Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Regie op Gegevens Referentiearchitectuur

Delen van persoonsgegevens

Versie 2023

Datum 1 september 2023

REGIE OP GEGEVENS

Zelf geregeld, veilig en betrouwbaar!

1 Inleiding

1.1 Versiehistorie

Versie 0.2	20-8-2020	Initiële versie voor interne review
Versie 0.3	8-9-2020	Versie voor externe review
Versie 0.4	12-1-2021	Feedback externe review verwerkt
Versie 0.5	12-5-2021	Aanpassing hoofdstuk 2 en enkele tekstuele aanpassingen t.b.v. de leesbaarheid.
Versie 0.6 (versie 2021)	25-10-2021	Andere opmaak i.v.m. leesbaarheid Toevoeging Europese ontwikkelingen Aanvullingen op hoofdstukken Applicaties en Infrastructuur
Versie 2022	1-11-2022	Algemeen: bevindingen openbare review verwerkt Hoofdstuk 2 Juridisch Kader Aangepast n.a.v. eIDAS amendement en toolbox In bijlagen 11-16 uitvoerige analyse van relevante EU-regelgeving i.r.t. actoren en rechten en plichten per actor paragraaf 2.3 WDO: geen wijzigingen omdat er in 2022 geen voortgang op deze wet is geweest. Hoofdstuk 3 Leidende principes koppeling met nieuwe NORA-principes gemaakt. Hoofdstuk 4 Functiemodel Regie op Gegevens Diverse aanpassingen n.a.v. review Hoofdstuk 5 Gegevens Aanvullingen n.a.v. toolbox eIDAS Hoofdstuk 6 Processen Aanvulling usecases Hoofdstuk 7 Applicaties Aanvullingen n.a.v. toolbox eIDAS Bijlage 10 Definitielijst

1.2 Doelstelling RoG

De overheid maakt voor de uitoefening van haar taken intensief gebruik van persoonlijke gegevens van burgers. Zowel de overheid zelf als de burgers hebben er belang bij dat die gegevens correct en actueel zijn, efficiënt worden gebruikt, en veilig worden bewaard en gebruikt, conform geldende wetgeving.

Een burger kan inzien welke gegevens de overheid heeft en waarvoor deze worden gebruikt, en kan deze zo nodig (laten) corrigeren of wijzigen als ze onjuist of niet meer actueel zijn. Ook heeft hij het recht om (basis)gegevens die de overheid al heeft niet onnodig (opnieuw) te verstrekken.
Dit is staand beleid en wettelijk verankerd in de Algemene wet bestuursrecht (Awb), de Algemene verordening gegevensbescherming

(AVG) en wetgeving voor de basisregistraties. Daarmee is de basis voor regie op de eigen gegevens gelegd.

Het kabinet wil deze bestaande regiemogelijkheden uitbreiden met een belangrijk nieuw spoor, door burgers in staat te stellen hun eigen gegevens zelf, digitaal te delen met private dienstverleners, zoals zorgverleners, onderwijsinstellingen, schuldhulpverleners of woningcorporaties.
Hierdoor kunnen deze hun klanten betere diensten leveren, en wordt de administratieve rompslomp beperkt (Beleidsbrief Regie op Gegevens: nadere uitwerking, p. 2).

Onder regie op persoonlijke gegevens wordt in de brief verstaan (p. 1): de handelingsopties die de burger heeft als het gaat om de gegevens die overheidsorganisaties en nader te bepalen andere organisaties in het BSN-domein (w.o. zorgverleners) over hem vastleggen.
Hierbij wordt onderscheid gemaakt in drie vormen van regie:
1. inzage en correctie
de eigen gegevens kunnen inzien en controleren, kunnen inzien welke gegevens worden en zijn uitgewisseld, en de gegevens kunnen (laten) corrigeren;
2. eenmalige verstrekking
kunnen weigeren om gegevens te verstrekken die binnen de overheid al beschikbaar zijn;
3. delen van gegevens
de eigen gegevens zelf, digitaal kunnen delen met dienstverleners buiten de overheid.

1.3 Doelstelling referentiearchitectuur

De doelstellingen van Regie op Gegevens zijn (of worden momenteel) vertaald naar wetgeving, beleid en principes (vgl. hoofdstuk 2). Dit geeft richting en kleur aan het gewenste maatschappelijke effect. Anderzijds zijn er al verscheidende initiatieven waarin concrete voorzieningen voor het delen van gegevens gerealiseerd zijn of worden. Deze referentie-architectuur wordt gepositioneerd als generiek model tussen wetgeving en beleid enerzijds en de concrete initiatieven die al onderweg zijn of nog gaan komen anderzijds. Anders gesteld: de wat-vraag (wat moet er geregeld/ingericht worden om de doelstellingen te kunnen realiseren met als 'scharnierpunt' het Functiemodel RoG) staat centraal en minder de hoe-vraag (met welke concrete oplossingen wordt die wat-vraag ingevuld). Die hoe-vraag wordt dus ingevuld door de (architectuur van de) sectoren/projecten zelf.

1.4 Scope van deze referentiearchitectuur

De doelstelling van Regie op Gegevens is de burger regie te laten voeren op zijn eigen persoonsgegevens door de mogelijkheid te bieden persoonsgegevens in administraties van de overheid in te zien, daar waar nodig te corrigeren en indien gewenst de delen met derden. Inzage heeft betrekking op de persoonsgegevens die de overheid in zijn administraties heeft opgenomen én inzicht geven in welke persoonsgegevens tussen welke overheden worden gedeeld. Het functiemodel in deze referentiearchitectuur ondersteunt deze doelstelling, naast de doelstelling van het delen van gegevens vanuit een overheidsadministratie met de burger zelf.

2 Juridisch kader

2.1 Europese ontwikkelingen t.a.v. de data-economie

Europese ontwikkelingen ten aanzien van een interne markt voor data (d.w.z. de samenwerking tussen 27 lidstaten waar Nederland onderdeel van is en een bijdrage aan levert) hebben directe invloed op de ontwikkeling van de data-economie in Nederland. Die Europese samenwerking is al een aantal jaren gericht op het creëren van een interne markt voor gegevens zodat gegevens vrij kunnen stromen binnen de EU en tussen sectoren, e.e.a. met inachtneming van de Europese waarden. De EU stelt hierover in zijn Europese Datastrategie (gehele tekst):

De EU werkt aan een interne markt voor data, waarin:
gegevens tussen de verschillende EU-landen en de sectoren kunnen circuleren ten voordele van iedereen;
de Europese regels volledig in acht worden genomen, vooral wat betreft privacy, gegevensbescherming en mededinging;
eerlijke, praktische en duidelijke regels voor de toegang tot en het gebruik van data gelden.
De EU wordt een aantrekkelijke, veilige en dynamische data-economie door:

- *duidelijke en eerlijke regels op te stellen voor toegang tot en hergebruik van data;*
- *te investeren in de volgende generatie van instrumenten en infrastructuren voor opslag en verwerking van data;*
- *de krachten te bundelen voor de ontwikkeling van Europese cloudcapaciteit;*
- *in belangrijke sectoren Europese data samen te brengen in de vorm van gemeenschappelijke en interoperabele dataruimten;*
- *gebruikers de rechten, tools en vaardigheden te geven om volledige controle over hun data uit te oefenen.*

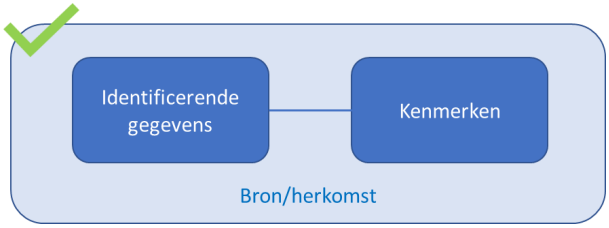
Een aantal onderdelen van deze Europese ontwikkeling van de data-economie heeft directe invloed op Regie op Gegevens. De belangrijkste is misschien wel de ontwikkeling van de Europese Digitale Identiteit (op basis van eIDAS-verordening uit 2014) ten behoeve van elektronische identificatie en waarmerken van die identificatie met behulp van vertrouwensservices.

