Europees Parlement
2019-2024

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

2021/0136(COD)

11.10.2022

ADVIES

van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

aan de Commissie industrie, onderzoek en energie

inzake 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))

Rapporteur voor advies: Cristian Terheş

PA_Legam

AMENDEMENTEN

De Commissie burgerlijke vrijheden, justitie en binnenlandse zaken verzoekt de bevoegde Commissie industrie, onderzoek en energie onderstaande amendementen in aanmerking te nemen:

Amendement 1

Voorstel voor een verordening
Overweging 6

Door de Commissie voorgestelde tekst	*Amendement*
(6) ***Verordening*** (EU) 2016/679[19] ***is*** van toepassing op de verwerking van persoonsgegevens uit hoofde van deze verordening. Daarom moet deze verordening specifieke waarborgen bevatten om te voorkomen dat aanbieders van elektronische identificatiemiddelen en van elektronische attestering van attributen persoonsgegevens van andere diensten combineren met persoonsgegevens met betrekking tot de diensten die binnen het toepassingsgebied van deze verordening vallen.	(6) ***Natuurlijke of rechtspersonen die beschikken over persoonsidentificatiegegevens moeten als personen met een digitale identiteit worden beschouwd. Verordeningen*** (EU) 2016/679[19] ***en (EU) 2018/1725[19 bis] en Richtlijn 2002/58/EG[19 ter] 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 van andere diensten combineren met persoonsgegevens met betrekking tot de diensten die binnen het toepassingsgebied van deze verordening vallen. ***In deze verordening wordt de toepassing van de beginselen van doelbinding, minimale gegevensverwerking en gegevensbescherming door ontwerp en door standaardinstellingen op specifieke use cases nader gespecificeerd, onverminderd Verordening (EU) 2016/679.***
[19] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van	[19] 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).

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).

[19 bis] 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).

[19 ter] 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 (PB L 201 van 31.7.2002, blz. 37).

Amendement 2

Voorstel voor een verordening
Overweging 8

Door de Commissie voorgestelde tekst	*Amendement*
(8) Om naleving ***binnen*** het Unierecht***,*** of ***binnen*** het ***met het Unierecht overeenstemmende*** nationale recht te waarborgen, moeten dienstverleners de lidstaten ***in kennis stellen van hun intentie om gebruik te maken van*** de Europese portemonnees voor digitale identiteit. Op die manier kunnen de lidstaten gebruikers tegen fraude beschermen, onrechtmatig gebruik van identiteitsgegevens en elektronische attesteringen van attributen voorkomen, en waarborgen dat de verwerking van gevoelige gegevens, zoals	(8) Om naleving ***van*** het Unierecht of het nationale recht te waarborgen, moeten dienstverleners ***zich bij*** de lidstaten ***registreren voordat zij een beroep kunnen doen op*** de Europese portemonnees voor digitale identiteit. ***Natuurlijke of rechtspersonen moeten een klacht kunnen indienen met betrekking tot het gebruik van de Europese portemonnees voor digitale identiteit door een vertrouwende partij.*** Op die manier kunnen de lidstaten gebruikers tegen fraude beschermen, onrechtmatig gebruik van

gezondheidsgegevens, door vertrouwende partijen kan worden geverifieerd overeenkomstig het Unierecht of het nationale recht.	identiteitsgegevens en elektronische attesteringen van attributen voorkomen, en waarborgen dat de verwerking van gevoelige gegevens, zoals gezondheidsgegevens, door vertrouwende partijen kan worden geverifieerd overeenkomstig het Unierecht of het nationale recht. ***De lidstaten moeten onrechtmatig gebruik van identiteitsgegevens voorkomen en erop toezien dat de vertrouwende partijen alleen gegevens verlangen die strikt noodzakelijk zijn voor de verlening van de dienst.***

Amendement 3

Voorstel voor een verordening
Overweging 9

Door de Commissie voorgestelde tekst	*Amendement*
(9) Alle Europese portemonnees voor digitale identiteit moeten gebruikers in staat stellen om zich online en offline grensoverschrijdend te identificeren en te authenticeren om toegang tot een breed scala openbare en particuliere diensten te krijgen. Onverminderd de prerogatieven van de lidstaten betreffende de identificatie van hun onderdanen en ingezetenen, kunnen deze portemonnees ook tegemoetkomen aan de institutionele behoeften van overheidsinstanties, internationale organisaties en de instellingen, organen of instanties van de Unie. Offlinegebruik is van belang in veel sectoren, zoals de gezondheidssector waar diensten vaak via persoonlijke interactie worden verleend, en waar e-recepten op QR-codes of soortgelijke technologieën moeten kunnen vertrouwen om de authenticiteit te verifiëren. Wegens de "hoge" mate van zekerheid moeten de Europese portemonnees voor digitale identiteit kunnen gebruikmaken van het potentieel van onvervalsbare ***oplossingen***, zoals beveiligde elementen, ter naleving	(9) Alle Europese portemonnees voor digitale identiteit moeten gebruikers in staat stellen om zich online en offline grensoverschrijdend te identificeren en te authenticeren om toegang tot een breed scala openbare en particuliere diensten te krijgen. Onverminderd de prerogatieven van de lidstaten betreffende de identificatie van hun onderdanen en ingezetenen, kunnen deze portemonnees ook tegemoetkomen aan de institutionele behoeften van overheidsinstanties, internationale organisaties en de instellingen, organen of instanties van de Unie. Offlinegebruik is van belang in veel sectoren, zoals de gezondheidssector waar diensten vaak via persoonlijke interactie worden verleend, en waar e-recepten op QR-codes of soortgelijke technologieën moeten kunnen vertrouwen om de authenticiteit te verifiëren. ***De gebruikers moeten toegang hebben tot een eenvoudige interface die hen in staat stelt een overzicht te krijgen van de huidige en eerdere toestemmingen die zij hebben gekregen voor het delen van***

