artikel 6, lid 7, van die verordening.***

---

14 ***Verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (digitalemarktenverordening) (PB L 265 van 12.10.2022, blz. 1).***

(50) Om de aan verleners van vertrouwensdiensten opgelegde cyberbeveiligingsvoorschriften te stroomlijnen en opdat die verleners en hun respectieve bevoegde autoriteiten baat kunnen hebben bij het bij Richtlijn ***(EU) 2022/2555*** opgerichte wettelijke kader, moeten vertrouwensdiensten passende technische en organisatorische maatregelen nemen overeenkomstig die richtlijn, zoals maatregelen tegen systeemfalen, menselijke fouten, kwaadwillige acties of natuurverschijnselen, met het oog op het beheren van de risico's voor de veiligheid van de netwerk- en informatiesystemen die die aanbieders gebruiken om hun diensten te verlenen, en met het oog op het melden van significante incidenten en cyberdreigingen overeenkomstig die richtlijn. Wat het melden van incidenten betreft, moeten verleners 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 die zich voordoen bij persoonsidentificatie. De vereisten inzake het risicobeheer en de verslagleggingsverplichtingen op het gebied van cyberbeveiliging overeenkomstig Richtlijn ***(EU) 2022/2555*** moeten als aanvullend op de overeenkomstig deze verordening aan verleners van vertrouwensdiensten opgelegde voorschriften worden beschouwd. Indien van toepassing, moeten de overeenkomstig Richtlijn ***(EU) 2022/2555*** 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. Deze verordening doet geen afbreuk aan de verplichting tot het melden van inbreuken op persoonsgegevens overeenkomstig Verordening (EU) 2016/679.

(51) De nodige aandacht moet worden besteed aan het waarborgen van doeltreffende samenwerking tussen de overeenkomstig artikel 46 ter van Verordening (EU) nr. 910/2014 aangewezen toezichthoudende organen en de overeenkomstig artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of opgerichte bevoegde autoriteiten. Indien het toezichthoudend orgaan geen bevoegde autoriteit is, moeten het orgaan en de bevoegde autoriteit nauw en tijdig samenwerken door de nodige informatie uit te wisselen om een doeltreffend toezicht te waarborgen en ervoor te zorgen dat de verleners van vertrouwensdiensten voldoen aan de eisen van Verordening (EU) nr. 910/2014 en van Richtlijn ***(EU) 2022/2555***. De overeenkomstig Verordening (EU) nr. 910/2014 aangewezen toezichthoudende organen moeten met name van de overeenkomstig Richtlijn ***(EU) 2022/2555*** aangewezen of opgerichte bevoegde autoriteiten kunnen verlangen dat zij de nodige informatie verstrekken om een gekwalificeerde status toe te kennen en om toezichtmaatregelen te nemen om na te gaan of de verleners van vertrouwensdiensten voldoen aan de toepasselijke eisen van ***Richtlijn (EU) 2022/2555***, of van hen kunnen verlangen dat zij een niet-naleving verhelpen.

(52) 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 verleners van vertrouwensdiensten in de Unie ook nieuwe afzetmogelijkheden kunnen openen voor het aanbieden van nieuwe Uniebrede diensten voor elektronisch aangetekende bezorging. ***Om*** ervoor te zorgen dat ***de gegevens die met behulp van een 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 ***volstaat***. ***De lidstaten moeten verleners 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 verleners van gekwalificeerde vertrouwensdiensten gegevens voor elektronisch aangetekende bezorging gemakkelijk kunnen worden uitgewisseld en eerlijke praktijken op de interne markt worden bevorderd.***

(53) Meestal kunnen burgers en ingezetenen van de Unie niet veilig en met een hoog niveau van gegevensbescherming grensoverschrijdend digitale informatie uitwisselen met betrekking tot hun identiteit, zoals hun adres, leeftijd en beroepskwalificaties, rijbewijs en andere vergunningen en betaalgegevens.

(54) Het moet mogelijk zijn betrouwbare ***elektronische*** attributen af te geven en te verwerken, de regeldruk te helpen verlagen, en burgers en ingezetenen van de Unie die attributen in hun private en publieke transacties te laten gebruiken. Burgers en ingezetenen van de Unie moeten bijvoorbeeld kunnen aantonen dat zij beschikken over een geldig rijbewijs dat door een instantie in een lidstaat is afgegeven, wat door de bevoegde autoriteiten in andere lidstaten kan worden geverifieerd en vertrouwd, en ze moeten hun socialezekerheidsgegevens of toekomstige digitale reisdocumenten grensoverschrijdend kunnen gebruiken.

(55) Dienstverleners die ***geattesteerde attributen in elektronische vorm afgeven***, zoals diploma's, ***vergunningen, geboorte***aktes, ***of volmachten en mandaten om natuurlijke of rechtspersonen te vertegenwoordigen of namens hen op te treden,*** moeten ***worden beschouwd als verleners van vertrouwensdiensten voor de elektronische attestering van attributen***. ▌ Aan een elektronische attestering van attributen mag geen rechtsgevolg worden ontzegd op grond van het feit dat de attestering elektronisch is of niet aan de eisen voor gekwalificeerde elektronische attestering van attributen voldoet. Er 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 Unie- of nationaal 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.

(56) ***De*** brede beschikbaarheid en bruikbaarheid van ***Europese portemonnees voor digitale identiteit moeten*** het gebruik ervan ***en het vertrouwen erin bij zowel particulieren en*** private dienstverleners vergroten. ***Daarom*** moeten private vertrouwende partijen die diensten verlenen op het gebied van ***bijvoorbeeld*** vervoer, energie, bankwezen, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, ***telecommunicatie of onderwijs***, het gebruik van ***Europese portemonnees voor digitale identiteit*** aanvaarden voor de verlening van diensten waarvoor op grond van ***het Unie- of nationaal recht*** of van een contractuele verbintenis sterke gebruikersauthenticatie vereist is. ***Ieder verzoek door de vertrouwende partij om informatie van een Europese portemonnee voor digitale identiteit*** moet ***noodzakelijk zijn voor en in verhouding staan tot het bedoelde gebruik in een concreet geval, voldoen aan*** het beginsel van minimale gegevensverwerking***, en transparantie waarborgen wat betreft welke gegevens worden gedeeld en voor welke doeleinden***. ***Om het gebruik*** van Europese portemonnees voor digitale identiteit te vergemakkelijken en de aanvaarding ervan te bevorderen, moeten bij de uitrol ervan ***breed gedragen industriële normen en specificaties in acht worden genomen*** ▌.

***(57)*** ***Indien zeer grote onlineplatforms in de zin van artikel 33, lid 1, van Verordening (EU) 2022/2065 van het Europees Parlement en de Raad[15] verlangen dat gebruikers worden geauthenticeerd om toegang tot onlinediensten te krijgen, moeten die platforms worden verplicht het gebruik van Europese portemonnees voor digitale identiteit op vrijwillig verzoek van de gebruiker te aanvaarden. Gebruikers mogen niet worden verplicht een Europese portemonnee voor digitale identiteit te gebruiken om toegang tot private diensten te krijgen en hun toegang tot diensten mag niet worden beperkt of belemmerd op grond van het feit dat zij geen Europese portemonnee voor digitale identiteit gebruiken. Indien gebruikers de portemonnee wel willen gebruiken, moeten zeer grote onlineplatforms deze voor dat doel aanvaarden, met inachtneming van het beginsel van minimale gegevensverwerking en het recht van de gebruiker om vrij gekozen pseudoniemen te gebruiken. Vanwege het belang van zeer grote onlineplatforms als gevolg van hun bereik, met name wat het aantal afnemers van hun diensten en economische transacties betreft, is de verplichting om Europese portemonnees voor digitale identiteit te aanvaarden noodzakelijk om gebruikers beter tegen fraude te beschermen en om een hoog niveau van gegevensbescherming te waarborgen.***

***(58)*** ***Er moeten gedragscodes op Unieniveau worden ontwikkeld om bij te dragen tot de wijdverspreide beschikbaarheid en bruikbaarheid van elektronische identificatiemiddelen, inclusief Europese portemonnees voor digitale identiteit, binnen het toepassingsgebied van deze verordening. De gedragscodes moeten bevorderlijk zijn voor een brede aanvaarding van elektronische identificatiemiddelen, met inbegrip van Europese portemonnees voor digitale identiteit door dienstverleners die niet als zeer grote platforms worden aangemerkt en die voor gebruikersauthenticatie gebruik maken van elektronische identificatiediensten van derden.***

---

**15** Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening) (PB L 277 van 27.10.2022, blz. 1).

(59) ***Selectieve verstrekking is een concept dat de gegevenseigenaar in staat stelt slechts bepaalde delen van een grotere datareeks te verstrekken, zodat de ontvangende entiteit uitsluitend de informatie ontvangt die nodig is 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 verstrekt voor vertrouwende partijen. Het moet voor de gebruiker technisch mogelijk zijn om ***selectief attributen te verstrekken, ook wanneer zij afkomstig zijn van meerdere afzonderlijke elektronische attesteringen, en om hen te combineren en naadloos aan vertrouwende partijen te presenteren***. Dit kenmerk moet een basiskenmerk in het ontwerp ***van Europese portemonnees voor digitale identiteit*** worden en aldus het gebruiksgemak en de bescherming ***van persoonsgegevens – waaronder het beginsel van minimale gegevensverwerking –*** versterken.

***(60) Tenzij specifieke regels van het Unie- of nationaal recht vereisen dat gebruikers zichzelf identificeren, mag gebruikers niet worden verboden zich met een pseudoniem toegang tot diensten te verschaffen.***

(61) Attributen die de verleners 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 op nationaal niveau erkend zijn overeenkomstig het Unierecht of het nationaal recht met het oog op de beveiligde uitwisseling van geattesteerde attributen tussen aanbieders van identiteitsdiensten 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 moeten het gebruik kunnen omvatten van specifieke intermediairs of technische oplossingen 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, strekt ertoe dat verleners van gekwalificeerde vertrouwensdiensten die gekwalificeerde elektronische attesteringen van attributen afgeven, gemakkelijker de verplichtingen uit hoofde van Verordening (EU) nr. 910/2014 kunnen naleven. In een nieuwe bijlage bij die verordening moet een lijst worden opgenomen 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.***

(62) 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 een toekomstige verordening tot oprichting van de antiwitwasautoriteit, 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.

*(63)* ***Het rechtsgevolg van een elektronische handtekening mag niet worden betwist op grond van het feit dat de handtekening elektronisch is of niet voldoet aan de eisen voor gekwalificeerde elektronische handtekeningen. Het rechtsgevolg van elektronische handtekeningen moet evenwel worden vastgesteld bij nationaal recht, behalve voor de vereisten van deze verordening volgens welke het rechtsgevolg van een gekwalificeerde elektronische handtekening wordt aangemerkt als gelijkwaardig aan dat van een handgeschreven handtekening. Bij het bepalen van de rechtsgevolgen van elektronische handtekeningen dienen de lidstaten rekening te houden met het beginsel van evenredigheid tussen de juridische waarde van een te ondertekenen document en het beveiligingsniveau en de kosten die voor een elektronische handtekening vereist zijn. Om de toegankelijkheid en het gebruik van elektronische handtekeningen te vergroten, worden de lidstaten aangemoedigd om tevens het gebruik van geavanceerde elektronische handtekeningen in dagelijkse transacties te overwegen, daar waar zij een voldoende hoog niveau van beveiliging en vertrouwen bieden.***

***(64) Ter wille van de consistentie in de certificeringspraktijken in de Unie 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 de publieke of private organen die gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen hebben gecertificeerd, om een dergelijk middel tijdelijk opnieuw te certificeren voor een kortstondige certificeringsperiode, op basis van de resultaten van de vorige certificeringsprocedure, wanneer een dergelijke hercertificering om een andere reden dan een beveiligingsinbreuk of een -incident niet binnen de wettelijk vastgestelde termijn mogelijk is, onverminderd de verplichting om een kwetsbaarheidsbeoordeling uit te voeren en onverminderd de toepasselijke certificeringspraktijk.***

(65) De afgifte van certificaten voor websiteauthenticatie heeft als doel gebruikers een ***hoge mate van vertrouwen in de identiteit van de entiteit achter*** de website te bieden, ***ongeacht het platform dat voor het aangeven van die identiteit wordt gebruikt***. Die certificaten ***moeten bijdragen*** aan toenemend vertrouwen in online zaken doen, aangezien een geauthentiseerde website het vertrouwen van de gebruikers ***krijgt***. ▌ Websites die gebruikmaken van dergelijke certificaten, ***moeten*** dat op vrijwillige basis kunnen doen. ▌ Om van websiteauthenticatie een middel te maken om het vertrouwen ***te bevorderen***, de gebruikers betere ervaringen ***te bezorgen*** en de groei in de interne markt ***te bevorderen***, voorziet deze verordening in ***een vertrouwenskader met*** minimumverplichtingen inzake beveiliging en aansprakelijkheid voor ***gekwalificeerde*** certificaten voor websiteauthenticatie ***alsook voorschriften voor de afgifte van deze certificaten***. ***De gekwalificeerde status van websiteauthenticatiediensten en hun verleners van vertrouwensdiensten, met inbegrip van hun volledige naleving van de vereisten van deze verordening met betrekking tot de afgifte van gekwalificeerde certificaten voor websiteauthenticatie, moet worden bevestigd met nationale vertrouwenslijsten. Aanbieders van webbrowsers mogen bij de erkenning van gekwalificeerde certificaten voor websiteauthenticatie die certificaten niet als niet-authentiek aanmerken als het er louter om gaat de link tussen de domeinnaam van de website en de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven, te bekrachtigen of de identiteit van die persoon te bevestigen. Aanbieders van webbrowsers moeten de gecertificeerde identiteitsgegevens en de overige geattesteerde attributen op een gebruikersvriendelijke manier in de browseromgeving zichtbaar maken voor de eindgebruiker, met gebruikmaking van technische middelen naar eigen keuze.***

Daartoe moeten ***aanbieders van*** webbrowsers zorgen voor ondersteuning van en interoperabiliteit met ***gekwalificeerde certificaten voor websiteauthenticatie die in volledige overeenstemming met deze verordening zijn afgegeven***. ***De verplichting tot erkenning, interoperabiliteit en ondersteuning van gekwalificeerde certificaten voor websiteauthenticatie doet geen afbreuk aan de vrijheid van aanbieders van webbrowsers om te zorgen voor webbeveiliging, domeinauthenticatie en encryptie van webverkeer op een wijze en met gebruikmaking van de technologie die zij het meest geschikt achten***. ***Aanbieders van webbrowsers moeten als bijdrage aan de onlineveiligheid van eindgebruikers, in uitzonderlijke omstandigheden bij concrete aanwijzingen voor inbreuken op de beveiliging of het verlies van integriteit van een geïdentificeerd certificaat of geïdentificeerde reeks certificaten, zowel noodzakelijke als evenredige voorzorgsmaatregelen kunnen treffen. Bij dergelijke voorzorgsmaatregelen moeten aanbieders van webbrowsers de Commissie, het nationale toezichthoudend orgaan, de entiteit waaraan het certificaat is afgegeven en de gekwalificeerde verlener van vertrouwensdiensten die dat certificaat of die reeks certificaten heeft afgegeven, onverwijld in kennis stellen van aanwijzingen voor een dergelijke inbreuk op de beveiliging of verlies van integriteit, en ook van de met betrekking tot één enkel certificaat of reeks certificaten getroffen maatregelen. Die maatregelen mogen geen afbreuk doen aan de verplichting van de aanbieders van webbrowsers om gekwalificeerde certificaten voor websiteauthenticatie in overeenstemming met de nationale vertrouwenslijsten te erkennen.*** Om ***burgers en ingezetenen van de Unie*** 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. ***De maatregelen in deze verordening ten behoeve van grotere samenhang tussen de uiteenlopende benaderingen en praktijken van de lidstaten op het vlak van toezichtprocedures, moeten helpen een groter vertrouwen in de beveiliging, kwaliteit en beschikbaarheid van*** gekwalificeerde certificaten voor websiteauthenticatie ***op te bouwen.***

(66) Veel lidstaten hebben nationale vereisten ingevoerd voor diensten die beveiligde en betrouwbare ***elektronische*** archivering aanbieden om elektronische gegevens ***en elektronische documenten***, alsmede bijbehorende vertrouwensdiensten voor de lange termijn te kunnen bewaren. Om de rechtszekerheid, ***het vertrouwen en de harmonisatie tussen de lidstaten te waarborgen, moet er een rechtskader voor gekwalificeerde elektronische archiveringsdiensten worden geschapen naar het voorbeeld van het in deze verordening opgenomen kader voor de andere vertrouwensdiensten***. ***Dat rechtskader voor gekwalificeerde elektronische archiveringsdiensten moet verleners van vertrouwensdiensten en gebruikers een efficiënte toolbox bieden met functionele vereisten voor elektronische archiveringsdiensten en met duidelijke rechtsgevolgen wanneer een gekwalificeerde elektronische archiveringsdienst wordt gebruikt. Die bepalingen moeten van toepassing zijn op elektronische gegevens en elektronische documenten die in elektronische vorm worden gecreëerd, als papieren documenten die gescand en gedigitaliseerd worden. Indien vereist, moeten die bepalingen het mogelijk maken dat de bewaarde elektronische gegevens en elektronische documenten naar andere dragers of in andere formaten worden overgezet om hun duurzaamheid en leesbaarheid tot na de technische geldigheidsperiode te verlengen, waarbij verlies van of wijzigingen aan gegevens of documenten zoveel mogelijk moet worden voorkomen.***

Indien de aan de elektronische archiveringsdienst overgedragen elektronische gegevens en elektronische documenten 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 vertrouwensdiensten. ***In gevallen waarin elektronische handtekeningen, elektronische zegels of elektronische tijdstempels worden gebruikt voor het aanmaken van bewijsmateriaal, moet een beroep worden gedaan op gekwalificeerde vertrouwensdiensten. Voor zover elektronische archiveringsdiensten niet bij deze verordening zijn geharmoniseerd, moeten de lidstaten overeenkomstig het Unierecht nationale bepalingen in verband met die diensten kunnen invoeren of handhaven, zoals specifieke bepalingen voor in een organisatie geïntegreerde diensten die uitsluitend voor de interne archivering van de betreffende organisatie worden gebruikt. Deze verordening mag geen onderscheid maken tussen elektronische gegevens en elektronische documenten die in elektronische vorm worden gecreëerd en fysieke documenten die zijn gedigitaliseerd***.