Naar aanleiding van een recente evaluatie (rapport) is door de Europese Commissie *voorgesteld* deze ontwikkeling uit te breiden op het gebied van het waarmerken van gegevenssets (dus de combinatie tussen identiteit en uitspraken over die identiteit, de *provision of electronic attributes,* sectie 9 van het amendement) en de eis aan de lidstaten om (direct of indirect) te voorzien in een eWallet voor burgers zodat zijn hun rechten beter kunnen effectueren. Gerelateerd aan eisen vanuit de GDPR zijn deze ontwikkelingen samen te vatten tot:

1. De eIDAS-verordening 2014 introduceert de elektronische identificatie en waarmerken van die identificatie met behulp van vertrouwensservices met als doel de ontwikkeling van de Single Digital Markt

2. De GDPR-verordening 2016 regelt de rechten van personen ten aanzien van de verwerking van hun persoonsgegevens in die Single Digital Market
3. Het amendement op de eIDAS-verordening 2021 introduceert de eWallet om personen de praktische mogelijkheid te geven controle over hun persoonsgegevens te krijgen.

Deze drie ontwikkelingen tezamen zorgen ervoor dat het dus mogelijk gaat worden dat een gekende bron een gewaarmerkte bewering (kenmerken) over een persoon (identificerende gegevens) kan doen:



Daarnaast wordt interoperabiliteit (door standaardisatie) van groot belang geacht voor de succesvolle realisatie van deze strategie. De lidstaten ontwikkelen daartoe gezamenlijk de IT-standaarden. Hiervoor wordt ieder jaar een plan opgesteld. Voor Regie op gegevens is o.a. van belang de standaarden voor *Electronic identification and trust services* en *e-privacy*.

Naast de eIDAS-verordering en de GDPR/AVG zijn (tenminste op onderdelen) van belang voor Regie op Gegevens:

1- Data Governance Act
- het voor hergebruik beschikbaar stellen van overheidsgegevens, wanneer die gegevens onderworpen zijn aan rechten van anderen;
- delen van gegevens tussen bedrijven tegen vergoeding, in welke vorm dan ook;
- toestaan dat persoonsgegevens worden gebruikt met behulp van een "bemiddelaar voor het delen van persoonsgegevens", die als taak heeft personen te helpen hun rechten uit hoofde van de algemene verordening gegevensbescherming (AVG) uit te oefenen;
- het gebruik van gegevens op altruïstische gronden toestaan.

2- Data Market Act
- Stelt regels voor poortwachters

3- Data Services Act
- Stelt regels voor alle online intermediairs (w.o. transparantie en verantwoording)

4- Single Digital Gateway
- Geeft invulling aan het grensoverschrijdende *once-only* principe en de regie van de burger hierop. Dit is binnen Nederland al langer staand beleid en opnieuw opgenomen in de Beleidsbrief 2019. Once-only binnen de grenzen van de EU is daarmee een uitbreiding op het werkingsgebied van dit principe binnen de Nederlandse overheid.

2.2 Globaal overzicht requirements vanuit eIDAS en GDPR

2.2.1 Regiehandelingen vanuit de GDPR

De basis voor regiehandelingen (recht op inzage, correctie en delen) is te vinden in de GDPR en de ePrivacy-verordening:

Regulation	Article	Rechten/plichten burger
AVG	7, lid 3	Recht zijn toestemming voor de verwerking van zijn persoonsgegevens ten alle tijde in te trekken
	13, lid 2, c)	Recht de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid.
	13, lid 2, d)	Recht om toestemming te allen tijde in te trekken
	13, lid 2, e)	Recht een klacht in te dienen bij een toezichthoudende autoriteit
	15, lid 1	Recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van de persoonsgegevens en 8 informatie-typen.
	15, lid 2	Recht om in kennis te worden gesteld van de passende waarborgen inzake de doorgifte aan een derde land of een internationale organisatie.
	16	Recht om onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen
	16	Recht om vervollediging van onvolledige persoonsgegevens te verkrijgen.
	17	Recht op gegevenswissing (recht op vergetelheid)
	18	Recht op beperking van de verwerking
	20	Recht op overdraagbaarheid van gegevens
	21	Recht op bezwaar
	22	Recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit.
	77	Recht om klacht in te dienen bij een toezichthoudende autoriteit
	79	Recht om een doeltreffende voorziening in rechte in te stellen tegen de verwerkingsverantwoordelijke of een verwerker
	80	Recht op het opdrachtgeven aan een externe om namens hem een klacht in te dienen.
ePrivacy	9, lid 3	Recht om toestemming voor de verwerking van elektronische communicatiegegevens te allen tijde in te trekken
	10, lid 2	Plicht om voor de voortzetting van de installatie van software een privacy-instelling te aanvaarden.
	16, lid 2	Recht om duidelijk en expliciet in de gelegenheid gesteld te zijn om kosteloos en op gemakkelijke wijze bezwaar te maken tegen het gebruik van elektronische contactgegevens t.b.v. direct marketing.
	22	Recht op schadevergoeding en aansprakelijkheid

2.2.2 Eisen aan de eWallet (eIDAS)

In het amendement op eIDAS (2021) zijn de requirements voor de eWallet uitgewerkt. In onderstaande tabel wordt een overzicht gegeven van deze requirements.

Article	Requirements
Art. 6a (3)	User shall: - securely - request and obtain, store, select, combine and share, - in a manner that is transparent to and traceable by the user - the necessary legal person identification data and electronic attestation of attributes - to authenticate online and offline - in order to use online public and private services; - sign by means of qualified electronic signatures.
Art. 6a (4a)	Digital Identity Wallets shall provide - a common interface - to qualified and non-qualified trust service providers - issuing qualified and non-qualified electronic attestations of attributes - or other qualified and non-qualified certificates - for the purpose of issuing such attestations and certificates to the European Digital Identity Wallet - (2) for relying parties to request and validate person identification data and electronic attestations of attributes - (3) for the presentation to relying parties of person identification data, electronic attestation of attributes or other data such as credentials, - in local mode not requiring internet access for the wallet - (4) for the user to allow interaction with the European Digital Identity Wallet - and display an "EU Digital Identity Wallet Trust Mark"
Art. 6a (4b)	- Ensure that trust service providers of qualified attestations of attributes cannot receive any information about the use of these attributes.
Art. 6a (4c)	- Meet the requirements set out in Article 8 with regards to assurance level "high", - in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication
Art. 6a (4d)	- Provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes.
Art. 6a (4e)	- Ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural or legal person is associated with it.
Art. 6a (6)	- The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'
Art. 6a (6)	- The use of the European Digital Identity Wallets shall be free of charge to natural persons
Art. 6a (7)	- The user shall be in full control of the European Digital Identity Wallet. - The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, - nor shall it combine person identification data and any other personal data stored - or relating to the use of the European Digital Identity Wallet - with personal data from any other services offered by this issuer - or from third-party services - which are not necessary for the provision of the wallet services, - unless the user has expressly requested it
Art. 6a (8)	- Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet.
Art. 6a (9)	- Article 24(2), points (b), (e), (g), and (h) shall apply mutatis mutandis to Member States issuing the European Digital Identity Wallets.
Art. 6a (10)	- The European Digital Identity Wallet shall be made accessible for persons with disabilities in accordance with the accessibility requirements of Annex I to Directive 2019/882.
Art. 6a (11)	- Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications and reference standards for the requirements referred to in paragraphs 3, 4 and 5 by means of an implementing act on the implementation of the European Digital Identity Wallet. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).
Art. 6c (1)	- European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a paragraphs 3, 4 and 5 in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