van de ***beveiligingsvoorschriften*** krachtens deze verordening. Met de Europese portemonnees voor digitale identiteit moeten gebruikers ook in de hele ***EU*** aanvaarde gekwalificeerde elektronische handtekeningen en zegels kunnen aanmaken en gebruiken. Met het oog op vereenvoudiging en kostenbesparingen voor personen en bedrijven in de hele ***EU***, onder meer door de mogelijkheid van vertegenwoordigingsbevoegdheden en e-mandaten, moeten de lidstaten gemeenschappelijke normen gebruiken wanneer zij Europese portemonnees voor digitale identiteit uitgeven zodat naadloze interoperabiliteit en een hoog beveiligingsniveau worden gewaarborgd. Alleen de bevoegde instanties van de lidstaten kunnen een hoge mate van vertrouwen bieden bij de vaststelling van de identiteit van een persoon en aldus uitmaken of de persoon die stelt een bepaalde identiteit te hebben, daadwerkelijk is wie de persoon zegt dat hij of zij is. Daarom moeten de Europese portemonnees voor digitale identiteit gebruikmaken van de wettelijke identiteit van burgers, andere ingezetenen of rechtspersonen. Het vertrouwen in de Europese portemonnees voor digitale identiteit zou nog hoger worden als de uitgevende partijen verplicht zijn passende technische en organisatorische maatregelen te treffen om een beveiligingsniveau te waarborgen dat in overeenstemming is met de risico's voor de rechten en vrijheden van natuurlijke personen, conform Verordening (EU) 2016/679.

persoonsgegevens of elektronische attestering van attributen. Zij moeten de mogelijkheid hebben hun toestemming in te trekken. Wegens de "hoge" mate van zekerheid moeten de Europese portemonnees voor digitale identiteit kunnen gebruikmaken van het potentieel van onvervalsbare ***technologie***, zoals beveiligde elementen, ter naleving van de ***beveiligings- en integriteitsvoorschriften*** krachtens deze verordening. Met de Europese portemonnees voor digitale identiteit moeten gebruikers ook in de hele ***Unie*** aanvaarde gekwalificeerde elektronische handtekeningen en zegels kunnen aanmaken en gebruiken. 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 gemeenschappelijke normen gebruiken wanneer zij Europese portemonnees voor digitale identiteit uitgeven zodat naadloze interoperabiliteit en een hoog beveiligingsniveau worden gewaarborgd. Alleen de bevoegde instanties van de lidstaten kunnen een hoge mate van vertrouwen bieden bij de vaststelling van de identiteit van een persoon en aldus uitmaken of de persoon die stelt een bepaalde identiteit te hebben, daadwerkelijk is wie de persoon zegt dat hij of zij is. Daarom moeten de Europese portemonnees voor digitale identiteit ***in bepaalde use cases*** gebruikmaken van de wettelijke identiteit van burgers, andere ingezetenen of rechtspersonen. Het vertrouwen in de Europese portemonnees voor digitale identiteit zou nog hoger worden als de uitgevende partijen verplicht zijn passende technische en organisatorische maatregelen te treffen om een beveiligingsniveau te waarborgen dat in overeenstemming is met de risico's voor de rechten en vrijheden van natuurlijke personen, conform Verordening (EU)

2016/679.

Amendement 4

Voorstel voor een verordening
Overweging 9 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(9 bis) Om de succesvolle invoering van de Europese portemonnee voor digitale identiteit te waarborgen, is het van cruciaal belang te zorgen voor vertrouwen in het technische kader achter en het digitale ecosysteem rondom de portemonnee. Een hoge mate van transparantie kan bijdragen tot het kweken van vertrouwen, en wel door gebruikers in staat te stellen weloverwogen beslissingen te nemen over de veiligheids- en privacykenmerken van de Europese portemonnee voor digitale identiteit, en door publieke controle op de activiteiten en actoren die bij het kader betrokken zijn mogelijk te maken. Daarom moeten de lidstaten erop toezien dat relevante informatie, zoals instellingen voor de bescherming van de privacy, technische architectuur, beveiligingskaders en de locatie waar persoonsgegevens worden verwerkt, wordt opgenomen in de minimale informatie over de Europese portemonnee voor digitale identiteit en openbaar beschikbaar wordt gesteld.

Amendement 5

Voorstel voor een verordening
Overweging 9 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(9 ter) Een van de doelstellingen van de Europese portemonnee voor digitale identiteit moet zijn om de burgers beter in

	staat te stellen zelf te kiezen welke gegevens zij delen, de hoeveelheid gedeelde gegevens voor de dienst die zij willen gebruiken tot een minimum te beperken en de gedeelde gegevens beter te beheren en te controleren.

Amendement 6

Voorstel voor een verordening
Overweging 10

Door de Commissie voorgestelde tekst	*Amendement*
(10) 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. De overeenstemming van de Europese portemonnees voor digitale identiteit met die vereisten moet worden gecertificeerd door vanwege de lidstaten aangewezen geaccrediteerde openbare of private organen. Het gebruik van een certificeringsregeling op basis van met de lidstaten overeengekomen ***beschikbare*** gemeenschappelijke normen moet een hoog niveau van vertrouwen ***en*** interoperabiliteit waarborgen. Certificering moet met name steunen op de overeenkomstig Verordening (EU) 2019/881 vastgestelde relevante Europese cyberbeveiligingscertificeringsregelingen[20] . Die certificering moet de certificering inzake de verwerking van persoonsgegevens overeenkomstig Verordening (EU) 2016/679 onverlet laten.	(10) 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. De overeenstemming van de Europese portemonnees voor digitale identiteit met die vereisten moet worden gecertificeerd door vanwege de lidstaten aangewezen geaccrediteerde openbare of private organen. Het gebruik van een certificeringsregeling op basis van ***geavanceerde technologie en*** met de lidstaten overeengekomen gemeenschappelijke normen moet een hoog niveau van vertrouwen**,** interoperabiliteit ***en gegevensbescherming*** waarborgen. Certificering moet met name steunen op de overeenkomstig Verordening (EU) 2019/881 vastgestelde relevante Europese cyberbeveiligingscertificeringsregelingen[20] . Die certificering moet de certificering inzake de verwerking van persoonsgegevens overeenkomstig Verordening (EU) 2016/679 onverlet laten.
[20] 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	[20] 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).	informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