***(67) De activiteiten van nationale archieven en geheugeninstellingen worden, als organisaties die zich in het openbaar belang wijden aan het behoud van documentair erfgoed, normaliter gereguleerd bij nationale wet en deze instellingen bieden niet noodzakelijk vertrouwensdiensten in de zin van deze verordening aan. Voor zover dergelijke instellingen dit soort diensten niet aanbieden, laat deze verordening hun werkzaamheden onverlet.***

(68) ▌Elektronisch registers ***zijn een opeenvolging van elektronische gegevensbestanden, ter waarborging van de integriteit en de nauwkeurigheid van de chronologische volgorde daarvan***. ***Elektronische registers moeten gegevensbestanden in chronologische volgorde opslaan. In combinatie met andere technologieën dienen zij mede oplossingen te bieden voor efficiëntere en transformatieve overheidsdiensten zoals elektronisch stemmen, grensoverschrijdende douanesamenwerking, grensoverschrijdende samenwerking tussen academische instellingen, alsmede eigendomsregistratie van vastgoed bij gedecentraliseerde grondkadasters. Gekwalificeerde elektronische registers dienen een rechtsvermoeden te scheppen voor de unieke en accurate chronologische volgorde en integriteit van de gegevensbestanden in het register. Gezien hun specifieke kenmerken, zoals de chronologische volgorde van gegevensbestanden, moeten elektronisch registers onderscheiden worden van andere vertrouwensdiensten zoals elektronische tijdstempels en diensten voor elektronisch aangetekende bezorging***. ***Ter waarborging van de rechtszekerheid en ter bevordering van de innovatie moet*** een Uniebreed rechtskader ***worden ingesteld*** dat voorziet in de grensoverschrijdende erkenning van vertrouwensdiensten voor de registratie van gegevens in elektronische registers. ***Dit moet in afdoende mate voorkomen dat digitale activa worden gekopieerd en vaker dan een keer aan verschillende partijen worden verkocht. Het aanmaken en actualiseren van een elektronisch register hangt af van het type register: centraal of decentraal. Deze verordening moet zorgen voor technologische neutraliteit door technologie voor de uitvoering van de nieuwe vertrouwensdienst voor elektronische registers noch te bevoordelen, noch te discrimineren. Daarnaast moet de Commissie bij de opstelling van de uitvoeringshandelingen tot nadere bepaling van de vereisten voor gekwalificeerde elektronische registers rekening houden met duurzaamheidsindicatoren met betrekking tot eventuele negatieve effecten op het klimaat of andere milieugerelateerde negatieve effecten.***

(69) ▌Verleners van vertrouwensdiensten ***voor elektronisch registers moeten tot taak krijgen zich van de chronologische volgorde van de gegevensbestanden in het register te vergewissen***. ***Deze verordening laat eventuele wettelijke verplichtingen van gebruikers van*** elektronische registers ***uit hoofde van*** het Unierecht ***en*** het nationaal recht onverlet. ***Zo*** moeten praktijkvoorbeelden waarbij persoonsgegevens worden verwerkt, voldoen aan Verordening (EU) 2016/679 ***en*** moeten praktijkvoorbeelden die betrekking hebben op financiële ***diensten, voldoen*** aan het relevante Unierecht ***betreffende*** financiële ▌diensten.

(70) Om versnippering en obstakels op de interne markt ten gevolge van uiteenlopende normen en technische beperkingen te voorkomen, en om door middel van een gecoördineerd proces de toekomstige uitvoering van het Europees kader voor een digitale identiteit niet ***te belemmeren***, moeten de Commissie, de lidstaten***, het maatschappelijk middenveld, de academische wereld*** en de private sector nauw en gestructureerd samenwerken. Daartoe moeten de lidstaten ***en de Commissie*** binnen het kader van ***Aanbeveling (EU) 2021/946***[16] van de Commissie samenwerken om een gemeenschappelijke toolbox voor het Europees kader voor digitale identiteit te ontwerpen. ***In die context dienen de lidstaten*** overeenstemming te bereiken over een alomvattende technische architectuur en een referentiekader, gemeenschappelijke normen en technische referenties en richtsnoeren, ***met inbegrip van bestaande normen***, alsook beschrijvingen van beste praktijken die ten minste alle functionaliteiten en de interoperabiliteit van ***Europese portemonnees voor digitale identiteit***, inclusief elektronische handtekeningen, en van de gekwalificeerde ***verleners van*** vertrouwensdiensten voor de ***elektronische*** attestering van attributen, als uiteengezet in deze verordening, omvatten. In dit verband moeten de lidstaten tevens de gemeenschappelijke elementen afspreken voor een bedrijfsmodel en een vergoedingsstructuur voor de ***Europese portemonnees 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 Europees kader voor digitale identiteit.

▌

---

**16** Aanbeveling (EU) 2021/946 van de Commissie van 3 juni 2021 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor een digitale identiteit (PB L 210 van 14.6.2021, blz. 51).

*(71)* ***Deze verordening voorziet in een geharmoniseerd niveau qua kwaliteit, betrouwbaarheid en beveiliging van gekwalificeerde vertrouwensdiensten waarborgen, ongeacht waar de werkzaamheden worden verricht. Het moet een verlener van gekwalificeerde vertrouwensdiensten toegestaan zijn eigen werkzaamheden in verband met het aanbieden van een gekwalificeerde vertrouwensdienst in een derde land uit te besteden, indien dat derde land voorziet in passende waarborgen, die ervoor zorgen dat toezichtsactiviteiten en audits kunnen worden gehandhaafd alsof zij in de Unie plaatsvinden. Indien de naleving van deze 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.***

*(72)* ***Ter waarborging van de rechtszekerheid met betrekking tot de geldigheid van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten, is het essentieel dat de beoordeling door de vertrouwende partij die op basis van gekwalificeerde certificaten de validering van die geavanceerde elektronische handtekening uitvoert, nader wordt omschreven.***

*(73)* ***Verleners van vertrouwensdiensten moeten cryptografische methoden gebruiken die sporen met de beste praktijken en een betrouwbare toepassing van die algoritmes weerspiegelen, teneinde de veiligheid en de betrouwbaarheid van hun vertrouwensdiensten te garanderen.***

*(74)* ***Deze verordening verplicht verleners van gekwalificeerde vertrouwensdiensten om op basis van diverse in de EU geharmoniseerde methoden de identiteit te verifiëren van een natuurlijke of rechtspersoon aan wie het gekwalificeerde certificaat of de gekwalificeerde elektronische attestering van attributen wordt afgegeven. Opdat gekwalificeerde certificaten en gekwalificeerde elektronische attesteringen van attributen worden afgegeven aan degene aan wie ze toebehoren en zij de juiste en unieke reeks gegevens attesteren die naar de identiteit van die persoon verwijzen, moeten verleners van gekwalificeerde vertrouwensdiensten die gekwalificeerde certificaten of gekwalificeerde elektronische attesteringen van attributen afgeven, op het moment van afgifte van die certificaten en attesteringen, de identificatie van die persoon met volledige zekerheid waarborgen. Indien van toepassing voor de afgifte van gekwalificeerde certificaten en van gekwalificeerde elektronische attesteringen van attributen, moeten gekwalificeerde verleners van vertrouwensdiensten naast de verplichte verificatie van de identiteit van de persoon bovendien de juistheid en nauwkeurigheid van de geattesteerde attributen van de persoon aan wie het gekwalificeerde certificaat of de gekwalificeerde elektronische attestering van attributen is afgegeven, met volledige zekerheid waarborgen.***

***Ter vervulling van die resultaatsverplichting en van de verplichting tot volledige zekerheid bij de verificatie van de geattesteerde gegevens, moeten passende middelen beschikbaar zijn, zoals het gebruik van één of, indien nodig, een combinatie van specifieke, bij deze verordening vastgestelde methoden. Het moet mogelijk zijn die methoden te combineren teneinde de verificatie van de identiteit van de persoon aan wie het gekwalificeerde certificaat of de gekwalificeerde elektronische attestering van attributen is afgegeven, van een passende basis te voorzien. Binnen een dergelijke combinatie moeten ook elektronische identificatiemiddelen kunnen worden gebruikt die aan de vereisten van betrouwbaarheidsniveau "substantieel" voldoen, gecombineerd met andere middelen voor identiteitsverificatie waarmee voldaan kan worden aan de geharmoniseerde eisen van deze verordening met betrekking tot het betrouwbaarheidsniveau "hoog" als onderdeel van aanvullende geharmoniseerde procedures op afstand die met een hoge mate van betrouwbaarheid de identificatie waarborgen. Die methoden moeten de gekwalificeerde verlener van vertrouwensdiensten die een gekwalificeerde elektronische attestering van attributen afgeeft, de mogelijkheid bieden om op verzoek van de gebruiker, in overeenstemming met het Unie- of nationaal recht, met inbegrip van authentieke bronnen, de attributen te verifiëren die langs elektronische weg moeten worden bevestigd.***

***(75) Om deze verordening in overeenstemming te houden met de wereldwijde ontwikkelingen en aan te sluiten bij de beste 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 die actualiseringen moet rekening worden gehouden met nieuwe technologieën, praktijken, normen of technische specificaties.***

(76) Daar de doelstellingen van deze verordening, te weten de ontwikkeling van het Uniebrede Europees kader voor digitale identiteit en van een kader voor vertrouwensdiensten, niet voldoende door de lidstaten kunnen worden verwezenlijkt, maar vanwege de omvang en de gevolgen ervan beter door de Unie kunnen worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om die doelstellingen te verwezenlijken.

(77) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725.

(78) Verordening (EU) nr. 910/2014 moet daarom dienovereenkomstig worden gewijzigd,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Wijzigingen van Verordening (EU) nr. 910/2014

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

1) artikel 1 wordt vervangen door:

"Artikel 1
Onderwerp

Doel van deze ***verordening*** is te zorgen voor een goede werking van de interne markt en voor een passend niveau van beveiliging van de ***in de hele Unie gebruikte*** elektronische identificatiemiddelen en vertrouwensdiensten***, opdat natuurlijke en rechtspersonen in de hele Unie het recht op veilige deelname aan de digitale samenleving en de toegang tot publieke en private onlinediensten gemakkelijker kunnen uitoefenen.*** Daartoe wordt bij deze verordening het volgende vastgesteld:

a) de voorwaarden waaronder de lidstaten elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen die onder een aangemeld stelsel voor elektronische identificatie van een andere lidstaat vallen, moeten erkennen, en ***Europese portemonnees voor digitale identiteit moeten 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 en certificatendiensten voor websiteauthenticatie, elektronische archivering en elektronische attestering van attributen, ▌ middelen voor het aanmaken van elektronische handtekeningen en middelen voor het aanmaken van elektronische zegels, 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 worden 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 Unie- of nationaal recht dat betrekking heeft op de totstandkoming en geldigheid van contracten, andere wettelijke of procedurele ***vorm***verplichtingen dan wel ***sectorspecifieke vormvereisten***.

***4. Deze verordening doet geen afbreuk aan Verordening (EU) 2016/679 van het Europees Parlement en de Raad*.***

---

* ***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).***";

3) artikel 3 wordt als volgt gewijzigd:

***a) de punten 1 tot en met 5 worden vervangen door:***

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

2. "elektronisch identificatiemiddel": een materiële en/of immateriële eenheid ▌ die persoonsidentificatiegegevens bevat en voor authenticatie bij een onlinedienst ***of, in voorkomend geval, een offlinedienst wordt gebruikt***;

***3. "persoonsidentificatiegegevens": een reeks gegevens die overeenkomstig het Unie- of nationaal recht is uitgegeven en aan de hand waarvan de identiteit van een natuurlijke of rechtspersoon, of van een natuurlijke persoon die een andere natuurlijke persoon of een rechtspersoon vertegenwoordigt, kan worden vastgesteld;***

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

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

▌

***b) het volgende punt wordt ingevoegd:***

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

c) punt 6 wordt vervangen door:

***"6. "vertrouwende partij": een natuurlijke of rechtspersoon die vertrouwt op elektronische identificatie, Europese portemonnees voor digitale identiteit of andere elektronische identificatiemiddelen, of op een vertrouwensdienst;***";

d) punt 16 wordt vervangen door:

"***16.*** "vertrouwensdienst": een elektronische dienst die gewoonlijk ***tegen betaling*** wordt verricht en uit een van de volgende elementen bestaat:

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

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

c) het aanmaken ***van elektronische handtekeningen of elektronische zegels***;

d) het ***valideren*** van elektronische handtekeningen ***of elektronische zegels***;

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

f) het beheer van ***middelen voor het op afstand aanmaken van*** elektronische handtekeningen ***of*** middelen voor het op afstand aanmaken van ***elektronische*** zegels;

g) het ***uitgeven*** van elektronische ***attesteringen van attributen***;

***h) het valideren van elektronische attesteringen van attributen;***

***i) het aanmaken van elektronische tijdstempels;***

***j) het valideren van elektronische tijdstempels;***

*k) het verlenen van diensten voor elektronisch aangetekende bezorging;*

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

*m) het elektronisch archiveren van elektronische gegevens en elektronische documenten;*

*n) het opslaan van elektronische gegevens in elektronische registers;*";

*e) punt 18 wordt vervangen door:*

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

f) punt 21 wordt vervangen door:

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

g) de volgende punten worden ingevoegd:

"23 bis. "gekwalificeerd middel voor het op afstand aanmaken van ***elektronische*** handtekeningen": 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 op afstand aanmaken van ***elektronische*** zegels": 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; ▌ ";

***h) punt 38 wordt vervangen door:***

***"38. "certificaat voor websiteauthenticatie": elektronische attestering die het mogelijk maakt de authenticiteit van een website vast te stellen en die de website verbindt aan de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven;***

i) punt 41 wordt vervangen door:

"41. "validering": proces waarmee wordt nagegaan of, en wordt bevestigd dat, ***gegevens in*** elektronische ***vorm overeenkomstig deze verordening geldig zijn***;";

j) de volgende punten ▌ worden toegevoegd:

"42. "Europese portemonnee voor digitale identiteit": ***een elektronisch identificatiemiddel*** dat de gebruiker in staat stelt gegevens voor persoonsidentificatie ***en elektronische attesteringen van attributen veilig*** op te slaan***, te beheren en te valideren*** met het oog op de verstrekking ervan aan vertrouwende partijen ▌ en ***andere gebruikers van Europese portemonnees voor digitale identiteit, en te ondertekenen middels gekwalificeerde elektronische handtekeningen of te verzegelen middels gekwalificeerde elektronische*** zegels;

43. "attribuut": ***een eigenschap, hoedanigheid, recht of toestemming*** van een natuurlijke of rechtspersoon of van een ***object***;

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 die voldoet aan de eisen van bijlage V;

***46. "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 septies en bijlage VII;***

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

48. "elektronische archivering": een dienst die de ontvangst, opslag, ***opvraging en verwijdering*** van elektronische gegevens ***en elektronische*** documenten 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;

49. “gekwalificeerde elektronische archiveringsdienst”: een ***elektronische archiveringsdienst*** die wordt verstrekt door een ***verlener van gekwalificeerde vertrouwensdiensten*** en die voldoet aan de eisen die zijn vastgelegd in artikel ***45 undecies***;

50. “EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit”: ***een verifieerbare*** eenvoudige, herkenbare en op een duidelijke wijze meegedeelde indicatie dat een ***Europese*** portemonnee voor digitale identiteit is ***verstrekt*** overeenkomstig deze verordening;

51. “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;

52. “elektronisch register”: een ***opeenvolging van*** elektronische ***gegevens-bestanden*** die ***de*** integriteit ***van die bestanden en de*** nauwkeurigheid van ***de*** chronologische volgorde ***van die bestanden*** waarborgt;

***53. “gekwalificeerd elektronisch register”: een elektronisch register dat wordt verstrekt door een verlener van gekwalificeerde vertrouwensdiensten en dat voldoet aan de eisen die zijn vastgelegd in artikel 45 duodecies;***

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

55. “***identiteitsmatching***”: een proces waarbij persoonsidentificatiegegevens of elektronische identificatiemiddelen met een bestaande account van dezelfde persoon worden gematcht of gekoppeld ▌;

▌

***56. “gegevensbestand”: elektronische gegevens die samen met daaraan gerelateerde metagegevens zijn opgeslagen ter ondersteuning van de verwerking van de gegevens;***

***57. "offlinemodus": wat het gebruik van Europese portemonnees voor digitale identiteit betreft, een interactie tussen een gebruiker en een derde op een fysieke locatie, waarbij de Europese portemonnee voor digitale identiteit door het gebruik van korteafstandtechnologieën geen toegang tot systemen op afstand via elektronische communicatienetwerken hoeft te hebben ten behoeve van de interactie.";***

4) artikel 5 wordt vervangen door:

"Artikel 5
Pseudoniemen in elektronische transacties

***Onverminderd specifieke regels van het Unie- of nationale recht op grond waarvan gebruikers zichzelf moeten identificeren of*** onverminderd het rechtsgevolg dat op grond van het nationaal recht aan het gebruik van pseudoniemen wordt toegekend, wordt het gebruik van pseudoniemen ***die door de gebruiker zijn gekozen,*** niet verboden. ▌";

5) in hoofdstuk II wordt de ***volgende afdeling ingevoegd***:

"AFDELING 1

***EUROPESE PORTEMONNEE VOOR DIGITALE IDENTITEIT***

Artikel 5

Europese portemonnees voor digitale identiteit

1. Opdat alle natuurlijke personen en rechtspersonen in de Unie veilige, betrouwbare en naadloze ***grensoverschrijdende*** toegang tot publieke en private diensten krijgen***, met volledige controle over hun gegevens, verstrekken*** alle lidstaten ***ten minste één Europese portemonnee voor digitale identiteit*** binnen 24 maanden na de datum van inwerkingtreding van ***de in lid 23 van dit artikel en in artikel 5 quater, lid 6, bedoelde uitvoeringshandelingen***.