Art. 12b (6)	-	For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9.

2.3 Relevante Nederlandse wetgeving voor Regie op gegevens

In 2020 heeft een inventarisatie plaatsgevonden naar het relevante juridische kader voor Regie op Gegevens. Samengevat bestaat dit uit:

1. Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG)
2. Verdieping AVG: toestemming als grondslag voor het verwerken van persoonsgegevens versus toestemming voor een regietoepassing
3. Wet basisregistratie personen (Wet BRP)
4. Wet algemene bepalingen burgerservicenummer (Wabb)
5. eIDAS-verordening (directe werking)
6. Wet elektronisch bestuurlijk verkeer (Webv)
7. Algemene beginselen van behoorlijk bestuur
8. Geheimhoudingsplichten
9. Vertegenwoordigen en machtigen in het BW en de Awb
10. Verantwoordelijkheden en aansprakelijkheden
11. Mededinging en de Wet Markt en Overheid (Wet M&O)
12. Archiefwet
13. Tijdelijk besluit digitale toegankelijkheid overheid
14. Diverse wet- en regelgeving voor bronnen van aanbieders

Voor een nadere toelichting wordt verwezen naar het rapport dat via bovenstaande link toegankelijk is gemaakt.

2.4 Wet Digitale Overheid

Het wetsvoorstel Wet digitale overheid (Wdo) legt de basis voor de verdere digitalisering van de overheid. De eerste tranche (deel) van Wdo gaat over veilig inloggen op dienstverlening bij (semi-) overheidsinstanties. De Wet digitale overheid is de opvolger van de Wet Generieke digitale infrastructuur (GDI). De GDI bestaat uit een set voorzieningen t.a.v. Identificatie & Authenticatie, Dienstverlening, Gegevens en Interconnectiviteit.

Het wetsvoorstel is een zogeheten kaderwet; de wet regelt algemene principes, verantwoordelijkheden en procedures, maar geen gedetailleerde regels. De wet zorgt zo voor flexibiliteit bij nieuwe ontwikkelingen. Maar ook dat belangrijke waarden en zekerheden voor burgers, zoals gebruikersvriendelijkheid, betrouwbaarheid, veiligheid, privacy en digitale inclusie altijd geborgd zijn.

Deze wet:

- legt de taken en verantwoordelijkheden vast voor veilige toegang tot de digitale overheid;
- legt verplichtingen op aan mede-overheden om veilig en betrouwbaar aan te sluiten, en hun dienstverlening in te delen op een betrouwbaarheidsniveau;
- stelt regels over de bekostiging daarvoor;
- biedt zekerheden voor burgers en bedrijven;
- biedt uitgangspunten voor informatiebeveiliging en de verwerking van persoonsgegevens.

Het wetsvoorstel gaat over veilig inloggen op dienstverlening bij (semi-) overheidsinstanties. In de Wdo staat welke van deze instanties te maken krijgen met de nieuwe regels voor de toegang tot hun elektronische dienstverlening. Dit zijn:

- bestuursorganen in de zin van de Awb, zoals gemeenten en uitvoeringsinstanties (UWV, SVB, Belastingdienst, DUO, RDW, etc.);
- aangewezen organisaties als de zorgsector, onderwijsinstellingen en pensioenfondsen;
- de rechterlijke macht.

De uitwerking van de Wdo als kaderwet vindt plaats in de lagere regelgeving. Zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen. Zo is er ruimte voor innovatie, verdere keuzes en nieuwe voorzieningen en functionaliteiten.

Dit voorstel maakt het mogelijk om straks via publieke én private inlogmiddelen digitaal zaken te doen met bijvoorbeeld gemeenten en zorginstanties. Alleen middelen die door de overheid op veiligheid en betrouwbaarheid zijn gecontroleerd worden toegelaten. Die zijn dan in het publieke domein toegestaan. Hoewel inloggen bij diensten van commerciële/private partijen zoals webwinkels niet in deze wet wordt geregeld, kunnen burgers met de gecontroleerde private middelen ook daar inloggen. Zo heeft het wetsvoorstel toch een breder effect en voordeel voor veilig inloggen.

Voor de tweede tranche van de Wet digitale overheid (Wdo) komen de volgende onderwerpen in aanmerking komen voor wettelijke verankering. Dit zijn:

- Het kader voor het verantwoord delen van digitale persoonsgegevens met partijen binnen en buiten de overheid (regie op gegevens).
- Het beleggen van de verantwoordelijkheid voor het stelsel van basisregistraties en het bewaken van de werking daarvan, waaronder het correct (en verplicht) gebruik van authentieke gegevens in het stelsel.
- Hoe kunnen in de Wdo het burger- en bedrijvendomein verder naar elkaar toe groeien?

3 Leidende principes

In fase 1 van het programma Regie op Gegevens zijn aan de hand van de (beoogde) wetgeving en beleid meer in detail de principes waarlangs Regie op gegevens ingevuld dient te worden, nader uitgewerkt. In dit hoofdstuk worden deze principes toegelicht, waarna vanaf paragraaf 3.6 deze principes worden gerelateerd aan de (nieuwe) NORA-principes.

1- Burger centraal
1. Digitale zelfbeschikking 2. Gebruiksvriendelijkheid/ begrijpelijkheid 3. Vertegenwoordiging is mogelijk 4. Menselijke tussenkomst
2- Vertrouwen
1. Privacy-by-design & default 2. Security by design & default
3- Transparantie
1. Informatiepositie burger 2. Openheid 3. Toegankelijkheid
4- Interoperabiliteit
1. Dataportabiliteit
5- Balans in belangen
1. Geen druk op het (digitaal) delen van gegevens 2. Geen druk ten aanzien van het gebruik van digitale regietoepassing

3.1 Burger centraal

Organisaties begrijpen wat de burger raakt en dat merkt de burger in zijn contact met hen, ongeacht diversiteit in fysieke, cognitieve, psychosociale aspecten, of de omstandigheden waarin burgers zich bevinden. Regie op gegevens leidt tot vergroting van inzicht in – en invloed op – zijn eigen persoonlijk gegevensverkeer, en hierdoor verstevigt de burger zijn positie ten opzichte van aanbieders en afnemers van deze gegevens. Denk daarbij aan de toegenomen mogelijkheid voor de burger voor:

1. delen van gegevens: de eigen gegevens zelf, digitaal kunnen delen met dienstverleners buiten de overheid;
2. eenmalige verstrekking: kunnen weigeren om gegevens te verstrekken die binnen de overheid al beschikbaar zijn;
3. inzage en correctie: de eigen gegevens kunnen inzien en controleren, kunnen inzien welke gegevens worden en zijn uitgewisseld, en de gegevens kunnen (laten) corrigeren.