Amendement 7

Voorstel voor een verordening
Overweging 11

Door de Commissie voorgestelde tekst	*Amendement*
(11) Europese portemonnees voor digitale identiteit moeten het hoogste beveiligingsniveau voor de voor authenticatie gebruikte persoonsgegevens waarborgen, ongeacht of die gegevens lokaal ***of*** in de cloud worden opgeslagen, met inachtneming van de verschillende risiconiveaus. Het gebruik van biometrische gegevens voor authenticatie ***is een van de identificatiemethoden die een hoog niveau van betrouwbaarheid bieden, met name in combinatie met andere authenticatie-elementen***. Omdat biometrische gegevens een uniek kenmerk van een persoon vormen, ***zijn voor*** het gebruik van biometrische gegevens organisatorische ***en*** beveiligingsmaatregelen vereist die in verhouding staan tot het risico dat de verwerking kan inhouden voor de rechten en vrijheden van natuurlijke personen, overeenkomstig ***Verordening (EU) 2016/679***.	(11) Europese portemonnees voor digitale identiteit moeten het hoogste beveiligingsniveau voor de voor authenticatie gebruikte persoonsgegevens waarborgen, ongeacht of die gegevens lokaal***,*** in de cloud ***of een combinatie van beide*** worden opgeslagen, met inachtneming van de verschillende risiconiveaus. Het gebruik van biometrische gegevens voor authenticatie ***mag geen voorwaarde zijn voor het gebruik van de Europese portemonnee voor digitale identiteit, ondanks het vereiste van sterke gebruikersauthenticatie***. Omdat biometrische gegevens een uniek kenmerk van een persoon vormen, ***is*** het gebruik van biometrische gegevens ***beperkt tot specifieke scenario's uit hoofde van Verordening (EU) 2016/679, en zijn daarvoor technische en*** organisatorische beveiligingsmaatregelen vereist die in verhouding staan tot het risico dat de verwerking kan inhouden voor de rechten en vrijheden van natuurlijke personen, overeenkomstig ***die verordening***. ***De mogelijkheid om informatie uit de Europese portemonnee voor digitale identiteit op te slaan in de cloud moet alleen worden geactiveerd als de gebruiker daarvoor uitdrukkelijk toestemming heeft gegeven. De lidstaten moeten toestaan dat de Europese portemonnee voor digitale identiteit cryptografisch materiaal opslaat en***

	transacties op het apparaat van de gebruiker verwerkt zonder gebruik te hoeven maken van clouddiensten, tenzij de gebruiker uitdrukkelijk toestemming geeft voor deze vorm van opslag. Indien de Europese portemonnee voor digitale identiteit beschikbaar is op het apparaat van de gebruiker, moet het cryptografische materiaal van de portemonnee in de beveiligde elementen van het apparaat worden opgeslagen.

Amendement 8

Voorstel voor een verordening
Overweging 12

Door de Commissie voorgestelde tekst	*Amendement*
(12) Om het Europese kader voor digitale identiteit toekomstbestendig en open voor innovatie en technologische ontwikkelingen te houden, moeten de lidstaten worden aangemoedigd om gezamenlijke testomgevingen op te zetten om innovatieve oplossingen in een gecontroleerde en veilige omgeving te testen, in het bijzonder om de functionaliteit, de bescherming van persoonsgegevens, de beveiliging en de interoperabiliteit van de oplossingen te verbeteren en om technische referenties en wettelijke vereisten in toekomstige updates op te nemen. Het Europese midden- en kleinbedrijf, startups en individuele innovatoren en onderzoekers moeten worden gestimuleerd om aan deze omgeving deel te nemen.	(12) Om het Europese kader voor digitale identiteit toekomstbestendig en open voor innovatie en technologische ontwikkelingen te houden, moeten de lidstaten worden aangemoedigd om gezamenlijke testomgevingen op te zetten om innovatieve oplossingen in een gecontroleerde en veilige omgeving te testen, in het bijzonder om de functionaliteit, de bescherming van persoonsgegevens, de beveiliging en de interoperabiliteit van de oplossingen te verbeteren en om technische referenties en wettelijke vereisten in toekomstige updates op te nemen. Het Europese midden- en kleinbedrijf, startups en individuele innovatoren en onderzoekers moeten worden gestimuleerd om aan deze omgeving deel te nemen***, waarbij de naleving moet worden verbeterd en moet worden voorkomen dat oplossingen op de markt worden gebracht die indruisen tegen het Unierecht inzake gegevensbescherming en IT-beveiliging***.

Amendement 9

Voorstel voor een verordening
Overweging 17

Door de Commissie voorgestelde tekst	*Amendement*
(17) Uit de reeks persoonsidentificatiegegevens die beschikbaar zijn uit stelsels voor elektronische identificatie op grond van Verordening (EU) nr. 910/2014 gebruiken dienstverleners de identiteitsgegevens om gebruikers uit een andere lidstaat te matchen met de wettelijke identiteit van die gebruiker. Ondanks het gebruik van de eIDAS-gegevens zijn voor een nauwkeurige match in veel gevallen evenwel aanvullende informatie over de gebruiker en specifieke unieke identificatieprocedures op nationaal niveau nodig. Met het oog op een ruimere bruikbaarheid van elektronische identificatiemiddelen, moeten de lidstaten krachtens de verordening specifieke maatregelen nemen om te waarborgen dat tijdens het elektronische identificatieproces de identiteit correct wordt gematcht. ***Voor datzelfde doel moet deze verordening ook de verplichte minimale reeks gegevens uitbreiden en*** het gebruik van ***een uniek*** en ***permanent elektronisch identificatiemiddel overeenkomstig het Unierecht vastleggen voor die gevallen waarin het noodzakelijk is*** de gebruiker ***op eigen verzoek op*** unieke en permanente ***wijze wettelijk te identificeren***.	(17) Uit de reeks persoonsidentificatiegegevens die beschikbaar zijn uit stelsels voor elektronische identificatie op grond van Verordening (EU) nr. 910/2014 gebruiken dienstverleners de identiteitsgegevens om gebruikers uit een andere lidstaat te matchen met de wettelijke identiteit van die gebruiker. Ondanks het gebruik van de eIDAS-gegevens zijn voor een nauwkeurige match in veel gevallen evenwel aanvullende informatie over de gebruiker en specifieke unieke identificatieprocedures op nationaal niveau nodig. Met het oog op een ruimere bruikbaarheid van elektronische identificatiemiddelen, moeten de lidstaten krachtens de verordening specifieke maatregelen nemen om te waarborgen dat tijdens het elektronische identificatieproces de identiteit correct wordt gematcht. ***Het gebruik van persoonsidentificatiegegevens of een combinatie van persoonsidentificatiegegevens, met inbegrip van*** het gebruik van ***door de lidstaten afgegeven of door de Europese portemonnee voor digitale identiteit gegenereerde unieke en permanente identificatiecodes, is van essentieel belang om ervoor te zorgen dat de identiteit van*** de gebruiker***, met name in de overheidssector en indien het Unierecht of het nationale recht dat vereist, kan worden geverifieerd***. ***De wetgeving van de lidstaten moet het gebruik van voor de sector of de vertrouwende partij specifieke,*** unieke en permanente ***identificatiecodes kunnen voorschrijven. De Europese portemonnee voor digitale identiteit moet die identificatiecodes kunnen opslaan en op verzoek van de gebruiker openbaar kunnen maken.***