2. Europese portemonnees voor digitale identiteit worden ***op een of meer van de volgende manieren verstrekt***:

   a) ***rechtstreeks*** door een lidstaat;

b) krachtens een mandaat van een lidstaat;

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

***3. De broncode van de applicatiesoftwarecomponenten van Europese portemonnees voor digitale identiteit wordt onder een opensourcelicentie geplaatst. De lidstaten kunnen bepalen dat de broncode van andere specifieke componenten dan die welke op apparaten van gebruikers zijn geïnstalleerd, om terdege gemotiveerde redenen niet openbaar wordt gemaakt.***

4. Met een Europese portemonnee voor digitale identiteit kunnen gebruikers ***op*** [...] ***gebruiksvriendelijke, transparante en voor hen traceerbare wijze***:

a) ***veilig, met volledige controle door de gebruiker,*** persoonsidentificatie-gegevens ***aanvragen, verkrijgen, selecteren, combineren, opslaan, verwijderen, delen en aanbieden, en, indien van toepassing, in combinatie met elektronische attesteringen van attributen, zich online en, indien passend, in*** offline***modus*** authenticeren ***bij vertrouwende partijen***, om toegang te krijgen tot ***publieke en private diensten, waarbij ervoor wordt gezorgd dat een selectieve verstrekking van gegevens mogelijk is;***

***b) pseudoniemen genereren en versleuteld en lokaal opslaan in de*** Europese portemonnee voor digitale identiteit***;***

***c) veilig de Europese portemonnee voor digitale identiteit van een andere persoon authenticeren en persoonsidentificatiegegevens en elektronische attesteringen van attributen op beveiligde wijze tussen de twee Europese portemonnees voor digitale identiteit ontvangen en delen;***

***d) toegang krijgen tot een log van alle transacties die met de Europese portemonnee voor digitale identiteit worden uitgevoerd via een gemeenschappelijk dashboard waarmee de gebruiker:***

***i) een actuele lijst van vertrouwende partijen waarmee de gebruiker een verbinding tot stand heeft gebracht en, indien van toepassing, alle uitgewisselde gegevens kan bekijken;***

***ii) gemakkelijk kan verzoeken om het wissen door een vertrouwende partij van persoonsgegevens overeenkomstig artikel 17 van Verordening (EU) 2016/679;***

***iii) gemakkelijk aan de bevoegde nationale gegevensbeschermingsautoriteit een vertrouwende partij kan aangeven, wanneer een vermeend onrechtmatig of verdacht verzoek om gegevens is ontvangen;***

e) ondertekenen middels gekwalificeerde elektronische handtekeningen ***of verzegelen middels gekwalificeerde elektronische zegels;***

***f)*** ***voor zover technisch haalbaar, de gegevens van de gebruiker, de elektronische attestering van attributen en configuraties downloaden;***

***g)*** ***de rechten van de gebruiker op gegevensoverdraagbaarheid uitoefenen.***

5. ***Europese*** portemonnees voor digitale identiteit moeten in het bijzonder:

a) gemeenschappelijke ***protocollen en interfaces ondersteunen:***

i) ***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;

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

iii) ***om online en, indien passend, ook in offlinemodus*** persoonsidentificatiegegevens***,*** elektronische attestering van attributen ***of van selectief verstrekte gegevens*** met [...] vertrouwende partijen ***te delen en hun*** aan te bieden;

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

***v) om de gebruiker een veilige instap te garanderen door gebruik van een elektronisch identificatiemiddel overeenkomstig artikel 5 bis, lid 24;***

***vi) om tussen de Europese portemonnees voor digitale identiteit van twee personen te communiceren teneinde op beveiligde wijze persoonsidentificatiesgegevens en elektronische attesteringen van attributen te ontvangen, te valideren en te delen;***

***vii) om vertrouwende partijen te authenticeren en identificeren door de toepassing van authenticatiemechanismen overeenkomstig artikel 5 ter;***

***viii) opdat vertrouwende partijen de authenticiteit en geldigheid van Europese portemonnees voor digitale identiteit kunnen verifiëren;***

***ix) om een vertrouwende partij te kunnen verzoeken om het wissen van persoonsgegevens overeenkomstig artikel 17 van Verordening (EU) 2016/679;***

***x) om het aan de bevoegde nationale gegevensbeschermingsautoriteit te melden wanneer van een vertrouwende partij een vermeend onrechtmatig of verdacht verzoek om gegevens is ontvangen;***

***xi) voor het aanmaken van gekwalificeerde elektronische handtekeningen of elektronische zegels door middel van middelen voor het aanmaken van gekwalificeerde elektronische handtekeningen of elektronische zegels;***

b) verleners van vertrouwensdiensten van ***elektronische*** attesteringen van attributen ***geen informatie verstrekken*** ▌ over het gebruik van die ***elektronische*** attesteringen;

***c) ervoor zorgen dat vertrouwende partijen kunnen worden geauthenticeerd en geïdentificeerd door toepassing van authenticatiemechanismen overeenkomstig artikel 5 ter;***

d) aan de voorwaarden van artikel 8 voldoen wat het betrouwbaarheidsniveau “hoog” betreft, met name betreffende de vereisten voor het bewijzen en verifiëren van identiteit, en het beheer en de authenticatie van elektronische identificatiemiddelen;

***e) bij elektronische attestering van attributen met een ingebed openbaarmakingsbeleid, het passende mechanisme toepassen om de gebruiker ervan in kennis te stellen dat de vertrouwende partij of de gebruiker van de Europese portemonnee voor digitale identiteit die om die elektronische attestering van attributen verzoekt tot die attestering toegang heeft;***

▌

f) waarborgen dat de persoonsidentificatiegegevens ***die beschikbaar zijn uit het stelsel voor elektronische identificatie in het kader waarvan de Europese portemonnee voor digitale identiteit wordt verstrekt,*** op unieke wijze ***de natuurlijke of rechtspersoon, dan wel de natuurlijke persoon die*** de natuurlijke of rechtspersoon ***vertegenwoordigt, vertegenwoordigen en*** verbonden zijn met ***die Europese portemonnee voor digitale identiteit;***

***g) alle natuurlijke personen de mogelijkheid bieden om standaard en kosteloos met een gekwalificeerde elektronische handtekening te ondertekenen.***

***Niettegenstaande punt g) van de eerste alinea kunnen de lidstaten voorzien in evenredige maatregelen om ervoor te zorgen dat het gratis gebruik van gekwalificeerde elektronische handtekeningen door natuurlijke personen beperkt blijft tot niet-professionele doeleinden.***

***6. De lidstaten stellen de gebruikers onverwijld in kennis van inbreuken op de beveiliging die hun Europese portemonnee voor digitale identiteit of de inhoud ervan volledig of gedeeltelijk zouden kunnen hebben aangetast, met name indien hun Europese portemonnee voor digitale identiteit overeenkomstig artikel 5 sexies is opgeschort of ingetrokken.***

***7. Onverminderd artikel 5 septies kunnen de lidstaten overeenkomstig het nationaal recht in extra functies van de Europese portemonnees voor digitale identiteit voorzien, waaronder interoperabiliteit met bestaande nationale elektronische identificatiemiddelen. Die extra functies voldoen aan dit artikel.***

8. De lidstaten voorzien in ***gratis*** valideringsmechanismen om:

a) ***ervoor te zorgen dat*** de authenticiteit en de geldigheid van ***Europese portemonnees voor digitale identiteit*** kunnen worden geverifieerd;

***b) gebruikers in staat te stellen de authenticiteit en de geldigheid van de identiteit van vertrouwende partijen die zijn geregistreerd overeenkomstig artikel 5 ter, te verifiëren.***

***9. De lidstaten zien erop toe dat de geldigheid van de Europese portemonnee voor digitale identiteit kan worden ingetrokken in de volgende omstandigheden:***

***a) op uitdrukkelijk verzoek van de gebruiker;***

***b) wanneer de beveiliging van de Europese portemonnee voor digitale identiteit is aangetast;***

***c) wanneer de gebruiker sterft of de rechtspersoon haar activiteiten beëindigt.***

***10.*** ***Aanbieders van Europese portemonnees voor digitale identiteit zorgen ervoor dat gebruikers gemakkelijk om technische ondersteuning kunnen verzoeken en technische problemen of andere incidenten die negatieve gevolgen hebben voor het gebruik van Europese portemonnees voor digitale identiteit kunnen melden.***

11. Europese portemonnees voor digitale identiteit worden ***verstrekt*** op grond van een ▌ stelsel voor elektronische identificatie op betrouwbaarheidsniveau "hoog". ▌

***12.*** ***De Europese portemonnees voor digitale identiteit waarborgen privacy by design.***

***13.*** De uitgifte, het gebruik en de intrekking van ***Europese portemonnees voor digitale identiteit zijn kosteloos voor alle natuurlijke personen.***

14. ***Gebruikers*** hebben volledige controle over het ***gebruik van en de gegevens in hun Europese portemonnee voor digitale identiteit***. De ***aanbieder*** van de Europese portemonnee voor digitale identiteit verzamelt geen informatie over het gebruik van de ***Europese*** portemonnee ***voor digitale identiteit*** die niet noodzakelijk is voor de verlening van de diensten ***in verband met Europese portemonnees voor digitale identiteit***, noch combineert hij of zij persoonsidentificatiegegevens of enige andere persoonsgegevens die zijn opgeslagen of betrekking hebben op het gebruik van de Europese portemonnee voor digitale identiteit met persoonsgegevens van andere door die ***aanbieder*** of derden aangeboden diensten als die niet noodzakelijk zijn voor de verlening van de diensten ***in verband met Europese portemonnees voor digitale identiteit***, tenzij de gebruiker uitdrukkelijk anders heeft gevraagd. Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnee voor digitale identiteit worden ▌ logisch gescheiden van andere ***door de aanbieder van de Europese portemonnee voor digitale identiteit*** opgeslagen gegevens. Indien de Europese portemonnee voor digitale identiteit wordt verstrekt door private partijen overeenkomstig lid 2, punten b) en c), is artikel 45 nonies, lid 3, van overeenkomstige toepassing.

15. ***Het gebruik van Europese portemonnees voor digitale identiteit is vrijwillig. De toegang tot publieke en private diensten, de arbeidsmarkt en vrij ondernemerschap van natuurlijke of rechtspersonen die de Europese portemonnees voor digitale identiteit niet gebruiken, wordt niet beperkt of belemmerd. Het blijft mogelijk om via andere bestaande identificatie- en authenticatiemiddelen toegang te krijgen tot publieke en private diensten.***

16. ***Het technische kader van de Europese portemonnee voor digitale identiteit:***

    a) ***mag het aanbieders van elektronische attesteringen van attributen of andere partijen na de afgifte van de attestering van attributen, niet mogelijk maken gegevens te verkrijgen waarmee kan worden gevolgd, gekoppeld of gecorreleerd of waarmee kennis van transacties of gebruikersgedrag anderszins kan worden verkregen, tenzij de gebruiker daar uitdrukkelijk toestemming voor heeft gegeven;***

    b) ***moet technieken voor privacybescherming mogelijk maken die onkoppelbaarheid waarborgen, waarbij de attestering van attributen geen identificatie van de gebruiker vereist.***

*17. Elke verwerking van persoonsgegevens door de lidstaten of namens hen door organen of partijen die verantwoordelijk zijn voor het verstrekken van Europese portemonnees voor digitale identiteit als elektronisch identificatiemiddel, wordt uitgevoerd overeenkomstig passende en doeltreffende gegevensbeschermingsmaatregelen. Aangetoond wordt dat dergelijke verwerkingsactiviteiten in overeenstemming zijn met Verordening (EU) 2016/679. De lidstaten kunnen nationale bepalingen vaststellen om de toepassing van dergelijke maatregelen nader te specificeren.*

*18. De lidstaten verstrekken de Commissie onverwijld informatie over:*

*a) de instantie die verantwoordelijk is voor het opstellen en bijhouden van de lijst van geregistreerde vertrouwende partijen die Europese portemonnees voor digitale identiteit gebruiken, overeenkomstig artikel 5 ter, lid 5, alsmede de plaats waar die lijst zich bevindt;*

*b) de instanties die verantwoordelijk zijn voor de verstrekking van Europese portemonnees voor digitale identiteit, overeenkomstig artikel 5 bis, lid 1;*

***c) de instanties die ervoor moeten zorgen dat de persoonsidentificatiegegevens worden verbonden met de Europese portemonnee voor digitale identiteit, overeenkomstig artikel 5 bis, lid 5, punt f);***

***d) het mechanisme voor de validering van de in artikel 5 bis, lid 5, punt f), bedoelde persoonsidentificatiegegevens en van de identiteit van de vertrouwende partijen;***

***e) het mechanisme voor het valideren van de authenticiteit en de geldigheid van Europese portemonnees voor digitale identiteit.***

***De Commissie stelt de krachtens de eerste alinea verstrekte informatie aan het publiek beschikbaar via een beveiligd kanaal, in een elektronisch ondertekende of bezegelde vorm die geschikt is voor geautomatiseerde verwerking.***

19. ***Onverminderd lid 22 van onderhavig artikel, is artikel 11*** van overeenkomstige toepassing op de Europese portemonnee voor digitale identiteit.

20. Artikel 24, lid 2, punt b), en punten d) tot en met h), zijn van overeenkomstige toepassing op ***de aanbieders van*** Europese portemonnees voor digitale identiteit.

21. Europese portemonnees voor digitale identiteit worden ***op voet van gelijkheid met andere gebruikers*** toegankelijk gemaakt voor ***gebruik door personen met een handicap, overeenkomstig Richtlijn (EU) 2019/882*** van het Europees Parlement en de Raad*.

***22. Voor het verstrekken van Europese portemonnees voor digitale identiteit zijn de vereisten van de artikelen 7, 9, 10, 12 en 12 bis niet op Europese portemonnees voor digitale identiteit van toepassing, noch op de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt.***

23. ***Uiterlijk op ... [***6 maanden na ***de datum*** van inwerkingtreding van deze ***wijzigings***verordening***]*** stelt de Commissie ***door middel van uitvoeringshandelingen een lijst met*** referentie***normen en, zo nodig,*** specificaties en ***procedures*** vast voor de in de leden 4***, 5, 8 en 18*** van dit artikel bedoelde vereisten betreffende de uitvoering van de Europese portemonnee voor digitale identiteit. ***Die*** uitvoerings***handelingen*** worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

***24. De Commissie stelt door middel van uitvoeringshandelingen een lijst van referentienormen en, zo nodig, technische specificaties en procedures vast met het oog op het faciliteren van de instap in de Europese portemonnee voor digitale identiteit voor gebruikers middels hetzij elektronische identificatiemiddelen van betrouwbaarheidsniveau "hoog" hetzij elektronische identificatiemiddelen van betrouwbaarheidsniveau "substantieel", in combinatie met extra instapprocedures op afstand die samen aan de eisen van het betrouwbaarheidsniveau "hoog" voldoen. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***

Artikel 5 ter

Vertrouwende partijen voor Europese portemonnees voor digitale identiteit

1. Indien ***een*** vertrouwende ***partij*** voornemens ***is*** om Europese portemonnees voor digitale identiteit te gebruiken ***voor het verlenen van publieke of private diensten door middel van digitale interactie, laat zij zich registreren*** in de lidstaat waar zij gevestigd is ▌.

2. ***Het registratieproces moet kosteneffectief zijn en evenredig met het risico. De vertrouwende partij verstrekt ten minste:***

   a) ***de informatie die nodig is om zich te authenticeren voor Europese portemonnees voor digitale identiteit, die ten minste het volgende omvat:***

      i) ***de lidstaat waar de vertrouwende partij gevestigd is, en***

      ii) ***de naam van de vertrouwende partij en, in voorkomend geval, haar registratienummer zoals vermeld in een officieel register, samen met de identificatiegegevens van dat officiële register;***

   b) ***de contactgegevens van de vertrouwende partij;***

   c) ***het beoogde gebruik van Europese portemonnees voor digitale identiteit, met inbegrip van een indicatie van de gegevens die de vertrouwende partij van gebruikers opvraagt.***

3. ***Vertrouwende partijen vragen gebruikers geen andere gegevens te verstrekken dan die welke in de overeenkomstig lid 2, punt c), verstrekte indicatie worden bedoeld.***

***4. De leden 1 en 2 laten het Unie- of nationaal recht dat van toepassing is op het verrichten van specifieke diensten, onverlet.***

***5. De lidstaten maken de in lid 2 bedoelde informatie online openbaar in elektronisch ondertekende of bezegelde vorm die geschikt is voor geautomatiseerde verwerking.***

***6. Vertrouwende partijen die overeenkomstig dit artikel zijn geregistreerd, stellen de lidstaten onverwijld in kennis van eventuele wijzigingen in de krachtens lid 2 bij de registratie verstrekte informatie.***

7. De lidstaten ***voorzien in*** een gemeenschappelijk mechanisme ***om de identificatie en de*** authenticatie van vertrouwende partijen ***mogelijk te maken, zoals bedoeld in artikel 5 bis, lid 5, punt c)***.