Voor regie op gegevens houdt dit een ontwikkeling in waarbij niet de organisatie leidend is, maar de leefwereld en behoeften van de burger, en waarbij de autonome burger zoveel mogelijk zelf regie voert op zijn eigen situatie.

3.1.1 Digitale zelfbeschikking

Burgers hebben digitale zelfbeschikkingsmacht. Tijdens alle fasen van dienstverlening (idee vorming, ontwerp, realisatie en exploitatie) is er participatie vanuit kwetsbare gebruikersgroepen en individuele burgers. Belangrijke uitgangspunt hier is dat wordt uitgegaan van feiten en niet van aannames.

3.1.2 Gebruiksvriendelijkheid/ begrijpelijkheid

Regie op de eigen gegevens is voor alle burgers. Kwetsbare en/of niet-digivaardige burgers hebben daarbij speciale aandacht. Dit betekent onder andere dat de informatie of communicatie beknopt, begrijpelijk en gemakkelijk toegankelijk zijn en er moet duidelijke en eenvoudige taal worden gebruikt. Hiernaast wordt deze groep, waar het nodig is, ondersteund.

3.1.3 Vertegenwoordiging

Specifiek als het gaat om kwetsbare en/of niet-digivaardige burgers heeft het kabinet in de brief "Digitale inclusie; iedereen moet kunnen meedoen" aangegeven hoe deze ondersteund moeten worden om mee te kunnen in de informatiesamenleving. De daarbij uiteengezette lijn is ook van toepassing op het voeren van regie op de eigen gegevens. Daarbij is de primaire inzet het digivaardig maken van wie dat nu niet is, onder meer door het aanbieden van cursussen. Wie ondanks alle ondersteuning niet digitaal kan, kan iemand machtigen om namens hem regie te voeren (zoals een zorgcoach of belastingconsulent). In overleg met de betreffende overheidsorganisatie kan ook een ander, analoog kanaal worden gezocht, zoals balie, telefoon of papieren post. Er is een ‘audit trail’ mogelijk op afgegeven en ingetrokken machtigingen en het bereik waarop deze van toepassing zijn.

3.1.4 Menselijke tussenkomst

Uitgangspunt van regie op gegevens is dat de leefwereld leidend is boven de systeemwereld. De met digitalisering gepaard gaande standaardisatie kan ertoe leiden dat fouten kunnen worden gemaakt, doordat in de systeemwereld vaak niet op voorhand rekening kan worden gehouden met alle relevante aspecten van de – vele malen complexere – leefwereld. Hierom is het van belang dat de betrokken bij de mogelijkheid heeft zich zo nodig tot een (menselijk) loket te wenden.

3.2 Vertrouwen

Afsprakenstelsels en regietoepassingen vergroten het vertrouwen van burgers, aanbieders en afnemers, in regie op gegevens. Het waarborgen van de privacy en veiligheid is een verantwoordelijkheid van alle betrokken partijen. Onder andere zijn privacy en security by design & default essentieel om vertrouwen in afsprakenstelsel en regietoepassingen te krijgen en te behouden. Deze thema’s worden onderstaand nader toegelicht. Het vertrouwen in gebruik wordt alleen vergroot worden indien het eenvoudig is om op een goede manier om te gaan met privacy en veiligheid ook geborgd is. Indien stelsels en regietoepassingen niet

gemakkelijk in gebruik zijn zullen ze minder toegepast worden en zal er minder vertrouwen in zijn.

3.2.1 Privacy-by-design & default

Privacy by design is een proactieve benadering van de bescherming van privacy door het borgen van privacy leidend te maken binnen afsprakenstelsels en regietoepassingen voor de verwerking van persoonsgegevens van de burger. De aandacht voor privacy blijft tijdens het gehele proces van gegevens-uitwisseling bestaan. Er is sprake van 'privacy by default' als de standaardinstellingen van de regietoepassing zodanig zijn dat maximale privacy wordt geborgd, zonder dat de regietoepassing in de knel komt.

3.2.2 Security by design & default

Bij beveiliging (security) gaat het erom dat waarborgen zijn getroffen ten behoeve van beschikbaarheid, integriteit, en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens. De noodzakelijk waarborgen hebben onder andere betrekking op:

- het beheer en de beveiliging van de regietoepassingen;
- de beveiliging van gegevens in transport en opslag;
- de behandeling van incidenten;
- het beheer van de continuïteit;
- het toezicht (monitoring), controle (auditing) en testen;
- de inachtneming van de internationale normen.
- de Identificatie, Authenticatie en Autorisatie (IAA).

Verder leidt het gebruik van authentieke bronnen tot verhoging van de gegevenskwaliteit en uniformiteit in dienstverlening en ondersteunende processen.

3.3 Transparantie

Burgers, aanbieders en afnemers en overige stakeholders zijn open en eerlijk over hun intenties en gedrag in regie op gegevens. Inzicht in wat organisaties met welke gegevens van burgers doen is belangrijk om transparantie te creëren en te behouden. Er moet zo weinig mogelijk verschil zijn in de informatiepositie die de verschillende partijen innemen. Technische en organisatorische aspecten van gegevensuitwisseling moeten controleerbaar en herleidbaar zijn.

3.3.1 Informatiepositie burger

De burger kan zijn gegevens inzien en is voor hem/haar herkenbaar wanneer, met wie en waarom zijn gegevens zijn opgevraagd of uitgewisseld. Een en ander gekoppeld aan de verleende toestemming of wettelijke regels.

3.3.2 Openheid

Openheid is voor veel zaken essentieel, denk bijvoorbeeld aan reguliere audits laten uitvoeren of kwaliteitsdashboards die iedereen kan raadplegen die de desbetreffende gegevens gebruikt. Ook openheid over geconstateerde datalekken, de genomen acties, etc.

3.3.3 Toegankelijkheid

Informatie over wet- en regelgeving en afspraken, beleid en andere informatie over het verwerken van gegevens is steeds op eenvoudige wijze raadpleegbaar.

3.4 Interoperabiliteit

Afsprakenstelsels en regietoepassingen borgen de koppelbaarheid tussen de diensten en gegevens van burgers, aanbieders en afnemers. Interoperabiliteit is de mogelijkheid van autonome, heterogene systemen (apparaten, afdelingen, organisaties) om met elkaar informatie uit te wisselen en samen te werken. Interoperabiliteit komt mede tot stand door afspraken op organisatorische als informatie-technische kant. In dergelijke afspraken kan worden vastgelegd welke standaard men zal gebruiken.

3.4.1 Dataportabiliteit

Het recht op overdraagbaarheid van persoonsgegevens (AVG) zorgt voor het vergroten van de controle van burger op zijn persoonsgegevens en voorkomt hiermee vendor lock-in.