Amendement 10

Voorstel voor een verordening
Overweging 25

Door de Commissie voorgestelde tekst	*Amendement*
(25) Meestal kunnen burgers en andere ingezetenen niet veilig en met een hoog niveau van gegevensbescherming grensoverschrijdend digitaal informatie uitwisselen met betrekking tot hun identiteit, zoals adres, leeftijd en beroepskwalificaties, rijbewijzen en andere vergunningen en betalingsgegevens.	(25) ***Op de interne markt moeten burgers de mogelijkheid krijgen om informatie over hun identiteit grensoverschrijdend uit te wisselen.*** Meestal kunnen burgers en andere ingezetenen ***echter*** niet veilig en met een hoog niveau van gegevensbescherming grensoverschrijdend digitaal ***officieel gecertificeerde*** informatie uitwisselen met betrekking tot hun identiteit, zoals adres, leeftijd en beroepskwalificaties, rijbewijzen en andere vergunningen en betalingsgegevens. ***Dit zou ertoe kunnen leiden dat die gegevens op een minder veilige en minder georganiseerde wijze worden doorgegeven.***

Amendement 11

Voorstel voor een verordening
Overweging 29

Door de Commissie voorgestelde tekst	*Amendement*
(29) Het moet technisch mogelijk zijn dat de Europese portemonnee voor digitale identiteit de attributen selectief openstelt voor vertrouwende partijen. Deze functie moet een fundamentele ontwerpfunctie worden, om het gemak en de bescherming van persoonsgegevens, inclusief minimale verwerking van persoonsgegevens, te vergroten.	(29) Het moet technisch mogelijk zijn dat de Europese portemonnee voor digitale identiteit de attributen selectief ***en op veilige en gebruikersvriendelijke wijze*** openstelt voor vertrouwende partijen ***als een van de belangrijkste kenmerken en voordelen ervan***. ***Er moet ook voor worden gezorgd dat er geen attributen openbaar worden gemaakt aan partijen die niet geregistreerd zijn om dergelijke attributen te ontvangen.*** Deze functie moet een fundamentele ontwerpfunctie worden, om het gemak en de bescherming van persoonsgegevens, inclusief minimale verwerking van persoonsgegevens, te vergroten***, met name privacy door ontwerp en door standaardinstellingen***.

	Mechanismen voor de validering van de Europese portemonnee voor digitale identiteit, selectieve openbaarmaking en authenticatie van gebruikers om toegang te krijgen tot onlinediensten moeten de privacy beschermen, waardoor het volgen van de gebruiker wordt voorkomen en het beginsel van doelbinding in acht wordt genomen, hetgeen een recht op pseudonimiteit inhoudt zodat de gebruiker niet in verband kan worden gebracht met verschillende vertrouwende partijen. De technische architectuur en de uitvoering van de Europese portemonnee voor digitale identiteit moeten volledig in overeenstemming zijn met Verordening (EU) 2016/679. Bovendien moet het gedecentraliseerde karakter van de portemonnee het mogelijk maken attributen en identificatiecodes zelf te ondertekenen en te herroepen.

Amendement 12

Voorstel voor een verordening
Overweging 29 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(29 bis) Tenzij specifieke regels van de Unie of het nationaal recht voorschrijven dat gebruikers zich moeten identificeren, moet het gebruik van diensten onder een pseudoniem worden toegestaan en mogen de lidstaten dit niet beperken, bijvoorbeeld door dienstverleners een algemene verplichting op te leggen om het gebruik van hun diensten onder pseudoniem te beperken.

Amendement 13

Voorstel voor een verordening
Overweging 35

Door de Commissie voorgestelde tekst	*Amendement*
(35) De certificering als gekwalificeerde aanbieders van vertrouwensdiensten moet rechtszekerheid bieden voor use cases die op elektronische registers voortbouwen. Deze vertrouwensdiensten voor elektronische registers en gekwalificeerde elektronische registers, en de certificering als gekwalificeerde aanbieder van vertrouwensdiensten voor elektronische registers moeten het feit dat use cases het Unierecht, of met het Unierecht overeenstemmende nationale recht moeten naleven, onverlet laten. Use cases waarbij persoonsgegevens worden verwerkt, moeten in overeenstemming zijn met Verordening (EU) 2016/679. Use cases die betrekking hebben op cryptoactiva, moeten verenigbaar zijn met alle toepasselijke financiële regels, zoals de richtlijn markten voor financiële instrumenten[23], de richtlijn betalingsdiensten[24] ***en*** de toekomstige verordening betreffende markten in cryptoactiva[25].	(35) De certificering als gekwalificeerde aanbieders van vertrouwensdiensten moet rechtszekerheid bieden voor use cases die op elektronische registers voortbouwen. Deze vertrouwensdiensten voor elektronische registers en gekwalificeerde elektronische registers, en de certificering als gekwalificeerde aanbieder van vertrouwensdiensten voor elektronische registers moeten het feit dat use cases het Unierecht, of met het Unierecht overeenstemmende nationale recht moeten naleven, onverlet laten. Use cases waarbij persoonsgegevens worden verwerkt, moeten in overeenstemming zijn met Verordening (EU) 2016/679. Use cases die betrekking hebben op cryptoactiva, moeten verenigbaar zijn met alle toepasselijke financiële regels, zoals de richtlijn markten voor financiële instrumenten[23], de richtlijn betalingsdiensten***[24],*** de toekomstige verordening betreffende markten in cryptoactiva[25] ***en de verordening geldovermakingen[25 bis]***.
[23] Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (Voor de EER relevante tekst), PB L 173 van 12.6.2014, blz. 349.	[23] Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (Voor de EER relevante tekst), PB L 173 van 12.6.2014, blz. 349.
[24] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35).	[24] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35).
[25] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten voor cryptoactiva en	[25] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten voor cryptoactiva en

tot wijziging van Richtlijn (EU) 2019/1937, COM(2020) 593 final.	tot wijziging van Richtlijn (EU) 2019/1937, COM(2020) 593 final.
	25 bis Voorstel voor een verordening van het Europees Parlement en de Raad betreffende bij overmakingen van geld en van bepaalde cryptoactiva te voegen informatie (herschikking), 2021/0241(COD).