***8. Indien vertrouwende partijen voornemens zijn om Europese portemonnees voor digitale identiteit te gebruiken, identificeren zij zichzelf bij de gebruiker.***

9. Vertrouwende partijen zijn verantwoordelijk voor de uitvoering van de procedure voor de authenticatie ***en validering*** van uit Europese portemonnees voor digitale identiteit ***opgevraagde*** persoonsidentificatiegegevens en elektronische attesteringen van attributen. ***Vertrouwende partijen mogen het gebruik van pseudoniemen niet weigeren indien de identificatie van de gebruiker krachtens Unie- of nationaal recht niet vereist is.***

***10. Intermediairs die namens vertrouwende partijen optreden, worden geacht vertrouwende partijen te zijn en mogen geen gegevens over de inhoud van de transactie opslaan.***

11. ***Uiterlijk op ... [***6 maanden na de ***datum van*** inwerkingtreding van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen betreffende de uitvoering van de Europese portemonnees voor digitale identiteit in de zin van artikel ***5 bis, lid 23***, technische specificaties en procedures voor de in de leden ***2, 5 en 6 tot en met 9*** van dit artikel bedoelde vereisten vast. ***Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***

Artikel 5 quater

Certificering van Europese portemonnees voor digitale identiteit

1. ***De overeenstemming van de*** Europese portemonnees voor digitale identiteit ***en het stelsel voor elektronische identificatie*** op grond ***waarvan zij worden verstrekt, met de vereisten van artikel 5 bis, leden 4, 5 en 8, met het vereiste van logische scheiding van artikel 5 bis, lid 14, en, in voorkomend geval, met de normen en technische specificaties zoals bedoeld in*** artikel ***5*** bis***, lid 24, wordt gecertificeerd door de lidstaten aangewezen conformiteitsbeoordelingsinstanties***.

2. ***De certificering van de overeenstemming van de Europese portemonnees voor digitale identiteit met de in lid 1 van dit artikel bedoelde vereisten, of delen daarvan, die relevant zijn voor cyberbeveiliging, wordt uitgevoerd overeenkomstig Europese regelingen voor cyberbeveiligingscertificering die zijn vastgesteld op grond van Verordening (EU) 2019/881 van het Europees Parlement en de Raad** en waarnaar wordt verwezen in de in lid 6 van dit artikel bedoelde uitvoeringshandelingen.***

*3. Voor de in lid 1 van dit artikel bedoelde vereisten die niet relevant zijn voor cyberbeveiliging en, voor de in lid 1 van dit artikel bedoelde vereisten die relevant zijn voor cyberbeveiliging, voor zover de in lid 2 van dit artikel bedoelde regelingen voor cyberbeveiligingscertificering die cyberbeveiligingsvereisten niet of slechts gedeeltelijk dekken, stellen de lidstaten ook voor die vereisten nationale certificeringsregelingen vast overeenkomstig de vereisten die zijn vastgesteld in de in lid 6 van dit artikel bedoelde uitvoeringshandelingen. De lidstaten zenden hun ontwerpen van nationale certificeringsregelingen toe aan de overeenkomstig artikel 46 sexies, lid 1, opgerichte Europese samenwerkingsgroep voor digitale identiteit (de "samenwerkingsgroep"). De samenwerkingsgroep kan adviezen en aanbevelingen uitbrengen.*

*4. Certificering op grond van lid 1 is maximaal vijf jaar geldig, mits om de twee jaar een kwetsbaarheidsbeoordeling wordt uitgevoerd. Indien een kwetsbaarheid wordt vastgesteld die niet tijdig wordt verholpen, wordt de certificering geannuleerd.*

5. *De naleving van de in artikel 5 bis van deze verordening opgenomen vereisten in verband met de verwerking van persoonsgegevens kan worden gecertificeerd op grond van Verordening (EU) 2016/679.*

6. ***Uiterlijk op ... [***6 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met*** referentie***normen en, waar nodig, specificaties en procedures*** vast voor de in de leden ***1, 2 en 3*** van dit artikel bedoelde certificering van Europese portemonnees voor digitale identiteit. ***Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld***.

7. De lidstaten verstrekken aan de Commissie de namen en adressen van de in lid 1 bedoelde conformiteitsbeoordelingsinstanties. De Commissie stelt die informatie beschikbaar aan alle lidstaten.

8. De Commissie is bevoegd overeenkomstig artikel 47 gedelegeerde handelingen vast te stellen ***tot bepaling*** van specifieke criteria waaraan de in ***lid 1 van dit artikel*** bedoelde aangewezen ***conformiteitsbeoordelingsinstanties*** moeten voldoen.

Artikel 5 quinquies

Bekendmaking van een lijst van gecertificeerde Europese portemonnees voor digitale identiteit

1. De lidstaten verstrekken de Commissie ***en de krachtens artikel 46 sexies, lid 1, opgerichte samenwerkingsgroep*** onverwijld informatie over de overeenkomstig artikel 5 bis verstrekte en door de in artikel 5 quater***, lid 1,*** bedoelde ***conformiteitsbeoordelingsinstanties*** gecertificeerde Europese portemonnees voor digitale identiteit. Zij stellen de Commissie ***en de krachtens artikel 46 sexies, lid 1, opgerichte samenwerkingsgroep*** er onverwijld van in kennis als een certificering wordt geannuleerd ***en daarbij geven zij de redenen voor de annulering op***.

***2. Onverminderd artikel 5 bis, lid 18, omvat de in lid 1 van dit artikel bedoelde door de lidstaten verstrekte informatie ten minste:***

***a) het certificaat en het certificeringsbeoordelingsverslag van de gecertificeerde Europese portemonnee voor digitale identiteit;***

***b) een beschrijving van het stelsel voor elektronische identificatie op grond waarvan de Europese portemonnee voor digitale identiteit wordt verstrekt;***

***c) de toepasselijke toezichtregeling en informatie over de aansprakelijkheidsregeling met betrekking tot de partij die de Europese portemonnee voor digitale identiteit verstrekt;***

***d) de autoriteit of autoriteiten die verantwoordelijk is respectievelijk zijn voor het stelsel voor elektronische identificatie;***

***e) regelingen voor de opschorting of intrekking van het stelsel voor elektronische identificatie of de authenticatie, of van de delen waarvan de integriteit geschonden is.***

3. Op basis van de overeenkomstig lid 1 ontvangen informatie stelt de Commissie een lijst van gecertificeerde Europese portemonnees voor digitale identiteit op, maakt zij de lijst ***in het Publicatieblad van de Europese Unie*** bekend ***en houdt zij deze in een machineleesbare vorm bij***.

***4. Een lidstaat kan bij de Commissie een verzoek indienen om een Europese portemonnee voor digitale identiteit en het stelsel voor elektronische identificatie op grond waarvan hij is verstrekt, van de in lid 3 bedoelde lijst te verwijderen.***

***5. Indien de overeenkomstig lid 1 verstrekte informatie wordt gewijzigd, verstrekt de lidstaat de Commissie de geactualiseerde informatie.***

***6.*** De Commissie houdt de in lid 3 bedoelde lijst bij door de overeenkomstige wijzigingen in de lijst binnen een maand na ontvangst van een verzoek overeenkomstig lid 4 of van geactualiseerde informatie overeenkomstig lid 5 bekend te maken ***in het Publicatieblad van de Europese Unie***.

7. ***Uiterlijk op ...*** [6 maanden na ***de datum van in***werkingtreding van deze ***wijzigings***verordening] stelt de Commissie door middel van uitvoerings-handelingen betreffende de uitvoering van Europese portemonnees voor digitale identiteit in de zin van artikel 5 ***bis, lid 23,*** de formaten en de procedures voor de toepassing van de leden 1, 4 ***en 5*** van dit artikel vast. ***Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***

***Artikel*** *5 sexies*

***Inbreuk op de beveiliging van Europese portemonnees voor digitale identiteit***

***1.*** ***Indien Europese portemonnees voor digitale identiteit die overeenkomstig artikel*** 5 ***bis zijn verstrekt, de in artikel*** 5 ***bis, lid 8, bedoelde validerings-mechanismen of het stelsel voor elektronische identificatie op grond waarvan Europese portemonnees voor digitale identiteit worden verstrekt, 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 lidstaat die de Europese portemonnees voor digitale identiteit heeft verstrekt, onverwijld de verstrekking en het gebruik van Europese portemonnees voor digitale identiteit op.***

***Indien de ernst van de in de eerste alinea bedoelde beveiligingsinbreuk of -aantasting dit rechtvaardigt, trekt de lidstaat onverwijld Europese portemonnees voor digitale identiteit in.***

***De lidstaat stelt de getroffen gebruikers, de overeenkomstig artikel 46 quater, lid 1, aangewezen centrale contactpunten, de vertrouwende partijen en de Commissie daarvan in kennis.***

***2.*** ***Indien de in lid 1, eerste alinea,*** van dit artikel ***bedoelde beveiligingsinbreuk of -aantasting niet binnen drie maanden na de opschorting wordt verholpen, trekt de lidstaat die Europese portemonnees voor digitale identiteit heeft verstrekt, deze en de geldigheid ervan in. De lidstaat stelt de getroffen gebruikers, de overeenkomstig artikel 46 quater, lid 1, aangewezen centrale contactpunten, de vertrouwende partijen en de Commissie van de intrekking in kennis.***

3. ***Indien de in lid 1*** van dit artikel ***bedoelde beveiligingsinbreuk of -aantasting verholpen is, herstelt de verstrekkende lidstaat de verstrekking en het gebruik van Europese portemonnees voor digitale identiteit, en stelt hij onverwijld de getroffen gebruikers en vertrouwende partijen, de overeenkomstig artikel 46 quater, lid 1, aangewezen centrale contactpunten en de Commissie daarvan in kennis.***

***4. De Commissie maakt de overeenkomstige wijzigingen aan de in artikel 5 quinquies bedoelde lijst onverwijld bekend in het Publicatieblad van de Europese Unie.***

***5. Uiterlijk op ... [6 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoerings-handelingen een lijst van referentienormen en, waar nodig, specificaties en procedures voor de in de leden 1, 2 en 3*** van dit artikel ***bedoelde maatregelen vast. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***

***Artikel*** *5 septies*

***Grensoverschrijdend gebruik van Europese portemonnees voor digitale identiteit***

***1. Indien de lidstaten elektronische identificatie en authenticatie vereisen om toegang tot een door een openbare instantie aangeboden onlinedienst te verkrijgen, aanvaarden zij tevens overeenkomstig deze verordening verstrekte Europese portemonnees voor digitale identiteit.***

*2. Indien private vertrouwende partijen die diensten verlenen, met uitzondering van micro-ondernemingen en kleine ondernemingen zoals gedefinieerd in artikel 2 van de bijlage bij Aanbeveling 2003/361/EG van de Commissie***, krachtens Uniewetgeving of nationaal recht sterke gebruikersauthenticatie voor online-identificatie moeten gebruiken, of indien sterke gebruikersauthenticatie voor online-identificatie vereist is op grond van een contractuele verbintenis op het gebied van bijvoorbeeld vervoer, energie, bankwezen, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie, aanvaarden die private vertrouwende partijen uiterlijk 36 maanden na de datum van inwerkingtreding van de in artikel 5 bis, lid 23 en artikel 5 quater, lid 6, bedoelde uitvoeringshandelingen, en uitsluitend op vrijwillig verzoek van de gebruiker tevens overeenkomstig deze verordening verstrekte Europese portemonnees voor digitale identiteit.*

3. ***Indien aanbieders van zeer grote onlineplatforms, zoals gedefinieerd in artikel 33 van Verordening (EU) 2022/2065*** van het Europees Parlement en de Raad**** ***van gebruikersauthenticatie verlangen om toegang tot onlinediensten te verkrijgen, aanvaarden en faciliteren zij tevens het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig deze verordening zijn verstrekt voor gebruikersauthenticatie, uitsluitend op vrijwillig verzoek van de gebruiker en met inachtneming van de minimaal benodigde gegevens voor de specifieke onlinedienst waarvoor authenticatie vereist is.***

4. ***In samenwerking met de lidstaten faciliteert de Commissie de ontwikkeling van gedragscodes in nauwe samenwerking met alle relevante belanghebbenden, met inbegrip van het maatschappelijk middenveld, om bij te dragen aan de brede beschikbaarheid en bruikbaarheid van Europese portemonnees voor digitale identiteit binnen het toepassingsgebied van deze verordening, en om dienstverleners aan te moedigen de ontwikkeling van gedragscodes te voltooien.***

*5.* ***Binnen 24 maanden na de uitrol van Europese portemonnees voor digitale identiteit beoordeelt de Commissie de vraag naar, de beschikbaarheid van en de bruikbaarheid van Europese portemonnees voor digitale identiteit, rekening houdend met criteria als gebruikersacceptatie, grensoverschrijdende aanwezigheid van dienstverleners, technologische ontwikkelingen, evolutie van gebruikspatronen en consumentenvraag.***

---

* 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).

** 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).

*** Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

**** Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening) (PB L 277 van 27.10.2022, blz. 1).”;

6) vóór artikel 6 wordt het volgende opschrift ingevoegd:

"AFDELING 2
STELSELS VOOR ELEKTRONISCHE IDENTIFICATIE";

▌

***7) in artikel 7 wordt punt g) vervangen door:***

"***g) ten minste zes maanden vóór aanmelding op grond van artikel 9, lid 1, verstrekt de aanmeldende lidstaat voor de toepassing van artikel 12, lid 5, de andere lidstaten een beschrijving van dat stelsel, in overeenstemming met de procedurele voorschriften die zijn vastgesteld bij de op grond van artikel 12, lid 6, vastgestelde uitvoeringshandelingen;***";

***8) in artikel 8, lid 3, wordt de eerste alinea vervangen door:***

"***3. Uiterlijk op 18 september 2015, rekening houdend met de geldende internationale normen en met inachtneming van lid 2, stelt de Commissie bij uitvoeringshandeling minimale technische specificaties, normen en procedures vast aan de hand waarvan voor elektronische identificatiemiddelen de betrouwbaarheidsniveaus laag, substantieel en hoog worden bepaald.***";

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

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

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

***10)*** ***in artikel 10 wordt de titel vervangen door:***

"***Inbreuk op de beveiliging van stelsels voor elektronische identificatie***";

11) het volgende artikel ▌ wordt ingevoegd:

"Artikel 11 bis

***Grensoverschrijdende identiteitsmatching***

1. ***Wanneer lidstaten optreden als vertrouwende partijen voor grensoverschrijdende diensten, garanderen zij ondubbelzinnige identiteitsmatching voor natuurlijke personen die gebruikmaken van aangemelde elektronische identificatiemiddelen of Europese portemonnees voor digitale identiteit*.

▌

***2. De lidstaten voorzien in technische en organisatorische maatregelen om een hoog niveau van bescherming te waarborgen van persoonsgegevens die worden gebruikt voor identiteitsmatching en ter voorkoming van profilering van gebruikers.***

3. ***Uiterlijk op ... [***6 maanden na ***de datum van in***werkingtreding van deze ***wijzigings***verordening***] stelt*** de Commissie door middel van uitvoeringshandelingen een lijst van ***referentienormen en, waar nodig, specificaties en procedures voor de*** in lid 1 van dit artikel ▌ bedoelde ***vereisten vast***. ***Die uitvoeringshandelingen worden volgens de*** in artikel ***48, lid 2,*** bedoelde ***onderzoeksprocedure vastgesteld***.";

▌

12) artikel 12 wordt als volgt gewijzigd:

***a) de titel wordt vervangen door:***

"***Interoperabiliteit***";

b) lid 3 wordt als volgt gewijzigd:

i) ***punt c) wordt vervangen door:***

"***c) het bevordert, door het ontwerp, de uitvoering van privacy en beveiliging;***

ii) ***punt d) wordt*** geschrapt;

▌

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

"d) een verwijzing naar een minimaal pakket persoonsidentificatiegegevens dat noodzakelijk is om ***een natuurlijke of rechtspersoon, of*** een natuurlijke ***persoon die een andere natuurlijke persoon vertegenwoordigt,*** op unieke wijze te ***vertegenwoordigen en dat beschikbaar is vanaf stelsels voor elektronische identificatie***;";

***d) leden 5 en 6 worden vervangen door:***

▌

***"5. De lidstaten voeren collegiale toetsingen uit van de onder deze verordening vallende stelsels voor elektronische identificatie die overeenkomstig artikel 9, lid 1, punt a), moeten worden aangemeld.***

***6. De Commissie stelt uiterlijk op 18 maart 2025 door middel van uitvoeringshandelingen de nodige procedurele voorschriften voor de in lid 5 van dit artikel bedoelde collegiale toetsingen vast teneinde een hoog op het risiconiveau afgestemd niveau van vertrouwen en veiligheid te waarborgen. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";***

*e) lid 7 wordt geschrapt;*

*f) lid 8 wordt vervangen door:*

*"8. De Commissie stelt uiterlijk op 18 september 2025 volgens de criteria in lid 3 van dit artikel en met inaanmerkingneming van de resultaten van de samenwerking tussen de lidstaten, uitvoeringshandelingen vast aangaande het in lid 4 van dit artikel beschreven interoperabiliteitskader ten behoeve van de vaststelling van eenduidige voorwaarden ter uitvoering van de in lid 1 van dit artikel bedoelde verplichting. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";*

13) in hoofdstuk II worden de volgende artikelen ingevoegd:

"Artikel 12 bis

Certificering van stelsels voor elektronische identificatie

1. De overeenstemming van ▌ ***aan te melden*** stelsels voor elektronische identificatie ***met*** de in ***deze verordening vastgelegde cyberbeveiligings***vereisten***, met inbegrip van de overeenstemming met de voor cyberbeveiliging relevante vereisten van artikel 8, lid 2, met betrekking tot de betrouwbaarheidsniveaus van stelsels voor elektronische identificatie***, wordt gecertificeerd door door de lidstaten aangewezen ***conformiteitsbeoordelingsinstanties***.

2. Certificering op grond van ***lid 1 van dit artikel wordt uitgevoerd op grond van*** een ▌ relevante regeling voor cyberbeveiligingscertificering overeenkomstig Verordening (EU) 2019/881 ***of delen daarvan, voor zover het cyberbeveiligingscertificaat of delen daarvan betrekking hebben op die cyberbeveiligingsvereisten***.