3.5 Balans in belangen

Burgers, aanbieders en afnemers hebben een verschillende maar gelijkwaardige positie ten aanzien van besluitvorming over de dienstverlening. Naast rechten en plichten van aanbieders en afnemers moeten ook de voorwaarden voor de burger duidelijk worden gemaakt. Wat zorgplicht voor regie op gegevens anders maakt, is dat de betrokken burger zelf verantwoordelijk is voor de beslissing om gegevens te delen met derden. Echter, in de 'digitale sluis' variant heeft/houdt de overheid een verantwoordelijkheid/ zorgplicht. Er geldt dan ook een aanvullende zorgplicht om de belangen van de burgers te beschermen, gezien het hier gaat om bronregistraties van de overheid.

3.5.1 Geen druk op het (digitaal) delen van gegevens

Het delen van gegevens gebeurt alleen op basis van expliciete toestemming van de burger. Het delen van gegevens digitaal is op basis van vrijwilligheid. Gegevens digitaal (in plaats van op papier) te delen mag bij de afnemer geen rol spelen voor het wel of niet verkrijgen van een dienst door de burger.
De burger mag niet gedwongen worden gegevens aan te leveren voor een bepaald dienst die niet noodzakelijk zijn en/of vereist zijn vanuit regelgeving.

3.5.2 Geen druk ten aanzien van het gebruik van een (digitale) regietoepassing

De burger kan niet worden verplicht gebruik te maken van een bepaalde digitale regietoepassing, althans niet als het gaat om overheidsdienstverlening. De mogelijkheid om dienstverlening niet via digitale weg te hoeven regelen en ontvangen, moet voor iedere betrokkene blijven bestaan.

3.6 Koppeling met NORA principes

3.6.1 Aanpak

De Gebruikersraad van de NORA heeft recent (2021-2022) een herijking uitgevoerd op de architectuur-principes. Dit heeft geleid tot een aangepaste versie van de NORA-architectuurprincipes. Bij het uitwer-ken

van de relatie tussen de principes van Regie op Gegevens (2019) en de NORA-principes wordt aangesloten bij de meest recente versie van de NORA-principes. Hieronder wordt in het kort een toelichting gegeven op de NORA Kernwaarden, Kwaliteitsdoelen en Architectuurprincipes.

3.6.2 *Kernwaarden van dienstverlening*

NORA Kernwaarden zijn fundamentele overtuigingen, gebaseerd op maatschappelijke waarden, waar overheidsdienstverlening aan moet voldoen.

ID	Kernwaarde	Omschrijving
KWD01	Vertrouwen	De dienstverlening van de overheid maakt het vertrouwen dat burgers en bedrijven daar in stellen waar
KWD02	Veilig	Niemand hoeft bij dienstverlening van de overheid te vrezen voor gevaren en bedreigingen.
KWD03	Toekomstgericht	De dienstverlening van de overheid is op de toekomst voorbereid.
KWD04	Doeltreffend	De dienstverlening van de overheid bereikt de gestelde doelen en voldoet zo aan de verwachtingen van burgers en bedrijven.
KWD05	Doelmatig	De dienstverlening van de overheid is zo ingericht dat met een optimale balans tussen kosten, tijdigheid en kwaliteit het beoogde doel wordt bereikt.

3.6.3 *Kwaliteitsdoelen*

De NORA-kwaliteitsdoelen geven de gewenste kenmerken van overheidsdienstverlening vanuit het perspectief van de wensen van de samenleving, de burgers en bedrijven. Kwaliteitsdoelen beschrijven aan welke kwaliteitskenmerken overheidsdienstverlening moet voldoen, gemotiveerd vanuit de Kernwaarden van Dienstverlening. Ze doen geen uitspraken over de wijze waarop deze doelen moeten worden gerealiseerd (het hoe). Dat wordt uitgewerkt in de Architectuurprincipes en de onderliggende implicaties.
De NORA-kwaliteitsdoelen zijn:

ID	Kwaliteitsdoel
KD01	Transparant
KD02	Betrouwbaar
KD03	Ontvankelijk
KD04	Verantwoord
KD05	Privacy
KD06	Beschikbaar
KD07	Integer
KD08	Vertrouwelijk
KD09	Wendbaar

KD10	Innovatief
KD11	Duurzaam
KD12	Proactief
KD13	Gebundeld
KD14	Toegankelijk
KD15	Begrijpelijk
KD16	Overzichtelijk
KD17	Vindbaar
KD18	Uniform
KD19	Noodzakelijk
KD20	Kostenefficiënt

3.6.4 *Architectuurprincipes*

NORA Architectuurprincipes zijn normatieve uitspraken die richting geven aan het in samenhang ontwerpen en realiseren van overheidsdiensten voor burgers en bedrijven. Elk Architectuurprincipe draagt bij aan het realiseren van een of meer van de Kwaliteitsdoelen die zijn afgeleid van de Kernwaarden van Dienstverlening. NORA Architectuurprincipes zijn bedoeld voor architecten die werken in het informatiedomein binnen de overheid.

De NORA Architectuurprincipes zijn:

ID	**Architectuurprincipe**
NAP01	Verplaats je in de gebruiker
NAP02	Geef inzicht in de afhandeling van de dienst
NAP03	Lever een kanaal-onafhankelijk resultaat
NAP04	Bundel diensten
NAP05	Bied de dienst proactief aan
NAP06	Hergebruik vóór kopen vóór maken
NAP07	Bouw diensten modulair op
NAP08	Standaardiseer waar mogelijk
NAP09	Beschrijf de dienst nauwkeurig
NAP10	Neem gegevens als fundament
NAP11	Pas doelbinding toe
NAP12	Informeer bij de bron
NAP13	Beheers risico's voortdurend
NAP14	Verifieer altijd
NAP15	Maak diensten schaalbaar
NAP16	Voorkom onnodige complexiteit
NAP17	Stuur cyclisch op kwaliteit

3.6.5 *Relatie tussen Kernwaarde, kwaliteitsdoel en architectuurprincipe*

Kwaliteitsdoelen beschrijven aan welke kwaliteitskenmerken overheidsdienstverlening moet voldoen, gemotiveerd vanuit de Kernwaarden van Dienstverlening. In deze tabel is de relatie tussen Kernwaarde, kwaliteitsdoel en architectuurprincipe uitgewerkt.