Amendement 14

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 3 – i
Verordening (EU) nr. 910/2014
Artikel 3 – alinea 1 – punt 42

Door de Commissie voorgestelde tekst	*Amendement*
(42) "Europese portemonnee voor digitale identiteit": een ***product en dienst die*** de gebruiker in staat ***stellen*** identiteitsgegevens, inloggegevens en attributen met betrekking tot ***zijn/haar*** identiteit te beheren op te slaan, op verzoek ***aan*** vertrouwende partijen te verstrekken, voor online en offline authenticatie voor een dienst overeenkomstig artikel 6 bis te gebruiken, en gekwalificeerde elektronische handtekeningen en zegels aan te maken;	(42) "Europese portemonnee voor digitale identiteit": een ***elektronisch identificatiemiddel dat*** de gebruiker in staat ***stelt op een door de gebruiker gecontroleerd apparaat*** identiteitsgegevens, ***expliciete bevestigingen van toestemming voor het delen van persoonsgegevens,*** inloggegevens en attributen met betrekking tot ***de*** identiteit ***van de gebruiker*** te beheren ***en*** op te slaan, op verzoek ***selectief*** aan ***naar behoren geregistreerde*** vertrouwende partijen te verstrekken en voor online en offline authenticatie voor een dienst overeenkomstig artikel 6 bis te gebruiken, en gekwalificeerde elektronische handtekeningen en zegels aan te maken;

Amendement 15

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 3 – i
Verordening (EU) nr. 910/2014
Artikel 3 – alinea 1 – punt 43

Door de Commissie voorgestelde tekst	*Amendement*
(43) "attribuut": een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit***, in elektronisch formaat***;	(43) "attribuut": ***een elektronische weergave van*** een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit;

Amendement 16

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 3 – i
Verordening (EU) nr. 910/2014
Artikel 3 – alinea 1 – punt 55

Door de Commissie voorgestelde tekst	*Amendement*
(55) "***unieke identificatie***": een proces waarbij persoonsidentificatiegegevens of persoonsidentificatiemiddelen met een bestaande account van dezelfde persoon worden gematcht of gekoppeld.";	(55) "***identiteitsmatching***": een proces waarbij persoonsidentificatiegegevens of persoonsidentificatiemiddelen met een bestaande account van dezelfde persoon worden gematcht of gekoppeld.";

Amendement 17

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 4
Verordening (EU) nr. 910/2014
Artikel 5 – titel

Door de Commissie voorgestelde tekst	*Amendement*
Pseudoniemen in elektronische transacties	***Bescherming van persoonsgegevens en*** pseudoniemen in elektronische transacties

Amendement 18

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 4
Verordening (EU) nr. 910/2014
Artikel 5 – alinea 1

Door de Commissie voorgestelde tekst	*Amendement*
Onverminderd het rechtsgevolg dat aan het	***1. De verwerking van***

gebruik van pseudoniemen op grond van nationaal recht wordt toegekend, wordt het gebruik ervan in elektronische transacties ***niet verboden****.;*

persoonsgegevens geschiedt in overeenstemming met Verordeningen (EU) 2016/679 en (EU) 2018/1725 en, in voorkomend geval, Richtlijn 2002/58/EG, door de beginselen van minimale gegevensverwerking, doelbinding en gegevensbescherming door ontwerp en door standaardinstellingen toe te passen, met name met betrekking tot de technische maatregelen voor de uitvoering van deze verordening en het interoperabiliteitskader overeenkomstig artikel 12 van die verordening.

2. Onverminderd het rechtsgevolg dat aan het gebruik van pseudoniemen op grond van nationaal recht wordt toegekend, wordt het gebruik ervan in elektronische transacties ***toegestaan***. ***Het gebruik van een door de gebruiker vrijelijk gekozen pseudoniem is altijd een optie om een unieke identificatiecode te vervangen wanneer de identificatie van de gebruiker niet vereist is op grond van het Unierecht of het nationale recht.***

3. Vertrouwende partijen leveren redelijke inspanningen om het gebruik van hun diensten zonder elektronische identificatie of authenticatie mogelijk te maken.”

Amendement 19

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 3 – punt b bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	b bis) een weloverwogen beslissing nemen over het delen van persoonsgegevens met vertrouwende partijen. Dit is inclusief de identificatie van de vertrouwende partij, de mogelijkheid tot een volledige of gedeeltelijke weigering van informatieverzoeken van vertrouwende

	partijen en een volledig transactieoverzicht.

Amendement 20

Voorstel voor een verordening
Artikel 1 – lid 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt a – 2

Door de Commissie voorgestelde tekst	*Amendement*
(2) voor vertrouwende partijen om persoonsidentificatiegegevens en elektronische attesteringen van attributen aan te vragen en te valideren;	(2) voor vertrouwende partijen om persoonsidentificatiegegevens en elektronische attesteringen van attributen aan te vragen en te valideren ***overeenkomstig Verordening (EU) 2016/679***;

Amendement 21

Voorstel voor een verordening
Artikel 1 – lid 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt a – 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(2 bis) voor vertrouwende partijen om naar behoren te worden geregistreerd op een openbaar toegankelijke lijst en om hun informatieverzoeken zichtbaar te maken op die openbaar beschikbare lijst;

Amendement 22

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt a – 3

Door de Commissie voorgestelde tekst	*Amendement*
(3) om lokaal en zonder internettoegang voor de portemonnee, persoonsidentificatiegegevens,	(3) om lokaal en zonder internettoegang voor de portemonnee, persoonsidentificatiegegevens***, zoals***

elektronische attestering van attributen of andere gegevens***, zoals inloggegevens,*** aan vertrouwende partijen aan te bieden;	***inloggegevens,*** elektronische attestering van attributen of andere gegevens aan vertrouwende partijen aan te bieden ***overeenkomstig Verordening (EU) 2016/679 en voor de gebruiker om een weloverwogen beslissing te nemen over het delen van persoonlijke informatie met vertrouwende partijen, waarbij wordt gewaarborgd dat selectieve openbaarmaking mogelijk is en de aangeboden gegevens kunnen bestaan uit een volledige of gedeeltelijke afwijzing van informatieverzoeken van vertrouwende partijen, een volledige transactiegeschiedenis, de mogelijkheid om eerder verleende toestemming voor informatieverzoeken en informatie over de uitoefening van rechten als betrokkene in te trekken***;