*3. Certificering overeenkomstig lid 1 is maximaal vijf jaar geldig, mits er om de twee jaar een kwetsbaarheidsbeoordeling wordt verricht. Indien er een kwetsbaarheid wordt vastgesteld die niet binnen drie maanden na de vaststelling wordt verholpen, wordt de certificering geannuleerd.*

*4. Niettegenstaande lid 2 kunnen de lidstaten een aanmeldende lidstaat overeenkomstig dat lid om aanvullende informatie verzoeken over stelsels voor elektronische identificatie of delen daarvan die 2 zijn gecertificeerd.*

*5. De in artikel 12, lid 5, bedoelde collegiale toetsing van stelsels voor elektronische identificatie heeft geen betrekking op stelsels voor elektronische identificatie of delen daarvan die overeenkomstig lid 1 van dit artikel zijn gecertificeerd. De lidstaten mogen gebruikmaken van een certificaat of een conformiteitsverklaring, uitgegeven op grond van een relevante certificeringsregeling of delen van dergelijke regelingen, met de niet met cyberbeveiliging verband houdende vereisten van artikel 8, lid 2, ten aanzien van de betrouwbaarheidsniveaus van stelsels voor elektronische identificatie.*

6. De lidstaten verstrekken aan de Commissie ▌ de namen en adressen van de in lid 1 bedoelde ***conformiteitsbeoordelingsinstanties***. De Commissie stelt die informatie beschikbaar aan ***alle*** lidstaten.

***Artikel 12 ter***

***Toegang tot hardware- en softwarekenmerken***

***Indien aanbieders van Europese portemonnees voor digitale identiteit en uitgevende instellingen van aangemelde elektronische identificatiemiddelen die handelen in een commerciële of professionele hoedanigheid en gebruikmaken van kernplatformdiensten zoals gedefinieerd in artikel 2, punt 2), van Verordening (EU) 2022/1925 van het Europees Parlement en de Raad*, of bij het aanbieden van diensten voor de Europese portemonnee voor digitale identiteit en elektronische identificatiemiddelen aan eindgebruikers, zakelijke gebruikers zijn zoals gedefinieerd in artikel 2, punt 21), van die verordening, zorgen poortwachters met name ervoor dat zij effectief interoperabel zijn met en ten behoeve van de interoperabiliteit toegang hebben tot dezelfde besturingssystemen, hardware of softwarekenmerken. Dergelijke effectieve interoperabiliteit en toegang worden kosteloos toegestaan en ongeacht of de hardware- of softwarekenmerken deel uitmaken van het besturingssysteem, zoals beschikbaar voor of gebruikt door die poortwachter bij het verlenen van dergelijke diensten, in de zin van artikel 6, lid 7, van Verordening (EU) 2022/1925. Dit artikel laat artikel 6 bis, lid 14, van deze verordening onverlet.";***

---

* ***Verordening (EU) 2022/1925 van het Europees Parlement en de Raad van 14 september 2022 over betwistbare en eerlijke markten in de digitale sector, en tot wijziging van Richtlijnen (EU) 2019/1937 en (EU) 2020/1828 (digitalemarktenverordening) (PB L 265 van 12.10.2022, blz. 1).***

▌

14) in artikel 13 wordt lid 1 vervangen door:

"1. ▌ Niettegenstaande lid 2 van dit artikel ***en onverminderd Verordening (EU) 2016/679*** 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. ***Natuurlijke of rechtspersonen die materiële of immateriële schade hebben geleden als gevolg van een inbreuk op deze verordening door een verlener van vertrouwensdiensten, hebben het recht schadevergoeding te vorderen overeenkomstig het Unierecht en het nationaal recht***. ▌

***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.***

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

15) de artikelen 14, 15 en 16 worden vervangen door:

"Artikel 14

Internationale aspecten

1. ***Vertrouwensdiensten verleend door in een derde land gevestigde verleners van vertrouwensdiensten of door een internationale organisatie worden rechtens erkend als gelijkwaardig aan gekwalificeerde vertrouwensdiensten verleend 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 door middel van uitvoeringshandelingen of op grond van een overeenkomst tussen*** de Unie en ***het derde land of de internationale organisatie overeenkomstig artikel 218 VWEU.***

***De in de eerste alinea bedoelde uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***

2. ***De in*** lid 1 ***bedoelde uitvoeringshandelingen en overeenkomst regelen dat de eisen die gelden voor gekwalificeerde verleners van*** vertrouwens***diensten die in de Unie zijn gevestigd en voor de gekwalificeerde*** vertrouwensdiensten die zij verlenen***, worden nageleefd door de verleners van vertrouwensdiensten*** in het betrokken derde land ***of door de internationale organisatie 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***. ▌

***3. De in lid 1 bedoelde overeenkomst regelt 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 door de internationale organisatie waarmee de overeenkomst is gesloten.***

Artikel 15

Toegankelijkheid voor personen met een handicap ***en bijzondere behoeften***

***Elektronische identificatiemiddelen***, vertrouwensdiensten en eindgebruikersproducten die bij de verlening van die diensten worden gebruikt, worden beschikbaar gesteld in duidelijke en begrijpelijke taal, in overeenstemming met het ***Verdrag van de Verenigde Naties inzake de rechten van personen met een handicap en de toegankelijkheidseisen van*** Richtlijn ***(EU) 2019/882, zodat zij ook personen met functionele beperkingen, zoals ouderen, en personen met beperkte toegang tot digitale technologieën ten goede komen***.

***Artikel 16***

***Sancties***

1. ***Onverminderd artikel 31 van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad* stellen de lidstaten de regels vast inzake de sancties die van toepassing zijn op inbreuken op deze verordening. Die sancties moeten doeltreffend, evenredig en afschrikkend zijn.***

***2. De lidstaten zorgen ervoor dat inbreuken op deze verordening door gekwalificeerde en niet-gekwalificeerde verleners van vertrouwensdiensten worden bestraft met administratieve boetes voor een maximumbedrag van ten minste:***

***a) 5 000 000 EUR, indien de verlener van vertrouwensdiensten een natuurlijke persoon is, of***

***b) 5 000 000 EUR of 1 % van de totale wereldwijde jaaromzet van de onderneming waartoe de verlener van vertrouwensdiensten behoorde in het boekjaar voorafgaand aan het jaar waarin de inbreuk plaatsvond, indien dat hoger is, indien de verlener van vertrouwensdiensten een rechtspersoon is.***

***3. Afhankelijk van het rechtsstelsel van de betrokken lidstaten kunnen de regels voor administratieve boetes zo worden toegepast dat de boete door het bevoegde toezichthoudende orgaan wordt geïnitieerd, en door de bevoegde nationale rechters wordt opgelegd. Bij de toepassing van dergelijke regels in die lidstaten wordt gewaarborgd dat de rechtsmiddelen doeltreffend zijn en hetzelfde effect hebben als rechtstreeks door toezichthoudende autoriteiten opgelegde administratieve boetes.";***

---

* Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

16) in hoofdstuk III, afdeling 2, wordt de titel vervangen door:

"Niet-gekwalificeerde vertrouwensdiensten";

***17) de artikelen 17 en 18 worden geschrapt;***

*18) in hoofdstuk III, afdeling 2, wordt het volgende artikel ingevoegd:*

*"Artikel 19 bis*

*Eisen aan niet-gekwalificeerde verleners van vertrouwensdiensten*

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

a) *voert een passend beleid en treft overeenkomstige maatregelen ter beheersing van juridische, zakelijke, operationele en andere directe of indirecte risico's met betrekking tot de verlening van de niet-gekwalificeerde vertrouwensdienst, die niettegenstaande artikel 21 van Richtlijn (EU) 2022/2555, ten minste de maatregelen omvatten met betrekking tot:*

*i) de registratie en instapprocedures voor een vertrouwensdienst;*

*ii) procedurele of administratieve controles die nodig zijn om vertrouwensdiensten te verlenen;*

*iii) het beheer en de uitvoering van vertrouwensdiensten;*

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

***2. Uiterlijk op ... [12 maanden na de datum van inwerkingtreding van deze wijzigingsverordening]▌ stelt de Commissie door middel van uitvoerings-handelingen een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor de toepassing van lid 1, punt a), van dit artikel. Indien die normen, specificaties en procedures worden nageleefd, wordt aangenomen dat er overeenstemming is met de in dit artikel bepaalde vereisten. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";***

19) artikel 20 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Gekwalificeerde verleners van vertrouwensdiensten worden ten minste eens in de 24 maanden op hun kosten aan een audit door een conformiteitsbeoordelingsinstantie 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 ***21*** van Richtlijn (EU) ***2022/2555*** vastgelegde eisen. Gekwalificeerde verleners van vertrouwensdiensten leggen het conformiteitsbeoordelingsverslag binnen drie werkdagen na ontvangst aan het toezichthoudend orgaan voor.";

***b) de volgende leden worden ingevoegd:***

***"1 bis. Gekwalificeerde verleners van vertrouwensdiensten stellen het toezichthoudend orgaan ten minste één maand vóór geplande audits daarvan in kennis en staan het toezichthoudend orgaan op verzoek toe hieraan als waarnemer deel te nemen.***

***1 ter. De lidstaten stellen de Commissie onverwijld in kennis van de namen, adressen en accreditatiegegevens van de in lid 1 bedoelde conformiteitsbeoordelingsinstanties en van alle latere wijzigingen daarvan. De Commissie stelt die informatie beschikbaar aan alle lidstaten.";***

c) de leden 2, 3 en 4 worden vervangen door:

"Onverminderd lid 1 kan het toezichthoudend orgaan op elk tijdstip een audit houden van, of een conformiteitsbeoordelingsorgaan verzoeken om een conformiteitsbeoordeling uit te voeren ten aanzien van de gekwalificeerde verleners van vertrouwensdiensten, en dat op kosten van die verleners van vertrouwensdiensten, om te bevestigen dat zij en de door hen verleende gekwalificeerde vertrouwensdiensten voldoen aan de in deze verordening vastgestelde vereisten. Indien er sprake blijkt te zijn van een inbreuk op de regels voor de bescherming van persoonsgegevens brengt het toezichthoudend orgaan de op grond van artikel 51 van Verordening (EU) 2016/679 opgerichte ***bevoegde*** toezichthoudende autoriteiten ***onverwijld*** op de hoogte ▌.

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 en, indien van toepassing binnen de door het toezichthoudend orgaan bepaalde tijdspanne, kan het toezichthoudend orgaan, ***wanneer dit gerechtvaardigd is door*** 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 de uit hoofde van artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteiten het toezichthoudend orgaan ervan in kennis stellen dat de gekwalificeerde verlener van vertrouwensdiensten enig van de vereisten van artikel 21 van die richtlijn niet naleeft, trekt het toezichthoudend orgaan, wanneer dit gerechtvaardigd is door 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 in.***

***3 ter. Indien de*** op grond van artikel 51 van Verordening (EU) 2016/679 opgerichte ***toezichthoudende autoriteiten het toezichthoudend orgaan ervan in kennis stellen dat de gekwalificeerde verlener van vertrouwensdiensten enig van de vereisten van die verordening niet naleeft, trekt het toezichthoudend orgaan, wanneer dit gerechtvaardigd is door 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 in.***

***3 quater.*** ***Het toezichthoudend orgaan stelt de gekwalificeerde verlener van vertrouwensdiensten in kennis van het feit dat zijn of haar status van gekwalificeerde of de status "gekwalificeerd" van de betrokken dienst is ingetrokken. Het toezichthoudend orgaan stelt het orgaan waarover uit hoofde van artikel 22, lid 3, van deze verordening informatie is verstrekt, hiervan in kennis zodat de in lid 1 van dat artikel bedoelde vertrouwenslijsten bijgewerkt kunnen worden, evenals de uit hoofde van artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde bevoegde autoriteit.***

4. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met*** referentie***normen en, waar nodig, specificaties en procedures*** 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, ***daaronder begrepen hun samengestelde beoordeling***, 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 uitbrengen.

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

20) artikel 21 wordt als volgt gewijzigd:

***a) de leden 1 en 2 worden vervangen door:***

***"1. Indien verleners van vertrouwensdiensten het voornemen hebben gekwalificeerde vertrouwensdiensten te gaan verlenen, stellen zij het toezichthoudend orgaan in kennis van hun voornemen, en dienen zij een door een conformiteitsbeoordelingsinstantie afgegeven conformiteitsbeoordelingsverslag in waarin wordt bevestigd dat is voldaan aan de vereisten van deze verordening en van artikel 21 van Richtlijn (EU) 2022/2555.***

2. Het toezichthoudend orgaan verifieert of de verlener van vertrouwensdiensten 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 vertrouwensdiensten en aan de gekwalificeerde vertrouwensdiensten die zij verlenen.

   Om te controleren of de verlener van vertrouwensdiensten de eisen van artikel ***21*** van Richtlijn ***(EU) 2022/2555*** naleeft, verzoekt het toezichthoudend orgaan de uit hoofde van artikel 8, lid 1, van die r***ichtlijn*** aangewezen of opgerichte bevoegde autoriteiten om toezichtmaatregelen ter zake uit te voeren en ***onverwijld en uiterlijk twee maanden na de ontvangst van dit verzoek*** informatie over de uitkomst te verstrekken. ***Indien de verificatie niet*** binnen ***twee maanden na de kennisgeving is afgerond, brengen die 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. ***Uiterlijk ... [***12 maanden na de ***datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie, voor de toepassing van de leden 1 en 2 van dit artikel, door middel van uitvoeringshandelingen de formaten en procedures vast voor de kennisgeving en de verificatie ▌. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***"***;

▌

21) 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 of zij 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 moet worden*** afgegeven. ▌

1 bis. De in lid 1 bedoelde ***identiteitsverificatie*** wordt door de gekwalificeerde verlener van vertrouwensdiensten ***met daartoe geschikte middelen*** verricht, hetzij rechtstreeks, hetzij door een beroep te doen op een derde, ***op basis van een van de volgende methoden of indien nodig een combinatie daarvan, en conform de in lid 1 quater bedoelde uitvoeringshandelingen***:

a) door middel van de ***Europese portemonnee voor digitale identiteit*** of een aangemeld elektronisch identificatiemiddel dat voldoet aan de vereisten van artikel 8 wat betreft het betrouwbaarheids***niveau*** "hoog";

b) door middel van ▌ 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 hoog niveau van vertrouwen, waarvan de overeenstemming wordt bevestigd door een conformiteitsbeoordelingsinstantie;

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

▌

1 ter. De in lid 1 bedoelde verificatie van de attributen wordt door de gekwalificeerde verlener van vertrouwensdiensten met daartoe geschikte middelen verricht, hetzij rechtstreeks, hetzij door een beroep te doen op een derde, op basis van een van de volgende methoden of indien nodig op basis van een combinatie daarvan, overeenkomstig de in lid 1 quater bedoelde uitvoeringshandelingen:

***a) door middel van de Europese portemonnee voor digitale identiteit of een aangemeld elektronisch identificatiemiddel dat voldoet aan de vereisten van artikel 8 wat betreft het betrouwbaarheidsniveau "hoog";***

***b) door middel van ▌ een certificaat van een gekwalificeerde elektronische handtekening of van een gekwalificeerd elektronisch zegel, afgegeven overeenkomstig lid 1 bis, punt a), c) of d);***

***c) door middel van een gekwalificeerde elektronische attestering van attributen;***

***d) door middel van andere methoden ter waarborging van de verificatie van de attributen met een hoog niveau van vertrouwen, waarvan de overeenstemming wordt bevestigd door een conformiteitsbeoordelingsinstantie;***

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

"1 quater. ***Uiterlijk ... [***12 maanden na ***de datum van*** inwerkingtreding van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met*** referentie***normen en, waar nodig, specificaties en procedures*** vast voor de identiteits- en attributenverificatie overeenkomstig de leden 1, 1 bis en 1 ter ***van dit artikel***. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld. ▌ ";

b) lid 2 wordt als volgt gewijzigd:

***i) punt a) wordt vervangen door:***

***"a) informeert het toezichthoudend 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 die activiteiten te staken;";***

ii) ***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, onder meer door gebruik te maken van passende cryptografische technieken;***

iii) de volgende punten worden ingevoegd:

"f bis) voert, niettegenstaande artikel 21 van Richtlijn (EU) 2022/2555, passend beleid en treft overeenkomstige maatregelen om juridische, zakelijke, operationele en andere directe of indirecte risico's met betrekking tot de verlening van de gekwalificeerde vertrouwensdienst te beheersen, waaronder ten minste maatregelen in verband met:

i) de registratie en instapprocedures voor een dienst;

ii) de procedurele of administratieve controles;

iii) 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 binnen 24 uur na het incident*** in kennis van beveiligingsinbreuken of verstoringen ***in de verlening van de dienst of de*** uitvoering van de maatregelen bedoeld in punt f bis, i), ii) of iii), die een aanzienlijk effect ***hebben*** op de verleende vertrouwensdienst of op de daarin bijgehouden persoonsgegevens.";

iv) de punten g), h) en i) 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 die 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; ▌

***i) heeft een geactualiseerd beëindigingsplan om de continuïteit van de dienst te verzekeren in overeenstemming met de door het toezichthoudend orgaan op grond van artikel 46 ter, lid 4, punt i), geverifieerde bepalingen;*****”;**

v) punt j) wordt geschrapt;

vi) de volgende alinea wordt toegevoegd:

“Het toezichthoudend orgaan kan om informatie, anders dan de overeenkomstig punt a) van de eerste alinea verstrekte informatie, of het resultaat van een conformiteitsbeoordeling verzoeken en kan voorwaarden verbinden aan de toestemming voor het doorvoeren van de voorgenomen wijzigingen in de gekwalificeerde vertrouwensdiensten. 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.”;

c) lid 5 wordt vervangen door:

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

4 ter. De Commissie is bevoegd ***overeenkomstig artikel 47*** gedelegeerde handelingen vast te stellen ***met daarin*** de in lid 2, punt f bis), ***van dit artikel*** bedoelde extra maatregelen.