Dezelfde tabel, alleen dan omgedraaid (welke architectuurprincipes dragen bij aan welk kwaliteitsdoel) vormt de basis voor de uitwerking van de relatie tussen de principes van Regie op Gegevens en de NORA-principes. Elk Architectuurprincipe draagt dus bij aan het realiseren van een of meer van de Kwaliteitsdoelen die zijn afgeleid van de Kernwaarden van Dienstverlening:

ID	Architectuurprincipe	Bij Kwaliteitsdoel(en)
NAP01	Verplaats je in de gebruiker	Ontvankelijk (Doel), Transparant (Doel), Verantwoord (Doel), Begrijpelijk (Doel), Toegankelijk (Doel), Overzichtelijk (Doel), Uniform (Doel)
NAP02	Geef inzicht in de afhandeling van de dienst	Transparant (Doel), Verantwoord (Doel), Privacy (Doel), Begrijpelijk (Doel), Overzichtelijk (Doel)
NAP03	Lever een kanaal-onafhankelijk resultaat	Ontvankelijk (Doel), Betrouwbaar (Doel), Toegankelijk (Doel), Uniform (Doel)
NAP04	Bundel diensten	Gebundeld (Doel), Toegankelijk (Doel), Overzichtelijk (Doel)
NAP05	Bied de dienst proactief aan	Ontvankelijk (Doel), Proactief (Doel)
NAP06	Hergebruik vóór kopen vóór maken	Duurzaam (Doel), Innovatief (Doel), Uniform (Doel), Kostenefficiënt (Doel)
NAP07	Bouw diensten modulair op	Duurzaam (Doel), Wendbaar (Doel), Innovatief (Doel), Noodzakelijk (Doel)
NAP08	Standaardiseer waar mogelijk	Wendbaar (Doel), Uniform (Doel), Kostenefficiënt (Doel)
NAP09	Beschrijf de dienst nauwkeurig	Vindbaar (Doel), Transparant (Doel), Verantwoord (Doel), Begrijpelijk (Doel)

NAP10	Neem gegevens als fundament	Vindbaar (Doel), Beschikbaar (Doel), Betrouwbaar (Doel), Begrijpelijk (Doel), Gebundeld (Doel), Integer (Doel), Toegankelijk (Doel), Overzichtelijk (Doel), Uniform (Doel), Kostenefficiënt (Doel)
NAP11	Pas doelbinding toe	Vertrouwelijk (Doel), Verantwoord (Doel), Privacy (Doel), Betrouwbaar (Doel)
NAP12	Informeer bij de bron	Wendbaar (Doel), Uniform (Doel), Noodzakelijk (Doel)
NAP13	Beheers risico's voortdurend	Beschikbaar (Doel), Vertrouwelijk (Doel), Integer (Doel), Kostenefficiënt (Doel)
NAP14	Verifieer altijd	Beschikbaar (Doel), Vertrouwelijk (Doel), Verantwoord (Doel), Integer (Doel)
NAP15	Maak diensten schaalbaar	Beschikbaar (Doel), Betrouwbaar (Doel), Wendbaar (Doel), Innovatief (Doel)
NAP16	Voorkom onnodige complexiteit	Begrijpelijk (Doel), Wendbaar (Doel), Innovatief (Doel), Kostenefficiënt (Doel)
NAP17	Stuur cyclisch op kwaliteit	Ontvankelijk (Doel), Verantwoord (Doel), Begrijpelijk (Doel), Wendbaar (Doel), Uniform (Doel), Kostenefficiënt (Doel)

3.7 Analyse relatie principes NORA en RoG

3.7.1 RoG-principes gerelateerd aan NORA-principes

In de tabel van paragraaf 1.5 is de relatie tussen de 17 NORA-architectuurprincipes en de kwaliteitsdoelen weergegeven. In onderstaande paragrafen zijn de principes van Regie op Gegevens (groen) gerelateerd aan de NORA-principes (blauw).

3.7.2 Verplaats je in de gebruiker

NAP01	**Verplaats je in de gebruiker**
Stelling	Ontwerp, realiseer en verbeter de dienst vanuit het perspectief van de afnemer
Rationale	Om een kwalitatief goede dienst met ondersteunende systemen te leveren is het nodig om niet alleen het perspectief van de overheidsdienstverlener, maar óók het perspectief, de beweegredenen, verwachtingen en context van de afnemer mee te nemen.
Relatie met principes RoG	– Digitale zelfbeschikking – Gebruiksvriendelijkheid/ begrijpelijkheid – Vertegenwoordiging – Menselijke tussenkomst – Privacy-by-design & default – Security by design & default – Informatiepositie burger – Openheid – Toegankelijkheid – Dataportabiliteit – Geen druk op het (digitaal) delen van gegevens – Geen druk t.a.v. het gebruik van een (digitale) regietoepassing
Toelichting	Het startpunt in de visieontwikkeling op Regie op Gegevens is het perspectief van de burger geweest. Om vast te stellen welke beweegredenen, verwachtingen en context die burger heeft als het gaat om regie op zijn persoonsgegevens, is uitvoerig onderzoek gedaan via burgerpanels, interviews enz. Die behoeften en verwachtingen zijn vertaald in fase 1 van het programma naar de set van principes RoG (als onderdeel van het ontwerp) zoals boven weergegeven. Deze principes dragen allemaal bij invulling van "verplaats je in de gebruiker".

3.7.3 Geef inzicht in de afhandeling van de dienst

NAP02	**Geef inzicht in de afhandeling van de dienst**
Stelling	Informeer de afnemer over de dienst, zowel procesmatig als inhoudelijk.
Rationale	Afnemers willen graag inzicht hebben in de voortgang en (deel)beslissingen van de dienstverlening. Dit is onder andere van belang wanneer de afnemer het resultaat nodig heeft voor vervolgactiviteiten. De overheidsdienstverlener neemt onzekerheid weg door deze transparantie te bieden: is mijn verzoek überhaupt aangekomen, krijg ik de uitslag op tijd?

	Verder geeft het inzagerecht invulling aan het streven naar een betrouwbare en transparante overheid. Door deze informatie duurzaam toegankelijk te houden wordt de traceerbaarheid van beslissingen gegarandeerd.".
Relatie met principes RoG	– Gebruiksvriendelijkheid/ begrijpelijkheid – Informatiepositie burger – Openheid – Toegankelijkheid
Toelichting	Bovenstaande principes geven invulling aan "Geef inzicht in de afhandeling van de dienst"

3.7.4 Lever een kanaal-onafhankelijk resultaat

NAP03	**Lever een kanaal-onafhankelijk resultaat**
Stelling	Lever een gelijkwaardige uitkomst, ongeacht het gebruikte kanaal. Bied de dienst aan via internet, fysiek (off-line) en eventueel via andere passende kanalen waar de afnemer gebruik van kan maken.
Rationale	Afnemers verwachten een gelijkwaardig resultaat, dat niet beïnvloed wordt door hun kanaalkeuze. Het mag dus voor het resultaat van de dienst geen verschil uitmaken of deze bijvoorbeeld via internet of fysiek is aangevraagd. De geleverde informatie is in alle gevallen hetzelfde, ongeacht de plaats of medewerker die deze informatie levert.
Relatie met principes RoG	– Geen druk t.a.v. het gebruik van een (digitale) regietoepassing
Toelichting	Een principe binnen RoG is dat de burger de diensten inzage, correctie en delen kunnen afnemen zonder gedwongen te worden in de keuze van het kanaal. Het resultaat zou gelijkwaardig moeten zijn.

3.7.5 Bundel diensten

NAP04	**Bundel diensten**
Stelling	Bundel de dienst met andere voor de afnemer relevante diensten binnen de keten, zodat die in één keer afgenomen kunnen worden.
Rationale	Door bundeling van diensten nemen gebruiksgemak en meerwaarde voor afnemers toe: waar voorheen meerdere aanvragen nodig waren, kan nu met één aanvraag worden volstaan. Tevens kunnen overheidsdienstverleners zo efficiënter samenwerken.
Relatie met principes RoG	– Informatiepositie burger
Toelichting	Door burgers middels een overzicht van persoonsgegevens, uit verschillende bronnen samengevoegd in één lijst, inzicht te geven in de persoonsgegevens die de overheid als geheel van hem heeft (dus niet per overheidsbron apart), wordt de burger in staat gesteld om in één keer de gevraagde gegevens in te zien, te corrigeren en te delen.