Amendement 23

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt b

Door de Commissie voorgestelde tekst	*Amendement*
b) waarborgen dat verleners ***van vertrouwensdiensten*** van gekwalificeerde attesteringen van attributen ***geen*** informatie over het gebruik van die attributen ***kunnen*** ontvangen;	b) waarborgen dat verleners van gekwalificeerde ***en niet-gekwalificeerde*** attesteringen van attributen ***door de technologie belemmerd worden om*** informatie over het gebruik van die attributen ***te*** ontvangen;

Amendement 24

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt e

Door de Commissie voorgestelde tekst	*Amendement*
e) waarborgen dat de in artikel 12, lid	e) waarborgen dat de in artikel 12, lid

4, punt d), bedoelde persoonsidentificatiegegevens uniek ***en permanent*** de ***daarmee verbonden*** natuurlijke of rechtspersonen vertegenwoordigen***.***	4, punt d), bedoelde persoonsidentificatiegegevens uniek de natuurlijke of rechtspersonen vertegenwoordigen ***en dat de verwijzing naar die gegevens voor alle vertrouwende partijen anders is, indien dat wettelijk vereist is;***

Amendement 25

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt e bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	e bis) de gebruiker in staat stellen toegang te krijgen tot een in leesbaar formaat opgestelde lijst met handelingen, transacties of het gebruik van elektronische attesteringen van attributen of persoonsidentificatiegegevens waarvoor de gebruiker toestemming heeft gegeven;

Amendement 26

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 – punt e ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	e ter) de gebruiker in staat stellen de gegevens van de Europese portemonnee voor digitale identiteit over te dragen en de toegang tot die portemonnee te blokkeren wanneer zich een inbreuk op de beveiliging voordoet zodat gegevens kunnen worden opgeschort, teruggeroepen of ingetrokken.

Amendement 27

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 4 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	4 bis. Als er sprake is van een keten van vertrouwende partijen verwerven tussenpersonen geen kennis over de inhoud van de transactie.

Amendement 28

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 7

Door de Commissie voorgestelde tekst	*Amendement*
7. De gebruiker heeft volledige controle over de Europese portemonnee voor digitale identiteit. De afgever van de Europese portemonnee voor digitale identiteit ***verzamelt geen*** informatie over het gebruik van de portemonnee ***die niet noodzakelijk is voor de levering van de portemonneediensten, noch combineert hij persoonsidentificatiegegevens en andere persoonsgegevens die zijn opgeslagen of betrekking hebben op het gebruik van*** de Europese portemonnee voor digitale identiteit ***met persoonsgegevens van*** andere ***door deze afgever of derden aangeboden diensten als die niet noodzakelijk zijn voor de levering van de portemonneediensten, tenzij*** de gebruiker ***daar uitdrukkelijk om heeft gevraagd***. Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnees voor digitale identiteit worden fysiek en logisch gescheiden van andere opgeslagen gegevens. Indien de Europese portemonnee voor digitale identiteit wordt verstrekt door particuliere partijen overeenkomstig lid 2,	7. ***Het technische kader voor de Europese portemonnee voor digitale identiteit is onderworpen aan de volgende beginselen:***

punten b) en c), is artikel 45 septies, lid 4, van overeenkomstige toepassing.

a) De gebruiker heeft volledige controle over de Europese portemonnee voor digitale identiteit ***en de gegevens van de gebruiker, waaronder zelfcertificering***.

b) De Europese portemonnee voor digitale identiteit maakt gebruik van gedecentraliseerde elementen voor de identiteitsarchitectuur.

c) De reeks elektronische identificatiemiddelen, attributen en certificaten in een Europese portemonnee voor digitale identiteit wordt veilig en uitsluitend opgeslagen op door de gebruiker gecontroleerde apparaten, tenzij de gebruiker vrijelijk instemt met opslag op apparaten van derden of met een cloudgebaseerde optie.

d) De Europese portemonnee voor digitale identiteit verschaft cryptografisch verifieerbare inloggegevens.

e) De Europese portemonnee voor digitale identiteit maakt beveiligde verbindingen tussen de gebruiker en de vertrouwende partijen mogelijk.

f) De technische architectuur van de Europese portemonnee voor digitale identiteit belet de afgever van de Europese portemonnee voor digitale identiteit***, de lidstaat of enige andere partij elektronische identificatiemiddelen, attributen, elektronische documenten in een Europese portemonnee voor digitale identiteit en*** informatie over het gebruik van de portemonnee ***via de gebruiker te verzamelen of te verkrijgen, tenzij de gebruiker daarom verzoekt met behulp van door hem/haar zelf gecontroleerde apparaten. De uitwisseling van informatie via*** de Europese portemonnee voor digitale identiteit ***maakt het niet mogelijk dat aanbieders van elektronische attesteringen van attributen transacties of gebruikersgedrag volgen, aan elkaar koppelen, met elkaar in verband brengen***

of anderszins kennis daarover verwerven.

g) Unieke en permanente identificatiecodes zijn niet toegankelijk voor vertrouwende partijen in andere ***gevallen dan wanneer de identificatie van*** de gebruiker ***op grond van het Unierecht of het nationale recht vereist is***.

h) De lidstaten zien erop toe dat de relevante informatie over de Europese portemonnee voor digitale identiteit openbaar beschikbaar is.

i) Persoonsgegevens met betrekking tot de verstrekking van de Europese portemonnees voor digitale identiteit worden fysiek en logisch gescheiden van andere opgeslagen gegevens.

j) Indien de Europese portemonnee voor digitale identiteit wordt verstrekt door particuliere partijen overeenkomstig lid 2, punten b) en c), is artikel 45 septies, lid 4, van overeenkomstige toepassing.

k) Indien voor de attestering van attributen geen identificatie van de gebruiker vereist is, wordt "zero knowledge" attestering uitgevoerd.

l) De afgever van de Europese portemonnee voor digitale identiteit is de verwerkingsverantwoordelijke voor de doeleinden van Verordening (EU) 2016/679 met betrekking tot de verwerking van persoonsgegevens in de Europese portemonnee voor digitale identiteit.

m) De Europese portemonnee voor digitale identiteit voorziet in een klachtenmechanisme om gebruikers in staat te stellen het toezichthoudende orgaan uit hoofde van deze verordening en de krachtens Verordening (EU) 2016/679 opgerichte toezichthoudende autoriteiten rechtstreeks te informeren wanneer een vertrouwende partij verzoekt om een onevenredige hoeveelheid gegevens die niet in overeenstemming is met het geregistreerde beoogde gebruik

van die gegevens.