"5. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** ▌ stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met*** referentie***normen en, waar nodig, specificaties en procedures*** vast voor de in lid ***2 van dit artikel*** bedoelde vereisten. Indien ***die normen, specificaties en procedures*** worden nageleefd, wordt aangenomen dat er overeenstemming is met de in ***dit lid*** bepaalde vereisten. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

*22) het volgende artikel wordt ingevoegd in hoofdstuk III, afdeling 3:*

*"Artikel 24 bis*

*Erkenning van gekwalificeerde vertrouwensdiensten*

*1. Een gekwalificeerde elektronische handtekening op basis van een in een lidstaat afgegeven gekwalificeerd certificaat, of een gekwalificeerde elektronische zegel op basis van een in een lidstaat afgegeven gekwalificeerd certificaat, wordt in alle andere lidstaten erkend als respectievelijk gekwalificeerde elektronische handtekening of gekwalificeerde elektronische zegel.*

*2. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en in een lidstaat gecertificeerde gekwalificeerde middelen voor het aanmaken van elektronische zegels, worden in alle andere lidstaten erkend als respectievelijk gekwalificeerde middelen voor het aanmaken van elektronische handtekening en gekwalificeerde middelen voor het aanmaken van elektronische zegels.*

3. ***Een in een lidstaat verstrekt gekwalificeerd certificaat voor elektronische handtekeningen, een gekwalificeerd certificaat voor elektronische zegels, een gekwalificeerde vertrouwensdienst voor het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische handtekeningen en een gekwalificeerde vertrouwensdienst voor het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische zegels, worden in alle andere lidstaten erkend als respectievelijk een gekwalificeerd certificaat voor elektronische handtekeningen, een gekwalificeerd certificaat voor elektronische zegels, een gekwalificeerde vertrouwensdienst voor het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische handtekeningen en een gekwalificeerde vertrouwensdienst voor het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische zegels.***

4. ***Een in een lidstaat verleende gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen en een gekwalificeerde valideringsdienst voor gekwalificeerde elektronische zegels, worden in alle andere lidstaten erkend als respectievelijk een gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen en een gekwalificeerde valideringsdienst voor gekwalificeerde elektronische zegels.***

5. ***Een in een lidstaat verleende gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen en een gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische zegels, wordt in alle andere lidstaten erkend als respectievelijk een gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen en een gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische zegels.***

6. ***Een in een lidstaat afgegeven gekwalificeerd elektronisch tijdstempel wordt in alle andere lidstaten erkend als een gekwalificeerde elektronische tijdstempel.***

7. ***Een in een lidstaat afgegeven gekwalificeerd certificaat voor websiteauthenticatie wordt in alle andere lidstaten erkend als een gekwalificeerd certificaat voor websiteauthenticatie.***

8. ***Een in een lidstaat verleende gekwalificeerde dienst voor elektronisch aangetekende bezorging wordt in alle andere lidstaten erkend als een gekwalificeerde dienst voor elektronisch aangetekende bezorging.***

*9. Een in een lidstaat afgegeven gekwalificeerde elektronische attestering van attributen wordt in alle andere lidstaten erkend als een gekwalificeerde elektronische attestering van attributen.*

*10. Een in een lidstaat verleende gekwalificeerde elektronische archiveringsdienst wordt in alle andere lidstaten erkend als een gekwalificeerde elektronische archiveringsdienst.*

*11. Een in een lidstaat verstrekt gekwalificeerd elektronisch register wordt in alle andere lidstaten erkend als een gekwalificeerd elektronisch register.*";

*23) in artikel 25 wordt lid 3 geschrapt;*

***24)*** ***artikel 26 wordt als volgt gewijzigd:***

a) de enige alinea wordt lid 1;

b) ***onderstaand lid wordt toegevoegd:***

***"2.*** Uiterlijk ... ***[24 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] beoordeelt de Commissie of uitvoeringshandelingen moeten worden vastgesteld met daarin een lijst met referentienormen en, waar nodig, specificaties en procedures voor geavanceerde elektronische handtekeningen. Op basis van die beoordeling kan de Commissie dergelijke uitvoeringshandelingen vaststellen. Indien een geavanceerde elektronische handtekening aan de toepasselijke normen, specificaties en procedures voldoet, wordt aangenomen dat er overeenstemming is met de eisen voor geavanceerde elektronische handtekeningen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";***

***25)*** in ***artikel 27 wordt lid 4 geschrapt***;

26) in artikel 28 wordt lid 6 vervangen door:

"6. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor gekwalificeerde certificaten voor elektronische handtekeningen. Indien een gekwalificeerd certificaat voor elektronische handtekeningen aan de toepasselijke normen, ***specificaties en procedures*** voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage I vastgelegde eisen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***"***;

27) in artikel 29 wordt het volgende lid ingevoegd:

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

28) het volgende artikel ▌ wordt ingevoegd:

"Artikel 29 bis

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

1. Het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische handtekeningen als gekwalificeerde vertrouwensdienst mag 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) niettegenstaande punt 1, d), van bijlage II, de gegevens voor het aanmaken van elektronische handtekeningen alleen voor back-updoeleinden ***dupliceert***, 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 op afstand aanmaken van gekwalificeerde elektronische handtekeningen voldoet.

2. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie voor de toepassing van lid 1 van dit artikel door middel van uitvoeringshandelingen een lijst met ***referentienormen en, waar nodig, specificaties en procedures*** vast. ***De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld***.";

29) in artikel 30 wordt het volgende lid ingevoegd:

"3 bis. De in lid 1 bedoelde certificering is ***niet langer dan*** vijf jaar geldig, op voorwaarde dat er elke twee jaar een kwetsbaarheidsbeoordelingen worden uitgevoerd. Indien kwetsbaarheden worden vastgesteld die niet worden verholpen, wordt de certificering ***geannuleerd***.***"***;

30) in artikel 31 wordt lid 3 vervangen door:

"3. ***Uiterlijk ... [***12 maanden na de ***datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie voor de toepassing van lid 1 van dit artikel door middel van uitvoeringshandelingen de nodige formaten en procedures vast. De 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 normen, ***specificaties en procedures*** voldoet, wordt aangenomen dat er overeenstemming is met de in de eerste alinea van dit lid vastgelegde eisen. ▌";

b) lid 3 wordt vervangen door:

"3. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor de validering van gekwalificeerde elektronische handtekeningen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

***32) het volgende artikel wordt ingevoegd:***

***"Artikel 32 bis***

***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 is afgegeven door een gekwalificeerd verlener van vertrouwensdiensten en op het tijdstip van ondertekening geldig was;***

***c) de gegevens voor de validering 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.***

***2. Het systeem dat is gebruikt voor de validering 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 veiligheidsproblemen te identificeren.***

*3. Uiterlijk ... [12 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoerings-handelingen een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor de validering van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten. Indien de validering van geavanceerde elektronische handtekeningen op basis van gekwalificeerde certificaten aan de toepasselijke normen, specificaties en procedures voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 van dit artikel vastgelegde eisen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";*

*33) in artikel 33 wordt lid 2 vervangen door:*

*"2. Uiterlijk ... [12 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoeringshandelingen een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor de in lid 1 van dit artikel bedoelde gekwalificeerde valideringsdienst. Indien de gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen aan de toepasselijke normen, specificaties en procedures voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 van dit artikel vastgelegde eisen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";*

34) artikel 34 wordt als volgt gewijzigd:

a) het volgende lid wordt ingevoegd:

"1 bis. Indien de voorzieningen voor de gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen aan de in lid 2 bedoelde normen, ***specificaties en procedures*** voldoen, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgelegde eisen.";

b) lid 2 wordt vervangen door:

"2. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor de gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld. ▌";

***35)*** ***in artikel 35 wordt lid 3 geschrapt;***

***36)*** ***artikel 36 wordt als volgt gewijzigd:***

a) de enige alinea wordt lid 1;

b) ***onderstaand lid wordt toegevoegd:***

***"2. Uiterlijk ... [24 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] beoordeelt de Commissie of uitvoeringshandelingen moeten worden vastgesteld met daarin een lijst met referentienormen en, waar nodig, specificaties en procedures voor geavanceerde elektronische zegels. Op basis van die beoordeling kan de Commissie dergelijke uitvoeringshandelingen vaststellen. Indien een geavanceerde elektronische zegel aan die normen, specificaties en procedures voldoet, wordt aangenomen dat er overeenstemming is met de eisen voor geavanceerde elektronische zegels. Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld***.";

***37)*** ***in artikel 37 wordt lid 4 geschrapt;***

38) in artikel 38 wordt lid 6 vervangen door:

"6. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor gekwalificeerde certificaten voor elektronische zegels. ***Indien een gekwalificeerd certificaat voor elektronische zegels aan die normen, specificaties en procedures voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage III vastgelegde eisen.*** Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***"***;

39) het volgende artikel ▌ wordt ingevoegd:

"Artikel 39 bis

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

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

***40) het volgende artikel wordt ingevoegd in hoofdstuk III, afdeling 5:***

***"Artikel 40 bis***

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

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

***41) in artikel 41 wordt lid 3 geschrapt;***

42) artikel 42 wordt als volgt gewijzigd:

a) het volgende lid wordt ingevoegd:

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

b) lid 2 wordt vervangen door:

"2. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor de koppeling van datum en tijdstip aan gegevens en voor ***de vaststelling van de nauwkeurigheid van*** tijdsbronnen. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld. ▌";

43) artikel 44 wordt als volgt gewijzigd:

a) het volgende lid wordt ingevoegd:

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

b) lid 2 wordt vervangen door:

"2. ***Uiterlijk ... [***12 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor processen voor het verzenden en ontvangen van gegevens. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld. ▌";

*c) de volgende leden worden ingevoegd:*

*"2 bis. Verleners van gekwalificeerde diensten voor elektronisch aangetekende bezorging kunnen een akkoord bereiken over interoperabiliteit van de gekwalificeerde diensten voor elektronisch aangetekende bezorging die zij verlenen. Een dergelijk interoperabiliteitskader voldoet aan de in lid 1 vastgelegde eisen, hetgeen wordt bevestigd door een conformiteitsbeoordelingsinstantie.*

*2 ter. De Commissie kan, door middel van uitvoeringshandelingen, een lijst met referentienormen en, waar nodig, specificaties en procedures vaststellen voor het in lid 2 bis van dit artikel bedoelde interoperabiliteitskader. De technische specificaties en de inhoud van de normen zijn kosteneffectief en evenredig. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";*

44) 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 die eisen*** wordt ***uitgevoerd overeenkomstig*** de in lid 2 ***van dit artikel*** bedoelde ***normen, specificaties*** en procedures.

1 bis. De ***overeenkomstig*** lid 1 van dit artikel ***afgegeven*** gekwalificeerde certificaten voor websiteauthenticatie worden erkend door aanbieders van webbrowsers. ▌ Aanbieders van webbrowsers moeten ervoor zorgen dat de ***in het certificaat geattesteerde*** identiteitsgegevens en ***aanvullende geattesteerde attributen*** op ***gebruiksvriendelijke*** wijze ***worden*** weergegeven. Aanbieders van webbrowsers moeten zorgen voor ondersteuning van en interoperabiliteit met de in lid 1 ***van dit artikel*** bedoelde gekwalificeerde certificaten voor websiteauthenticatie, met uitzondering van micro- of kleine ondernemingen zoals gedefinieerd in artikel 2 van de bijlage bij Aanbeveling 2003/361/EG ***tijdens*** de eerste vijf jaar waarin zij actief zijn als aanbieders van webbrowserdiensten.

***1 ter. Voor gekwalificeerde certificaten voor websiteauthenticatie gelden geen andere dwingende eisen dan de in lid 1 vastgelegde eisen.***

2. ***Uiterlijk ... [***12 maanden na ***de datum*** van inwerkingtreding van deze ***wijzigings***verordening***]*** stelt de Commissie door middel van uitvoeringshandelingen ***een lijst met*** referentie***normen en, waar nodig, specificaties en procedures vast*** voor de in lid 1 ***van dit artikel*** bedoelde gekwalificeerde certificaten voor websiteauthenticatie. ▌ De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.";

45) het volgende artikel wordt ingevoegd:

***"Artikel 45 bis***

***Voorzorgsmaatregelen op het gebied van cyberbeveiliging***

***1. Aanbieders van webbrowsers mogen geen maatregelen nemen die in strijd zijn met hun verplichtingen uit hoofde van artikel 45, met name de eis om gekwalificeerde certificaten voor websiteauthenticatie te erkennen en de verstrekte identiteitsgegevens op een gebruiksvriendelijke wijze weer te geven.***

***2. In afwijking van lid 1 en alleen in geval van concrete aanwijzingen voor inbreuken op de beveiliging of het verlies van integriteit van een geïdentificeerd certificaat of reeks van certificaten, kunnen aanbieders van webbrowsers voorzorgsmaatregelen treffen voor dat certificaat of die reeks certificaten.***

*3. Indien een aanbieder van een webbrowser krachtens lid 2 voorzorgsmaatregelen heeft genomen, stelt de aanbieder van de webbrowser de Commissie, het bevoegde toezichthoudende orgaan, de entiteit waaraan het certificaat was afgegeven en de gekwalificeerde verlener van vertrouwensdiensten die het certificaat of de reeks certificaten heeft afgegeven onverwijld schriftelijk in kennis van zijn aanwijzingen, waarbij hij beschrijft welke maatregelen zijn genomen om de situatie te verhelpen. Na ontvangst van een dergelijke kennisgeving stuurt de bevoegde toezichthoudende instantie een ontvangstbevestiging naar de aanbieder van de webbrowser in kwestie.*

*4. Het bevoegde toezichthoudende orgaan onderzoekt overeenkomstig artikel 46 ter, lid 4, punt k), de in de kennisgeving aan de orde gestelde kwesties. Indien dat onderzoek niet leidt tot de intrekking van de status van gekwalificeerd certificaat, brengt het toezichthoudende orgaan de aanbieder van de webbrowser hiervan op de hoogte en verzoekt zij die aanbieder de in lid 2 van dit artikel bedoelde voorzorgsmaatregelen te beëindigen.*";

46) in hoofdstuk III worden de volgende afdelingen ingevoegd:

"AFDELING 9

ELEKTRONISCHE ATTESTERING VAN ATTRIBUTEN

Artikel 45 ter

Rechtsgevolgen van elektronische attestering van attributen

1. Het rechtsgevolg van een elektronische attestering van attributen of de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures worden niet ontzegd louter op grond van het feit dat de attestering 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 attestering van attributen uitgegeven door of namens een openbare instantie die in één lidstaat 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 quater.
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 attributen van andere lidstaten ook aanvaard. ▌

Artikel 45 quinquies

Eisen voor gekwalificeerde ***elektronische*** attestering van attributen

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

***2. De evaluatie van de overeenstemming met de eisen van bijlage V wordt uitgevoerd overeenkomstig de in lid 5 van dit artikel bedoelde normen, specificaties en procedures.***

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

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

5. ***Uiterlijk ... [***6 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***]*** stelt de Commissie ***door middel van uitvoeringshandelingen een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor gekwalificeerde elektronische attesteringen van attributen. ***De uitvoeringshandelingen stemmen overeen met de in artikel 5 bis, lid 23, bedoelde*** uitvoeringshandelingen betreffende de uitvoering van de Europese ***portemonnee*** voor digitale identiteit. ***Zij worden vastgesteld volgens de*** in artikel 48, ***lid 2, bedoelde onderzoeksprocedure***.

Artikel 45 sexies

Verificatie van attributen aan de hand van authentieke bronnen

1. De lidstaten waarborgen ***binnen 24 maanden na de datum van inwerkingtreding van de in artikel 5 bis, lid 23, en artikel 5 quater, lid 6, bedoelde uitvoeringshandelingen*** dat er, ten minste voor de in bijlage VI vermelde attributen, voor zover die authentieke bronnen binnen de publieke sector gebruiken, maatregelen worden genomen zodat gekwalificeerde verleners van ***vertrouwensdiensten*** elektronische attesteringen van attributen afgeven ***die attributen*** langs elektronische weg kunnen verifiëren op verzoek van de gebruiker, overeenkomstig het Unie- of nationaal recht.

2. ***Uiterlijk ... [***6 maanden na ***de datum van inwerkingtreding*** van deze ***wijzigings***verordening***] stelt de Commissie***, rekening houdend met de toepasselijke internationale normen, ***door middel van uitvoeringshandelingen een lijst met referentie***normen ***en, waar nodig, specificaties en procedures*** vast voor de catalogus van attributen en regelingen voor de attestering van attributen en verificatieprocedures voor gekwalificeerde elektronische attesteringen van attributen voor de toepassing van lid 1 van dit artikel***. De uitvoeringshandelingen stemmen overeen met de in artikel 5 bis, lid 23, bedoelde*** uitvoeringshandelingen betreffende de uitvoering van de Europese ***portemonnee*** voor digitale identiteit. ***Zij worden vastgesteld volgens de*** in artikel ***48, lid 2***, bedoelde ***onderzoeksprocedure***. ▌

***Artikel 45 septies***.

***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) die van bijlage VII;***

*b) het gekwalificeerde certificaat ter ondersteuning van de gekwalificeerde elektronische handtekening of de gekwalificeerde elektronische zegel van de in artikel 3, punt 46, 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 en:*

*i) waaruit blijkt dat overeenkomstig Unie- of nationaal recht is vastgesteld dat de afgevende instantie de verantwoordelijke instantie 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 bevat die ondubbelzinnig naar de in punt i) bedoelde authentieke bron verwijzen; en*

*iii) waarin wordt verwezen naar het in punt i) bedoelde Unie- of nationaal recht.*

*2. De lidstaat waar de in artikel 3, punt 46, 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.*

*3. De lidstaten melden de in artikel 3, punt 46, bedoelde openbare instanties aan bij de Commissie. Die aanmelding omvat een conformiteitsbeoordelingsverslag van een conformiteitsbeoordelingsinstantie waarin wordt bevestigd dat aan de eisen van de leden 1, 2 en 6 van dit artikel wordt voldaan. De Commissie maakt via een beveiligd kanaal de lijst van de in artikel 3, punt 46, bedoelde openbare instanties in elektronisch ondertekende of verzegelde en voor automatische verwerking geschikte vorm publiek beschikbaar.*

*4. Indien een elektronische attestering uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron, na initiële afgifte wordt ingetrokken, verliest deze haar geldigheid vanaf het moment van intrekking en de status ervan wordt niet teruggedraaid.*

*5. 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, indien de attestering aan de in lid 6 bedoelde normen, specificaties en procedures voldoet.*

6. ***Uiterlijk ... [6 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoeringshandelingen een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor elektronische attesteringen van attributen uitgegeven door of namens een openbare instantie die verantwoordelijk is voor een authentieke bron. De uitvoeringshandelingen stemmen overeen met de in artikel 5 bis, lid 23, bedoelde uitvoeringshandelingen betreffende de uitvoering van de Europese portemonnee voor digitale identiteit. Zij worden vastgesteld volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure.***

7. ***Uiterlijk ... [6 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoeringshandelingen een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor de toepassing van lid 3 van dit artikel. De uitvoeringshandelingen stemmen overeen met de in artikel 5 bis, lid 23, bedoelde uitvoeringshandelingen betreffende de uitvoering van de Europese portemonnee voor digitale identiteit. Zij worden vastgesteld volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure.***

***8. De in artikel 3, punt 46, bedoelde openbare instanties die elektronische attesteringen van attributen uitgeven, bieden een interface met de overeenkomstig artikel 5 bis verstrekte Europese portemonnees voor digitale identiteit.***

Artikel 45 octies

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

***1. Aanbieders van elektronische attesteringen van attributen bieden gebruikers van Europese portemonnees voor digitale identiteit de mogelijkheid de elektronische attestering van attributen aan te vragen, te verkrijgen, op te slaan en te beheren, ongeacht de lidstaat waar de Europese portemonnee voor digitale identiteit is verstrekt.***

***2.*** Aanbieders van gekwalificeerde elektronische attesteringen van attributen bieden een interface met overeenkomstig artikel 5 bis ***verstrekte*** Europese portemonnees voor digitale identiteit. ▌

Artikel 45 nonies

Aanvullende voorschriften voor de verlening 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.