3.7.6 *Bied de dienst proactief aan*

NAP05	**Bied de dienst proactief aan**
Stelling	Bied de dienst aan wanneer dit in het belang is of zou kunnen zijn voor de afnemer.
Rationale	Het gebruik en gemak van diensten neemt toe wanneer overheidsdienstverleners acteren op signalen die duiden op (latente) behoeften bij de afnemer. Op basis hiervan nemen zij het initiatief om (aanvullende) diensten aan te bieden of er naar door te wijzen. Afnemers hoeven daardoor niet eerst zelf de vraag te stellen, of te weten welke diensten beschikbaar zijn. Proactiviteit is een belangrijk aspect van de kwaliteit van dienstverlening die de overheid nastreeft.
Relatie met principes RoG	– Gebruiksvriendelijkheid/ begrijpelijkheid – Vertegenwoordiging – Menselijke tussenkomst – Privacy-by-design & default – Security by design & default – Informatiepositie burger – Openheid – Toegankelijkheid – Dataportabiliteit – Geen druk op het (digitaal) delen van gegevens – Geen druk t.a.v. het gebruik van een (digitale) regietoepassing
Toelichting	Vanuit de samenleving worden al geruime tijd signalen afgegeven om het geven van inzicht, corrigeren en delen van persoonsgegevens van burgers in overheidsbronnen te vergemakkelijken. RoG heeft tot doel dit mogelijk te maken. Voor burgers betekent dit dat zij op hun eigen initiatief gebruik kunnen maken van diensten die deze wens ondersteunen. Hiervoor worden digitale middelen op een begrijpelijke en toegankelijke wijze ter beschikking gesteld, inzicht gegeven in de informatiepositie van de burger, gegevenscatalogi ontwikkeld waaruit burgers kunnen kiezen, burger ondersteund bij dataminimalisatie enz.

3.7.7 *Hergebruik vóór kopen vóór maken*

NAP06	**Hergebruik vóór kopen vóór maken**
Stelling	Ga uit van overheidsbreed hergebruik van diensten, of onderdelen daarvan voordat je overgaat tot het kopen of het laten maken.
Rationale	Hergebruik van diensten of onderdelen daarvan is duurzaam en kostenefficiënt, en bovendien leidt dit tot standaardisering van dienstverlening en informatievoorzieningen. Als hergebruik niet mogelijk is, ga dan na of aanpassing op het bestaande mogelijk is. Pas daarna komt het alternatief om iets te kopen of desnoods te (laten) maken in zicht.

Relatie met principes RoG	–
Toelichting	De generieke bouwblokken uit de GDI vormen de basis onder de dienstverlening vanuit de overheid. De Wet GDI (de basis voor de GDI) wordt vervangen door de Wet Digitale Overheid. Oplossingen vanuit RoG sluiten aan op deze nieuwe wet en bouwblokken door zoveel als mogelijk gebruik te maken van bestaande oplossingen en standaarden. Daar waar aanpassingen noodzakelijk zijn, zal zoveel mogelijk aangesloten worden bij Europese ontwikkelingen. Binnen die context worden generieke oplossingen gerealiseerd die door lidstaten gebruikt kunnen gaan worden. Om hier verder invulling aan te geven zal het functiemodel van RoG aansluiten bij de vier domeinen van de GDI: 1. **Domein: Toegang** Oplossingen om burgers en ondernemers toegang te geven tot digitale diensten, ook als zij een ander vertegenwoordigen. 2. **Domein: Interactie** Oplossingen voor digitale informatie-uitwisseling met burgers en ondernemers. 3. **Domein: Gegevensuitwisseling** Oplossingen voor uitwisseling van gegevens via de GDI tussen informatiesystemen van overheidsorganisaties onderling en met informatiesystemen van andere organisaties. 4. **Domein: Infrastructuur** Oplossingen van algemeen belang voor de GDI die vaak een basis vormen voor oplossingen in de andere drie domeinen.

3.7.8 Bouw diensten modulair op

NAP07	**Bouw diensten modulair op**
Stelling	Maak bij de ontwikkeling van diensten gebruik van een modulaire indeling met een maximale interne samenhang en minimale externe koppelingen.
Rationale	Door diensten modulair op te bouwen en te ontkoppelen wordt de flexibiliteit vergroot, wat leidt tot meer wendbaarheid, meer hergebruik en duurzaamheid.
Relatie met principes RoG	–
Toelichting	Dit inrichtingsprincipe wordt binnen de architectuur van RoG ingevuld door (conform het functiemodel) onderscheid te maken tussen de domeinen van de GDI (toegang, interactie, gegevensuitwisseling en infrastructuur) aangevuld met gegevensdiensten t.b.v. dataminimalisatie en vertrouwensdiensten, zoals definieert in de eIDAS-verordening. Met name de gegevens- en vertrouwensdiensten zullen modulair beschikbaar gesteld moeten worden om optimaal te

	kunnen voldoen aan specifieke klantwensen t.a.v. die diensten.

3.7.9 Standaardiseer waar mogelijk

NAP08	**Standaardiseer waar mogelijk**
Stelling	Standaardiseer waar het kan, maak specifiek waar het moet.
Rationale	Standaardisatie reduceert variëteit en kosten, en zorgt voor een betere interoperabiliteit en beveiliging. Hiermee komt bovendien een grotere wendbaarheid tot stand. Door te kiezen voor open standaarden wordt vendor lock-in voorkomen.
Relatie met principes RoG	– Dataportabiliteit –
Toelichting	Interoperabiliteit wordt o.a. gerealiseerd door standaardisatie, waardoor dataportabiliteit ook mogelijk gemaakt wordt.

3.7.10 Beschrijf de dienst nauwkeurig

NAP09	**Beschrijf de dienst nauwkeurig**
Stelling	Beschrijf de dienst nauwkeurig en positioneer deze helder binnen het dienstenaanbod.
Rationale	Een heldere beschrijving van het wat, het doel en wettelijk kader inclusief interactiemomenten en positionering draagt bij aan het gebruik van de dienst. Het maakt diensten gemakkelijker vindbaar voor afnemers. Het draagt bij aan het begrip bij afnemers van wat de dienst wel en niet te bieden heeft, ten opzichte van andere verwante diensten.
Relatie met principes RoG	– Digitale zelfbeschikking – Gebruiksvriendelijkheid/ begrijpelijkheid – Vertegenwoordiging – Openheid – Toegankelijkheid – Dataportabiliteit
Toelichting	Bovenstaande principes geven invulling aan de eisen die aan de regiedienst gesteld worden. Dit zal concrete invulling krijgen in het Vertrouwensraamwerk, waar per dienst afspraken gemaakt worden over het wat, het doel en wettelijk kader inclusief interactiemomenten en positionering.