Amendement 29

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 7
Verordening (EU) nr. 910/2014
Artikel 6 bis – lid 7 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	7 bis. De toegang van natuurlijke personen tot openbare en particuliere diensten, tot onlineplatforms in de zin van Verordening (EU) XXX/XXX [wet inzake digitale diensten] of tot de arbeidsmarkt wordt niet afhankelijk gesteld van het gebruik van de Europese portemonnee voor digitale identiteit.
	Het gebruik van de Europese portemonnees voor digitale identiteit is facultatief en gratis en geeft in geen geval aanleiding tot enige vorm van discriminatie.
	Natuurlijke personen ondervinden geen nadelen bij het niet-gebruiken van de Europese portemonnee voor digitale identiteit.

Amendement 30

Voorstel voor een verordening
Artikel 1 – lid 1 – punt 12
Verordening (EU) nr. 910/2014
Artikel 11 bis – titel

Door de Commissie voorgestelde tekst	*Amendement*
Unieke identificatie	***Identiteitsmatching***

Amendement 31

Voorstel voor een verordening
Artikel 1 – lid 1 – punt 12

Verordening (EU) nr. 910/2014
Artikel 11 bis – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. Indien aangemelde elektronische identificatiemiddelen en de Europese portemonnees voor digitale identiteit worden gebruikt voor ***authenticatie***, waarborgen de lidstaten ***een unieke identificatie***.	1. Indien aangemelde elektronische identificatiemiddelen en de Europese portemonnees voor digitale identiteit worden gebruikt voor ***elektronische identificatie***, waarborgen de lidstaten ***identiteitsmatching***.

Amendement 32

Voorstel voor een verordening
Artikel 1 – lid 1 – punt 12
Verordening (EU) nr. 910/2014
Artikel 11 bis – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
2. ***Voor de toepassing van deze verordening nemen de lidstaten in de minimale reeks gegevens van de in artikel 12, lid 4, punt d), bedoelde persoonsidentificatiegegevens een unieke en permanente identificatiecode overeenkomstig het Unierecht op,*** om de gebruiker op hun verzoek te identificeren in die gevallen waarin gebruikersidentificatie wettelijk voorgeschreven is.	2. Om de gebruiker op hun verzoek te identificeren in die gevallen waarin gebruikersidentificatie wettelijk voorgeschreven is***, worden door de lidstaten afgegeven of door de Europese portemonnees voor digitale identiteit gegenereerde unieke en permanente identificatiecodes verstrekt, samen met de minimale reeks gegevens van de in artikel 12, lid 4, punt d) bedoelde persoonsidentificatiegegevens***. ***De lidstaten kunnen eisen dat unieke en permanente identificatiecodes specifiek zijn voor de sector of vertrouwende partij, mits die codes de gebruiker in de hele Unie op unieke wijze identificeren.***

Amendement 33

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 13 – b
Verordening (EU) nr. 910/2014
Artikel 12 – lid 4 – punt d

Door de Commissie voorgestelde tekst	*Amendement*
d) een verwijzing naar een ***minimale*** reeks persoonsidentificatiegegevens die nodig is om een natuurlijke of rechtspersoon op unieke ***en permanente*** wijze te vertegenwoordigen***;***;	d) een verwijzing naar een reeks persoonsidentificatiegegevens die nodig is om een natuurlijke of rechtspersoon op unieke wijze te vertegenwoordigen ***en die beschikbaar is vanaf stelsels voor elektronische identificatie***;

Amendement 34

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 20 – a – 2
Verordening (EU) nr. 910/2014
Artikel 17– lid 4 – punt f

Door de Commissie voorgestelde tekst	*Amendement*
f) samenwerken met de overeenkomstig Verordening (EU) 2016/679 opgerichte toezichthoudende autoriteiten en in het bijzonder deze instanties onverwijld informeren over de resultaten van de audits van gekwalificeerde verleners van vertrouwensdiensten indien er regels inzake de bescherming van persoonsgegevens zijn overtreden, en over beveiligingsinbreuken die inbreuken op persoonsgegevens vormen;”;	f) samenwerken met de overeenkomstig Verordening (EU) 2016/679 opgerichte toezichthoudende autoriteiten en in het bijzonder deze instanties onverwijld informeren over de resultaten van de audits van gekwalificeerde verleners van vertrouwensdiensten indien er ***bewijs bestaat dat*** regels inzake de bescherming van persoonsgegevens zijn overtreden, en over beveiligingsinbreuken die ***waarschijnlijk*** inbreuken op persoonsgegevens vormen***, of over vermoedens van zulke inbreuken die zijn geconstateerd bij de uitvoering van zijn taken, onverminderd Verordening (EU) 2016/679***;”;

Amendement 35

Voorstel voor een verordening
Artikel 1 – alinea 1 – punt 22 – b
Verordening (EU) nr. 910/2014
Artikel 20 – alinea 2

Door de Commissie voorgestelde tekst	*Amendement*
Indien er sprake blijkt te zijn van een inbreuk op de regels voor de bescherming van persoonsgegevens brengt het toezichthoudend orgaan de toezichthoudende autoriteiten op grond van Verordening (EU) 2016/679 op de hoogte ***van*** de resultaten van de audits.;	***Onverminderd eventuele verdere verplichtingen voor verwerkingsverantwoordelijken of verwerkers die voortvloeien uit Verordening (EU) 2016/679,*** brengt het toezichthoudende orgaan***, indien er redenen zijn om aan te nemen dat de gegevensbeschermingsregels kunnen zijn geschonden,*** de toezichthoudende autoriteiten op grond van Verordening (EU) 2016/679***, de afgever en de verwerkingsverantwoordelijke van de Europese portemonnee voor digitale identiteit daarvan onverwijld*** op de hoogte ***en verstrekt het*** de resultaten van de audits ***zodra die beschikbaar zijn***;