▌

3. Verleners van gekwalificeerde diensten voor elektronische attestering van attributen ***zorgen ervoor dat de verlening van dergelijke gekwalificeerde vertrouwens***diensten ***verloopt op een wijze die functioneel gescheiden is van andere door hen verleende diensten***.

AFDELING 10

ELEKTRONISCHE ARCHIVERINGSDIENSTEN

Artikel 45 decies

***Rechtsgevolg van elektronische archiveringsdiensten***

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

2. ***Voor via een gekwalificeerde elektronische archiveringsdienst bewaarde elektronische gegevens en elektronische documenten 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.***

*Artikel 45 undecies*

*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 de duurzaamheid en leesbaarheid van elektronische gegevens en elektronische documenten kunnen waarborgen tot na de technologische geldigheidsduur en ten minste gedurende de wettelijke of contractuele bewaringstermijn, en handhaven daarbij de integriteit en de juistheid van de oorsprong van de gegevens;*

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

*d) zij stellen gemachtigde vertrouwende partijen ertoe in staat, op geautomatiseerde wijze verslagen te ontvangen waarin wordt bevestigd dat voor elektronische gegevens en elektronische documenten 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.*

*Het in punt d) bedoelde verslag wordt op betrouwbare en efficiënte wijze verstrekt en draagt de gekwalificeerde elektronische handtekening of gekwalificeerde elektronische zegel van de verlener van de gekwalificeerde elektronische archiveringsdienst.*

*2. Uiterlijk ... [12 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoeringshandelingen een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor gekwalificeerde elektronische archiveringsdiensten. Indien een gekwalificeerde elektronische archiveringsdienst aan de toepasselijke normen, specificaties en procedures voldoet, wordt aangenomen dat er overeenstemming is met de eisen voor gekwalificeerde elektronische archiveringsdiensten. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.*

AFDELING 11

ELEKTRONISCHE REGISTERS

Artikel 45 duodecies

Rechtsgevolgen van elektronische registers

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

Artikel 45 terdecies

Eisen voor gekwalificeerde elektronische registers

1. Gekwalificeerde elektronische registers voldoen aan de volgende eisen:

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

   b) zij ***stellen de oorsprong*** van de gegevens***bestanden*** in het register ***vast***;

   c) zij waarborgen de ***unieke*** chronologische volgorde van de gegevens***bestanden*** 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 zo de integriteit ervan in de tijd***.

2. Indien een elektronisch register aan de in lid 3 bedoelde normen, ***specificaties en procedures*** voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgelegde eisen.

3. ***Uiterlijk … [12 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt*** de Commissie door middel van uitvoeringshandelingen ***een lijst met referentienormen en, waar nodig, specificaties en procedures vast voor de in lid 1 van dit artikel vastgelegde eisen***. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.***"***;

▌

***47) het volgende hoofdstuk wordt ingevoegd:***

***"HOOFDSTUK IV BIS***
***GOVERNANCEKADER***

*Artikel 46 bis*

***Toezicht op het Rechtskader voor Europese portemonnees voor digitale identiteit***

1. ***De lidstaten wijzen een of meer op hun grondgebied gevestigde toezichthoudende organen aan.***

   ***De uit hoofde van de eerste alinea aangewezen toezichthoudende organen krijgen de noodzakelijke bevoegdheden en toereikende middelen om hun taken doeltreffend, efficiënt en onafhankelijk te kunnen uitvoeren.***

2. ***De lidstaten stellen de Commissie in kennis van de namen en adressen van hun overeenkomstig lid 1 aangewezen toezichthoudende organen en van alle latere wijzigingen daarvan. De Commissie maakt een lijst bekend van de aangemelde toezichthoudende organen.***

3. ***De rol van de overeenkomstig lid 1 aangewezen of opgerichte toezichthoudende organen is:***

   a) ***toezicht te houden op in de aanwijzende lidstaat gevestigde aanbieders van Europese portemonnees voor digitale identiteit en door middel van toezichthoudende activiteiten vooraf en achteraf te waarborgen dat die aanbieders en door hen aangeboden Europese portemonnees voor digitale identiteit voldoen aan de eisen in deze verordening;***

***b) indien nodig maatregelen te nemen ten aanzien van op het grondgebied van de aanwijzende lidstaat gevestigde aanbieders van Europese portemonnees voor digitale identiteit door middel van toezichthoudende activiteiten achteraf, wanneer zij ervan in kennis worden gesteld dat aanbieders of door hen aangeboden Europese portemonnees voor digitale identiteit inbreuk maken op deze verordening.***

***4. De taken van de overeenkomstig lid 1 aangewezen toezichthoudende organen zijn met name:***

***a) samenwerken met andere toezichthoudende organen en bijstand verlenen aan die organen overeenkomstig artikelen 46 quater en 46 sexies;***

***b) de nodige informatie opvragen om toezicht te houden op de naleving van deze verordening;***

*c) de overeenkomstig artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde relevante bevoegde autoriteiten van de betrokken lidstaten in kennis stellen van significante inbreuken op de veiligheid of integriteitsverlies waarvan zij kennis krijgen bij de uitvoering van hun taken en, in het geval van een significante inbreuk op de veiligheid of een integriteitsverlies betreffende andere lidstaten, het overeenkomstig artikel 8, lid 3, van Richtlijn (EU) 2022/2555 aangewezen of opgerichte centrale contactpunt van de betrokken lidstaat en de overeenkomstig artikel 46 quater, lid 1, van deze verordening aangewezen centrale contactpunten in de andere betrokken lidstaten op de hoogte brengen, en het publiek informeren of van aanbieders van een Europese portemonnee voor digitale identiteit vereisen dit te doen wanneer het toezichthoudende orgaan van oordeel is dat de bekendmaking van de inbreuk op de veiligheid of het verlies van integriteit in het algemeen belang zou zijn;*

*d) inspecties ter plaatse uitvoeren en toezicht buiten de locatie houden;*

*e) verlangen dat aanbieders van Europese portemonnees voor digitale identiteit iedere niet-naleving van de in deze verordening vastgelegde voorschriften rechtzetten;*

***f)*** ***de registratie van vertrouwende partijen en hun opname in het in artikel 5 ter, lid 7, bedoelde mechanisme opschorten of annuleren in geval van illegaal of frauduleus gebruik van de Europese portemonnee voor digitale identiteit;***

***g)*** ***samenwerken met de op grond van artikel 51 van Verordening (EU) 2016/679 opgerichte bevoegde toezichthoudende autoriteiten en in het bijzonder die 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.***

5. ***Indien het overeenkomstig lid 1 aangewezen toezichthoudend orgaan van de aanbieder van een Europese portemonnee voor digitale identiteit verlangt dat hij de niet-naleving van de voorschriften uit hoofde van deze verordening overeenkomstig lid 4, punt e), corrigeert en de aanbieder, indien van toepassing, niet binnen een door dat toezichthoudend orgaan vastgestelde termijn dienovereenkomstig handelt, kan het overeenkomstig lid 1 aangewezen toezichthoudend orgaan, met name rekening houdend met de omvang, de duur en de gevolgen van het niet handelen, de aanbieder gelasten de verstrekking van de Europese portemonnee voor digitale identiteit op te schorten of te beëindigen. Het toezichthoudende orgaan stelt de toezichthoudende organen van de andere lidstaten, de Commissie, de vertrouwende partijen en de gebruikers van de Europese portemonnee voor digitale identiteit onverwijld in kennis van het besluit om de opschorting of stopzetting van de afgifte van de Europese portemonnee voor digitale identiteit te verlangen.***

6. ***Elk overeenkomstig lid 1 aangewezen of opgerichte toezichthoudend orgaan legt de Commissie jaarlijks uiterlijk op 31 maart een verslag over betreffende zijn hoofdactiviteiten in het voorgaande kalenderjaar. De Commissie stelt die jaarlijkse verslagen beschikbaar aan het Europees Parlement en de Raad.***

*7. Uiterlijk op ... [twaalf maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie door middel van uitvoeringshandelingen de formaten en procedures voor het in lid 6 van dit artikel bedoelde verslag vast. De uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.*

*Artikel 46 ter*

*Toezicht op vertrouwensdiensten*

*1. De lidstaten wijzen een toezichthoudend orgaan aan dat op hun grondgebied is gevestigd of wijzen, in overeenstemming met een andere lidstaat, een in die andere lidstaat gevestigd toezichthoudend orgaan aan. Dat toezichthoudend orgaan is verantwoordelijk voor toezichthoudende taken in de aanwijzende lidstaat wat betreft vertrouwensdiensten.*

*De uit hoofde van de eerste alinea aangewezen toezichthoudende organen krijgen de noodzakelijke bevoegdheden en toereikende middelen voor de uitvoering van hun opdrachten.*

*2. De lidstaten stellen de Commissie in kennis van de namen en adressen van hun overeenkomstig lid 1 aangewezen of opgerichte toezichthoudende organen en van alle latere wijzigingen daarvan. De Commissie maakt een lijst bekend van de aangemelde toezichthoudende organen.*

*3. De taken van de overeenkomstig lid 1 aangewezen toezichthoudende organen zijn:*

*a) toezicht houden op gekwalificeerde verleners van vertrouwensdiensten die gevestigd zijn in de aanwijzende lidstaat en er door middel van toezichthoudende activiteiten vooraf en achteraf ervoor te zorgen dat die gekwalificeerde verleners van vertrouwensdiensten en de door hen verleende gekwalificeerde vertrouwensdiensten voldoen aan de voorschriften van deze verordening;*

*b) indien nodig optreden tegen niet-gekwalificeerde verleners van vertrouwensdiensten die gevestigd zijn in de aanwijzende lidstaat door middel van toezichthoudende activiteiten achteraf, wanneer het orgaan verneemt dat die niet-gekwalificeerde verleners van vertrouwensdiensten of de door hen verleende vertrouwensdiensten niet zouden voldoen aan de vereisten van deze verordening.*

*4. De taken van het overeenkomstig lid 1 aangewezen toezichthoudend orgaan zijn met name:*

*a) de overeenkomstig artikel 8, lid 1, van Richtlijn (EU) 2022/2555 aangewezen of ingestelde relevante bevoegde autoriteiten van de betrokken lidstaten in kennis stellen van significante inbreuken op de veiligheid of integriteitsverlies waarvan het kennis krijgt bij de uitvoering van zijn taken en, in het geval van een significante inbreuk op de veiligheid of een integriteitsverlies betreffende andere lidstaten, het overeenkomstig artikel 8, lid 3, van Richtlijn (EU) 2022/2555 aangewezen of opgerichte centrale contactpunt van de betrokken lidstaat en de overeenkomstig artikel 46 quater, lid 1, van deze verordening aangewezen centrale contactpunten in de andere betrokken lidstaten op de hoogte brengen, en het publiek informeren of van de verlener van vertrouwensdiensten vereisen dit te doen wanneer het toezichthoudend orgaan van oordeel is dat de bekendmaking van de inbreuk op de veiligheid of het verlies van integriteit in het algemeen belang zou zijn;*

*b) samenwerken met andere toezichthoudende organen en bijstand verlenen aan die organen overeenkomstig artikelen 46 quater en 46 sexies;*

*c) analyseren van de conformiteitsbeoordelingsverslagen bedoeld in artikel 20, lid 1, en artikel 21, lid 1;*

*d) aan de Commissie verslag uitbrengen over zijn hoofdactiviteiten, overeenkomstig lid 6;*

*e) audits uitvoeren of een conformiteitsbeoordelingsinstantie verzoeken een conformiteitsbeoordeling te doen van de gekwalificeerde verleners van vertrouwensdiensten overeenkomstig artikel 20, lid 2;*

*f) samenwerken met de op grond van artikel 51 van Verordening (EU) 2016/679 opgerichte bevoegde toezichthoudende autoriteiten en in het bijzonder die 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;"*

*g) de status van gekwalificeerd verlener van vertrouwensdiensten toekennen aan verleners van vertrouwensdiensten en aan de door hen verleende diensten, en die status intrekken, overeenkomstig de artikelen 20 en 21;*

***h) het voor de nationale vertrouwenslijst verantwoordelijke orgaan, bedoeld in artikel 22, lid 3, op de hoogte brengen van zijn besluiten om de status van gekwalificeerde toe te kennen of in te trekken, tenzij dit orgaan ook het overeenkomstig lid 1 van dit artikel aangewezen toezichthoudend orgaan is;***

***i) indien de gekwalificeerde verlener van vertrouwensdiensten zijn activiteiten beëindigt, nagaan of er bepalingen bestaan over beëindigingsplannen en of deze correct worden toegepast, waarbij zij onder meer nagaan hoe informatie toegankelijk wordt gehouden overeenkomstig artikel 24, lid 2, punt h);***

***j) verlangen dat verleners van vertrouwensdiensten iedere niet-naleving van de in deze verordening vastgestelde voorschriften rechtzetten;***

***k) onderzoeken van beweringen van aanbieders van webbrowsers overeenkomstig artikel 45 bis en zo nodig actie ondernemen.***

***5. De lidstaten mogen verlangen dat het overeenkomstig lid 1 aangewezen toezichthoudend orgaan een vertrouwensinfrastructuur opzet, onderhoudt en actualiseert in overeenstemming met het nationaal recht.***

*6. Elk overeenkomstig lid 1 aangewezen toezichthoudend orgaan legt de Commissie jaarlijks uiterlijk op 31 maart een verslag over betreffende zijn hoofdactiviteiten in het voorgaande kalenderjaar. De Commissie stelt die jaarlijkse verslagen beschikbaar aan het Europees Parlement en de Raad.*

*7. Uiterlijk op ... [twaalf maanden na de datum van inwerkingtreding van deze wijzigingsverordening] stelt de Commissie richtlijnen vast voor de uitoefening door de overeenkomstig lid 1 van dit artikel aangewezen toezichthoudende organen van de in lid 4 van dit artikel bedoelde taken en bepaalt zij door middel van uitvoeringshandelingen de formaten en procedures voor het in lid 6 van dit artikel bedoelde verslag. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure.*

*Artikel 46 quater*
*Centrale contactpunten*

*1. Elke lidstaat wijst een centraal contactpunt aan voor vertrouwensdiensten, Europese portemonnees voor digitale identiteit en aangemelde stelsels voor elektronische identificatie.*

*2.* Elk ***centraal contactpunt oefent een verbindingsfunctie uit om de grensoverschrijdende samenwerking tussen de toezichthoudende organen voor verleners van vertrouwensdiensten en tussen de toezichthoudende organen voor de aanbieders van Europese portemonnees voor digitale identiteit en, in voorkomend geval, met de Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en met andere bevoegde autoriteiten in zijn lidstaat te vergemakkelijken.***

*3.* ***Elke lidstaat maakt de namen en adressen van het overeenkomstig lid 1 aangewezen centrale contactpunt en eventuele latere wijzigingen daarvan openbaar en stelt de Commissie daarvan onverwijld in kennis.***

*4.* ***De Commissie maakt een lijst van de overeenkomstig lid 3 aangemelde centrale contactpunten bekend.***

***Artikel 46 quinquies***
***Wederzijdse bijstand***

*1.* ***Om het toezicht op en de handhaving van verplichtingen uit hoofde van deze verordening te vergemakkelijken, kunnen de overeenkomstig artikel 46 bis, lid 1) en artikel 46 ter, lid 1, aangewezen toezichthoudende organen onder meer via de krachtens artikel 46 sexies, lid 1, opgerichte samenwerkingsgroep, om wederzijdse bijstand verzoeken van de toezichthoudende organen van een andere lidstaat waar de aanbieder van de Europese portemonnee voor digitale identiteit of de verlener van vertrouwensdiensten is gevestigd of waar zijn netwerk- en informatiesystemen zich bevinden of zijn diensten worden verleend.***

*2. De wederzijdse bijstand houdt ten minste het volgende in:*

*a) het toezichthoudend orgaan dat in de ene lidstaat toezicht- en handhavingsmaatregelen toepast, informeert en raadpleegt het toezichthoudend orgaan van de andere betrokken lidstaat;*