ANNEX: LIST OF ENTITIES OR PERSONS FROM WHOM THE RAPPORTEUR HAS RECEIVED INPUT

De volgende lijst wordt op zuiver vrijwillige basis opgesteld onder de exclusieve bevoegdheid van de rapporteur voor advies. De rapporteur heeft bij de opstelling van het advies tot het moment van goedkeuring in de commissie informatie ontvangen van de volgende entiteiten of personen:

Entity and/or person

1. European Commission DG CNECT

2. The European Data Protection Supervisor
3. Brussels Privacy Hub, *THE EUROPEAN COMMISSION PROPOSAL AMENDING THE eIDAS REGULATION (EU) No 910/2014: A PERSONAL DATA PROTECTION PERSPECTIVE*
4. Professor Ricardo Genghini, Chairman of the European Standardization Committee E-Signature and Infrastructures (ESI) within the European Telecommunications Standards Institute (ETSI) - *Notes on the current draft of eIDAS Revision Proposal*
5. epicenter.works & European Digital Rights (EDRI)
6. Luukas Ilves, Deputy Secretary General of the Estonian Ministry of Economic Affairs and Communications for Digital Development
7. European Consumer Organisation (BEUC) - *Making European Digital Identity as Safe as It Is needed - BEUC Position Paper*
8. Jaap-Henk Hoepman, Associate Professor of privacy enhancing protocols and privacy by design in the Digital Security group at the Institute for Computing and Information Sciences of the Radboud University Nijmegen, *Civil liberties aspects of the commission proposal to amend the eIDAS regulation*
9. Eric Verheul, professor in the Digital Security Group of the Radboud University Nijmegen - *Issues and recommendations on the eIDAS wallet as proposed in the eIDAS update*
10. Manuel Atug expert in IT Security and engineering Chaos Computer Club & Christian Kahlo eID expert - *written input*
11. Lukasz Olejnik, PhD, https://lukaszolejnik.com, *written contribution*
12. Carmela Troncoso - Professor on Security and Privacy at Swiss Federal Institute of Technology Lausanne - *written input*
13. Dr. F. S. Gürses, Associat Professor at the Faculty of Technology, Policy and Management, TU Delft - *written input*
14. Eurosmart - The Voice Of The Digital Security Industry - Feedback on the revision of eIDAS
15. Mozzila
16. Google
17. Apple
18. The International Association for Trusted Blockchain Applications (INATBA) - Establishing a Framework for a European Digital Identity (eIDAS) - Policy Position
19. TWG Trusted Information of the EU Observatory for ICT Standardisation - report on "Trust in the European digital space in the age of automated bots and fakes"
20. Rule of Law Defense Coalition, Bucharest Romania
21. American Chamber of Commerce to the European Union, Brussels - *written input*

PROCEDURE VAN DE ADVISERENDE COMMISSIE

Titel	Wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit
Document- en procedurenummers	COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)
Bevoegde commissie Datum bekendmaking	ITRE 8.7.2021
Advies uitgebracht door Datum bekendmaking	LIBE 8.7.2021
Medeverantwoordelijke commissies - datum bekendmaking	16.12.2021
Rapporteur voor advies Datum benoeming	Cristian Terheş 29.11.2021
Behandeling in de commissie	12.1.2022 30.5.2022
Datum goedkeuring	10.10.2022
Uitslag eindstemming	+: 51 –: 1 0: 4
Bij de eindstemming aanwezige leden	Abir Al-Sahlani, Konstantinos Arvanitis, Malik Azmani, Pietro Bartolo, Malin Björk, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Clare Daly, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Assita Kanko, Alice Kuhnke, Jeroen Lenaers, Lukas Mandl, Nuno Melo, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Emil Radev, Paulo Rangel, Terry Reintke, Karlo Ressler, Diana Riba i Giner, Isabel Santos, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Ramona Strugariu, Tomas Tobé, Yana Toom, Milan Uhrík, Elissavet Vozemberg-Vrionidi, Elena Yoncheva, Javier Zarzalejos
Bij de eindstemming aanwezige vaste plaatsvervangers	Romeo Franz, Erik Marquardt, Fulvio Martusciello, Peter Pollák, Paul Tang, Róża Thun und Hohenstein, Miguel Urbán Crespo
Bij de eindstemming aanwezige plaatsvervangers (art. 209, lid 7)	Marek Paweł Balt, Gilles Boyer, Jonás Fernández, Hannes Heide, Othmar Karas, Georgios Kyrtsos, Karsten Lucke, Evelyn Regner, Antonio Maria Rinaldi, Simone Schmiedtbauer, Ralf Seekatz, Michal Šimečka, Ivan Štefanec

HOOFDELIJKE EINDSTEMMING IN DE ADVISERENDE COMMISSIE

51	+
PPE	Andrzej Halicki, Othmar Karas, Jeroen Lenaers, Lukas Mandl, Fulvio Martusciello, Nuno Melo, Nadine Morano, Peter Pollák, Emil Radev, Paulo Rangel, Karlo Ressler, Simone Schmiedtbauer, Ralf Seekatz, Sara Skyttedal, Ivan Štefanec, Tomas Tobé, Elissavet Vozemberg-Vrionidi, Javier Zarzalejos
RENEW	Abir Al-Sahlani, Malik Azmani, Gilles Boyer, Sophia in 't Veld, Georgios Kyrtsos, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Róża Thun und Hohenstein, Yana Toom
S&D	Marek Paweł Balt, Pietro Bartolo, Jonás Fernández, Hannes Heide, Evin Incir, Karsten Lucke, Javier Moreno Sánchez, Evelyn Regner, Isabel Santos, Birgit Sippel, Paul Tang, Elena Yoncheva
THE LEFT	Konstantinos Arvanitis, Malin Björk, Clare Daly, Miguel Urbán Crespo
VERTS/ALE	Patrick Breyer, Saskia Bricmont, Romeo Franz, Alice Kuhnke, Erik Marquardt, Terry Reintke, Diana Riba i Giner

1	-
NI	Milan Uhrík

4	0
ECR	Assita Kanko, Vincenzo Sofo
ID	Patricia Chagnon, Antonio Maria Rinaldi

Verklaring van gebruikte tekens:
+ : voor
- : tegen
0 : onthouding