*b) een toezichthoudend orgaan kan het toezichthoudend orgaan van een andere betrokken lidstaat verzoeken toezicht- of handhavingsmaatregelen te nemen, waaronder bijvoorbeeld verzoeken om inspecties uit te voeren in verband met de in de artikelen 20 en 21 bedoelde conformiteitsbeoordelingsverslagen inzake het verlenen van vertrouwensdiensten;*

*c) in voorkomend geval kunnen de toezichthoudende organen gezamenlijke onderzoeken uitvoeren met de toezichthoudende organen van andere lidstaten.*

*De regelingen en procedures voor gezamenlijke acties uit hoofde van de eerste alinea worden door de betrokken lidstaten overeenkomstig hun wetgeving overeengekomen en vastgelegd.*

*3. Een toezichthoudend orgaan tot welk een verzoek om bijstand wordt gericht, mag dat verzoek om alle onderstaande redenen weigeren:*

*a) de gevraagde bijstand staat niet in verhouding tot de toezichthoudende activiteiten van het toezichthoudend orgaan, uitgevoerd overeenkomstig artikelen 46 bis en 46 ter;*

*b) het toezichthoudend orgaan is niet bevoegd om de gevraagde bijstand te leveren;*

*c) het aanbieden van de gevraagde bijstand zou onverenigbaar zijn met deze verordening.*

*4. Uiterlijk op... [12 maanden na de datum van inwerkingtreding van deze wijzigingsverordening] en vervolgens om de twee jaar verstrekt de krachtens artikel 46 sexies, lid 1, opgerichte samenwerkingsgroep richtsnoeren over de organisatorische aspecten en procedures voor de in de leden 1 en 2 van dit artikel bedoelde wederzijdse bijstand.*

*Artikel 46 sexies*

*Europese samenwerkingsgroep voor digitale identiteit*

1. *Om de grensoverschrijdende samenwerking en uitwisseling van informatie over vertrouwensdiensten, Europese portemonnees voor digitale identiteit en aangemelde stelsels voor elektronische identificatie van de lidstaten te ondersteunen en te vergemakkelijken, richt de Commissie een Europese samenwerkingsgroep voor digitale identiteit (de "samenwerkingsgroep") op.*

2. *De samenwerkingsgroep bestaat uit vertegenwoordigers die zijn aangewezen door de lidstaten en de Commissie. De samenwerkingsgroep wordt voorgezeten door de Commissie. De Commissie voert het secretariaat van de samenwerkingsgroep.*

3. *Vertegenwoordigers van relevante belanghebbenden kunnen op ad-hocbasis worden uitgenodigd om de vergaderingen van de samenwerkingsgroep bij te wonen en als waarnemer deel te nemen aan de werkzaamheden ervan.*

4. *Enisa wordt uitgenodigd om als waarnemer deel te nemen aan de werkzaamheden van de samenwerkingsgroep bij de uitwisseling van standpunten, beste praktijken en informatie over relevante cyberbeveiligingsaspecten, zoals de melding van inbreuken op de beveiliging, het gebruik van cyberbeveiligingscertificaten of -normen.*

*5. De samenwerkingsgroep heeft de volgende taken:*

*a) advies uitwisselen en samenwerken met de Commissie wat betreft nieuwe beleidsinitiatieven op het gebied van portemonnees voor digitale identiteit, elektronische identificatiemiddelen en vertrouwensdiensten;*

*b) in voorkomend geval de Commissie advies verstrekken tijdens de vroege fase van het opstellen van ontwerpuitvoeringshandelingen en ontwerpen van gedelegeerde handelingen die op grond van deze verordening moeten worden vastgesteld;*

*c) ter ondersteuning van de toezichthoudende organen bij de uitvoering van de bepalingen van deze verordening:*

*i) beste praktijken en informatie betreffende de uitvoering van de bepalingen van deze verordening uitwisselen;*

*ii) relevante ontwikkelingen onderzoeken met betrekking tot digitale portemonnees, elektronische identificatie en de sectoren van vertrouwensdiensten;*

*iii) gezamenlijke bijeenkomsten organiseren met relevante belanghebbende partijen uit de hele Unie om de activiteiten van de samenwerkingsgroep te bespreken en input te verzamelen over nieuwe beleidsuitdagingen;*

*iv) met de steun van Enisa standpunten, beste praktijken en informatie uitwisselen over relevante cyberbeveiligingsaspecten met betrekking tot Europese portemonnees voor digitale identiteit, stelsels voor elektronische identificatie en vertrouwensdiensten;*

*v) beste praktijken uitwisselen betreffende de ontwikkeling en uitvoering van het beleid inzake de kennisgeving van beveiligingsinbreuken, en gemeenschappelijke maatregelen zoals bedoeld in de artikelen 5 sexies en 10;*

*vi) gezamenlijke vergaderingen organiseren met de bij artikel 14, lid 1, van Richtlijn (EU) 2022/2555 opgerichte NIS-samenwerkingsgroep om relevante informatie uit te wisselen met betrekking tot met vertrouwensdiensten en elektronische identificatie verband houdende cyberdreigingen, incidenten, kwetsbaarheden, bewustmakingsinitiatieven, opleidingen, oefeningen en vaardigheden, capaciteitsopbouw, capaciteit op het gebied van normen en technische specificaties, alsook normen en technische specificaties;*

*vii) op verzoek van een toezichthoudend orgaan specifieke verzoeken om wederzijdse bijstand zoals bedoeld in artikel 46 quinquies bespreken;*

*viii) de informatie-uitwisseling tussen de toezichthoudende organen vergemakkelijken door richtsnoeren te verstrekken over de organisatorische aspecten en procedures voor de in artikel 46 quinquies bedoelde wederzijdse bijstand;*

*d) collegiale toetsingen organiseren van stelsels voor elektronische identificatie die moeten worden aangemeld uit hoofde van deze verordening.*

*6. De lidstaten zorgen ervoor dat hun aangewezen vertegenwoordigers op doeltreffende en efficiënte wijze samenwerken binnen de samenwerkingsgroep.*

*7. Uiterlijk op... [12 maanden na de inwerkingtreding van deze wijzigings-verordening] stelt de Commissie door middel van uitvoeringshandelingen de noodzakelijke procedureregels vast om de samenwerking tussen de in lid 5, punt d), van dit artikel bedoelde lidstaten te faciliteren. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure.*";

*48) artikel 47 wordt als volgt gewijzigd:*

*a) de leden 2 en 3 worden vervangen door:*

*"2. De in artikel 5 quater, lid 7, artikel 24, lid 6, en artikel 30, lid 4, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen wordt met ingang van 17 september 2014 voor onbepaalde tijd aan de Commissie toegekend.*

*3. Het Europees Parlement of de Raad kan de in artikel 5 quater, lid 7, artikel 24, lid 6, en artikel 30, lid 4, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.";*

***b) lid 5 wordt vervangen door:***

***"5. Een overeenkomstig artikel 5 quater, lid 7, artikel 24, lid 6, of artikel 30, lid 4, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben meegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.***";

49) het volgende artikel ▌ wordt ingevoegd in hoofdstuk VI:

"Artikel 48 bis

Verslagleggingsvereisten

1. De lidstaten waarborgen dat statistieken worden verzameld over de ▌ werking van Europese portemonnees voor digitale identiteit en de gekwalificeerde vertrouwensdiensten ***die op hun grondgebied worden verstrekt***.

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) het aantal klachten van gebruikers en incidenten op het gebied van consumentenbescherming of gegevensbescherming die verband houden met vertrouwende partijen en gekwalificeerde vertrouwensdiensten;***

   d) een ***samenvattend verslag met gegevens over incidenten*** die het gebruik van ***de Europese*** portemonnee voor digitale identiteit verhinderen ▌;

   ***e) een samenvatting van significante beveiligingsincidenten, datalekken en getroffen gebruikers van Europese portemonnees voor digitale identiteit of van gekwalificeerde vertrouwensdiensten.***

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 over betreffende de overeenkomstig lid 2 verzamelde statistieken.***"***;

50) artikel 49 wordt vervangen door:

"Artikel 49
Evaluatie

1. De Commissie evalueert de toepassing van deze verordening en brengt daarover uiterlijk op ... [24 maanden na de datum van inwerkingtreding van de wijzigingsverordening] verslag uit bij het Europees Parlement en de Raad. In dat verslag evalueert de Commissie met name of het gepast is het toepassingsgebied van deze verordening dan wel de specifieke bepalingen ervan, ***met inbegrip van met name de bepalingen in artikel 5 quater, lid 5,*** te wijzigen, rekening houdend met de ervaring met de toepassing van deze verordening, alsook met technologische, markt- en juridische ontwikkelingen. Dat verslag gaat zo nodig vergezeld van een voorstel tot wijziging van deze verordening.

2. Het in lid 1 bedoelde verslag omvat een beoordeling van de beschikbaarheid***,*** ***de veiligheid*** en de bruikbaarheid van de ***aangemelde elektronische*** identificatiemiddelen ***en*** Europese portemonnees voor digitale identiteit die binnen het toepassingsgebied van deze verordening vallen, en beoordeelt of alle private onlinedienstverleners die voor gebruikersauthenticatie gebruikmaken van elektronische identificatiediensten van derden, is opgelegd om het gebruik van aangemelde elektronische identificatiemiddelen en Europese ***portemonnees voor digitale identiteit*** te aanvaarden.

3. Uiterlijk ... [6 jaar na de datum van inwerkingtreding van deze wijzigingsverordening] en daarna om de vier jaar dient de Commissie het in lid 1 bedoelde verslag een verslag over de vooruitgang bij de verwezenlijking van de doelstellingen van deze verordening in bij het Europees Parlement en de Raad.";

51) 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 wijzigingsverordening] 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 wijzigingsverordening] beschouwd als gekwalificeerde certificaten voor elektronische handtekeningen in de zin van deze verordening ▌.

***3. Het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische handtekeningen en zegels door gekwalificeerde verleners van vertrouwensdiensten die geen gekwalificeerde verleners van vertrouwensdiensten zijn die gekwalificeerde vertrouwensdiensten verlenen voor het beheer van gekwalificeerde middelen voor het op afstand aanmaken van elektronische handtekeningen en zegels overeenkomstig de artikelen 29 bis en 39 bis, kan tot en met ... [24 maanden na de inwerkingtreding van deze wijzigingsverordening] worden verricht zonder de gekwalificeerde status te hoeven verkrijgen voor het verlenen van deze beheerdiensten.***

***4. Gekwalificeerde verleners van vertrouwensdiensten aan wie uit hoofde van deze verordening de status "gekwalificeerd" is toegekend vóór ... [datum van inwerkingtreding van deze wijzigingsverordening], leggen het toezichthoudend orgaan zo spoedig mogelijk en in ieder geval uiterlijk ... [24 maanden na de inwerkingtreding van deze wijzigingsverordening] een conformiteitsbeoordelingsverslag voor dat bewijst dat aan artikel 24, leden 1, 1 bis en 1 ter, is voldaan.***";

52) de bijlagen I tot en met IV worden respectievelijk gewijzigd overeenkomstig de bijlagen I tot en met IV bij deze verordening.

53) de nieuwe bijlagen V, VI en VII worden toegevoegd zoals bepaald in de bijlagen V, VI en VII bij deze verordening.

Artikel ***2***

***Inwerkingtreding***

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 …,

| | |
|---|---|
| *Voor het Europees Parlement* | *Voor de Raad* |
| *De voorzitter* | *De voorzitter* |

BIJLAGE I

In bijlage I bij Verordening (EU) nr. 910/2014 wordt punt i) 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

In bijlage II bij Verordening (EU) nr. 910/2014 worden de punten 3 en 4 geschrapt.

BIJLAGE III

In bijlage III bij Verordening (EU) nr. 910/2014 wordt punt i) 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 bij Verordening (EU) nr. 910/2014 wordt als volgt gewijzigd:***

1) ***punt c) wordt vervangen door:***

"c) ***voor natuurlijke personen: op zijn minst de naam van de persoon aan wie het certificaat is afgegeven of een pseudoniem; indien een pseudoniem wordt gebruikt, een duidelijke vermelding in die zin;***

ca) ***voor rechtspersonen: een unieke reeks gegevens die de rechtspersoon aan wie het certificaat wordt afgegeven ondubbelzinnig weergeven, met ten minste de naam van de rechtspersoon aan wie het certificaat is afgegeven en, in voorkomend geval, het registratienummer zoals vermeld in de officiële administratie;";***

2) 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

“BIJLAGE V

EISEN VOOR

GEKWALIFICEERDE ELEKTRONISCHE ATTESTERING VAN ATTRIBUTEN

Gekwalificeerde elektronische attesteringen van attributen bevatten:

a) 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;

b) 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

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

   ii) voor een natuurlijk persoon: de naam van de persoon;

c) een reeks gegevens die ondubbelzinnig de entiteit weergeven waarnaar de geattesteerde attributen ***verwijzen***; indien een pseudoniem wordt gebruikt, een duidelijke aanwijzing in die zin;

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 gekwalificeerde verlener van vertrouwensdiensten 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 gekwalificeerde verlener van vertrouwensdiensten;

h) de locatie waar het certificaat ter ondersteuning van de ***gekwalificeerde*** elektronische handtekening of het ***gekwalificeerde*** elektronische zegel zoals bedoeld in punt ***g)***, gratis beschikbaar is;

i) de informatie of de locatie van de diensten waarbij informatie kan worden opgevraagd over de geldigheidsstatus van de gekwalificeerde attestering.”.

BIJLAGE VI

“BIJLAGE VI

MINIMALE LIJST VAN ATTRIBUTEN

Uit hoofde van artikel 45 sexies waarborgen de lidstaten dat, indien 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 ***Unie- of nationaal*** recht, 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. ***bevoegdheden en mandaten om natuurlijke of rechtspersonen te vertegenwoordigen***

10. openbare vergunningen en licenties;

11. ***voor rechtspersonen:*** financiële en bedrijfsgegevens.”.

*BIJLAGE VII*

*"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, een 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 zoals bedoeld in punt g), gratis beschikbaar is;*

*i) de informatie of de locatie van de diensten waarbij informatie kan worden opgevraagd over de geldigheidsstatus van de attestering.”.*

**BIJLAGE BIJ DE WETGEVINGSRESOLUTIE**

**Verklaring van de Commissie betreffende artikel 45 naar aanleiding van de vaststelling van Verordening 2024/…**[+]

De Commissie is ingenomen met het bereikte akkoord, waarin volgens haar duidelijk wordt gemaakt dat webbrowsers gekwalificeerde certificaten voor websiteauthenticatie moeten ondersteunen en ervoor moeten zorgen dat deze interoperabel zijn, met als enig doel de identiteitsgegevens van de eigenaar van de website op een gebruikersvriendelijke manier weer te geven. De Commissie is zich ervan bewust dat deze verplichting niet vooruitloopt op de methoden die worden gebruikt om deze identiteitsgegevens weer te geven.

De Commissie is ingenomen met het bereikte akkoord, waarin volgens haar duidelijk wordt gemaakt dat webbrowsers niet in hun veiligheidsbeleid worden beperkt doordat zij gekwalificeerde certificaten voor websiteauthenticatie moeten erkennen, en dat het in het voorgestelde artikel 45 aan de webbrowsers wordt overgelaten om hun eigen procedures en criteria te behouden en toe te passen teneinde de privacy van onlinecommunicatie met behulp van versleuteling en andere beproefde methoden te handhaven. De Commissie beseft dat in ontwerpartikel 45 aan webbrowsers geen verplichtingen of beperkingen worden opgelegd met betrekking tot de wijze waarop zij versleutelde verbindingen met websites tot stand brengen of waarop zij de cryptografische sleutels authenticeren die bij het opzetten van die verbindingen worden gebruikt.

De Commissie wijst erop dat zij, overeenkomstig punt 28 van het Interinstitutioneel Akkoord tussen het Europees Parlement, de Raad van de Europese Unie en de Europese Commissie over beter wetgeven van 13 april 2016, een beroep zal doen op deskundigengroepen, gericht belanghebbenden zal raadplegen en in voorkomend geval openbare raadplegingen zal houden.

---

[+] PB: gelieve het nummer in de tekst in te voegen en de overeenkomstige voetnoot voor 2021/0136(COD) aan te vullen.

**Verklaring van de Commissie over onzichtbaarheid naar aanleiding van de vaststelling van Verordening 2024/…**[+]

De Commissie is ingenomen met het bereikte akkoord, waarin volgens haar wordt bevestigd dat aanbieders van de Europese portemonnee voor digitale identiteit op grond van deze wijzigingsverordening geen persoonsgegevens mogen verwerken die zijn opgenomen in of voortvloeien uit het gebruik van de portemonnee, voor andere doeleinden dan de levering van portemonneediensten.

De Commissie is ook verheugd dat het begrip "onzichtbaarheid" in overweging 11 quater van het ontwerp van wijzigingsverordening is opgenomen, wat ervoor moet zorgen dat aanbieders van portemonnees geen details over de dagelijkse transacties van gebruikers kunnen zien en verzamelen. De Commissie is van mening dat dit begrip betekent dat er geen correlatie van gegevens tussen verschillende diensten mag zijn met het oog op het traceren van gebruikers of voor het bepalen, analyseren en voorspellen van persoonlijk gedrag, interesses of gewoonten.

Tegelijkertijd erkent de Commissie dat aanbieders van Europese portemonnees voor digitale identiteit, in volledige overeenstemming met Verordening (EU) 2016/679 en met uitdrukkelijke toestemming van de gebruiker, toegang mogen hebben tot bepaalde categorieën persoonsgegevens, bijvoorbeeld om te waarborgen dat zij ononderbroken portemonneediensten kunnen leveren of om de gebruikers te beschermen tegen verstoringen in de verlening ervan. Die gegevens moeten beperkt blijven tot wat voor elk specifiek doel noodzakelijk is."

---

[+] PB: gelieve het nummer in de tekst in te voegen en de overeenkomstige voetnoot voor 2021/0136(COD) aan te vullen.