3.7.11 Neem gegevens als fundament

NAP10	**Neem gegevens als fundament**
Stelling	Gebruik gegevens als fundament voor het ontwerp, realisatie en doorontwikkeling van de dienst en richt het beheer hiervan goed in.
Rationale	De kwaliteit en toegankelijkheid van gegevens bepaalt de waarde van de dienst. De onderliggende gegevens kennen meestal een veel langere levenscyclus dan de systemen waarin deze verwerkt wordt. Als gegevens op duurzame wijze

	toegankelijk zijn gemaakt voor mens én machine kunnen deze gegevens dienen als fundering voor verschillende diensten in verschillende toepassingen, door de tijd en over de hele keten heen. Daarom is het essentieel dat het beheer van gegevens in de keten op orde is, vanaf het ontstaan ervan tot en met de vernietiging (conform bewaartermijnen).
Relatie met principes RoG	– Digitale zelfbeschikking – Gebruiksvriendelijkheid/ begrijpelijkheid – Vertegenwoordiging – Menselijke tussenkomst – Privacy-by-design & default – Security by design & default – Informatiepositie burger – Openheid – Toegankelijkheid – Dataportabiliteit – Geen druk op het (digitaal) delen van gegevens – Geen druk t.a.v. het gebruik van een (digitale) regietoepassing
Toelichting	De principes van RoG hebben als uitgangspunt gegevens.

3.7.12 Pas doelbinding toe

NAP11	**Pas doelbinding toe**
Stelling	Geef burgers en bedrijven de zekerheid dat informatie over hen alleen wordt gebruikt voor de doelen waarvoor deze oorspronkelijk is verzameld.
Rationale	Afspraken over het gebruik van informatie zijn nodig voor een vertrouwen in de dienstverlening. Door informatie niet te gebruiken voor andere processen of diensten binnen de overheid, wordt zekerheid naar burgers en bedrijven geboden.
Relatie met principes RoG	–
Toelichting	De grondslag voor het delen van persoonsgegevens vanuit overheidsbronnen met burgers is de tweede tranche van de WDO. Doelbinding zoals geformuleerd in de NORA heeft betrekking op de overheid intern.

3.7.13 Informeer bij de bron

NAP12	**Informeer bij de bron**
Stelling	Maak bij de dienst gebruik van gegevens die afkomstig zijn uit een bronregistratie.
Rationale	Voor betrouwbare dienstverlening is het hergebruik van de juiste informatie en documenten van cruciaal belang. Om de kwaliteit over de juistheid van een gegeven te borgen, moet duidelijk zijn welke organisatie bepaalt wat de juiste informatie is. Uitgangspunt is dat er voor gegevens waar de overheid gebruik van maakt, altijd één bron bestaat, die leidend is.

Relatie met principes RoG	–
Toelichting	Doelstelling van RoG is inzage, correctierecht en delen van persoonsgegevens. Hierin wordt in beginsel geen onderscheid gemaakt tussen bronregistraties (daar waar eigenaarschap van het gegeven bestaat) en bronnen die doorgeleverde gegevens bevatten. Beide bronnen zijn voor burgers van belang. Ook heeft de burger nu al (conform bestaande regels) het recht om een melding te doen bij een bron met het verzoek om correctie zonder dat hij zich af hoeft te vragen of dit een bronregistratie of een andere registratie is. Voor wat betreft het delen van gegevens is het streven dat de systeemwereld van de overheid zich zo inricht dat een persoonsgegeven uit een bronregistratie gehaald wordt. Dit zou voor een burger volledig indifferent moeten zijn.

3.7.14 Beheers risico's voortdurend

NAP13	**Beheers risico's voortdurend**
Stelling	Maak in alle stappen van ontwerp en doorontwikkeling van de dienst de risico's inzichtelijk en stuur op een afgewogen beheersing ervan.
Rationale	Wanneer helder in beeld is welke gevaren en bedreigingen van toepassing zijn voor de dienst, kun je gepaste beheersmaatregelen nemen. De manieren waarop componenten kunnen falen of hoe er misbruik van kan worden gemaakt zijn onderdeel van de risicoanalyse. Telkens kan dan de afweging worden gemaakt in welke mate de kosten en inspanningen van verdere mitigatie in verhouding staan tot de gevolgen als een risico zich voordoet. De bereidheid van de overheidsdienstverlener om restrisico's te accepteren maakt onderdeel uit van de afweging. Door risico's tijdig te onderkennen zijn beheersmaatregelen effectiever en efficiënter te implementeren.
Relatie met principes RoG	– Digitale zelfbeschikking – Gebruiksvriendelijkheid/ begrijpelijkheid – Vertegenwoordiging – Menselijke tussenkomst – Privacy-by-design & default – Security by design & default – Informatiepositie burger – Openheid – Toegankelijkheid – Dataportabiliteit – Geen druk op het (digitaal) delen van gegevens – Geen druk t.a.v. het gebruik van een (digitale) regietoepassing
Toelichting	De risicogedreven benadering uit dit principe vormt de basis voor de RoG: het delen van persoonsgegevens uit

	overheidsbronnen met burgers brengt voor die burger, naast een aantal voordelen, ook risico's met zich mee welke zoveel als mogelijk beheerst dienen te worden. Maatregelen worden genomen in de wet, architectuur en vertrouwensraamwerk.

3.7.15 Verifieer altijd

NAP14	**Verifieer altijd**
Stelling	Verifieer doorlopend de juiste werking van de componenten en beheersmaatregelen van de dienst.
Rationale	Vertrouwen in het service-niveau van een overheidsdienstverlener, in de beschikbaarheid van een dienst, in de betrouwbaarheid van informatie, in de werking van een component, of de adequaatheid van beheersmaatregelen, is alleen gerechtvaardigd als de componenten en beheersmaatregelen van de dienst doorlopend wordt geverifieerd.
Relatie met principes RoG	– Digitale zelfbeschikking – Gebruiksvriendelijkheid/ begrijpelijkheid – Vertegenwoordiging – Menselijke tussenkomst – Privacy-by-design & default – Security by design & default – Informatiepositie burger – Openheid – Toegankelijkheid – Dataportabiliteit – Geen druk op het (digitaal) delen van gegevens – Geen druk t.a.v. het gebruik van een (digitale) regietoepassing
Toelichting	Binnen het Vertrouwensraamwerk zal invulling gegeven worden aan afspraken rond het serviceniveau van de dienst. Onderdeel van afspraken over het serviceniveau zijn afspraken over de mate waarin aan de principes van RoG invulling gegeven is.

3.7.16 Maak diensten schaalbaar

NAP15	**Maak diensten schaalbaar**
Stelling	Bereid de dienst voor op veranderende werklast of reikwijdte.
Rationale	Een schaalbare dienst kan omgaan met zowel verwachte als onverwachte intensivering of extensivering. Dit waarborgt de beschikbaarheid van de dienst en hiermee ook de wendbaarheid. Het voorkomt het ad hoc en onder hoge tijdsdruk realiseren van het opschalen van de dienst.
Relatie met principes RoG	– Dataportabiliteit – Geen druk op het (digitaal) delen van gegevens – Geen druk t.a.v. het gebruik van een (digitale) regietoepassing

Toelichting	Afspraken over de beschikbaarheid van de dienst inzage, correctie en delen worden gemaakt in het Vertrouwensraamwerk. Punt van aandacht is het monitoren van het gebruik en de mogelijkheid tot opschalen, omdat het hier om een nieuwe dienst gaat en nog niet duidelijk is hoe de burger de dienst in de praktijk daadwerkelijk zal gaan gebruiken.

3.7.17 Voorkom onnodige complexiteit

NAP16	**Voorkom onnodige complexiteit**
Stelling	Voorkom onnodige complexiteit door activiteiten en middelen die geen waarde toevoegen, weg te laten.
Rationale	Meer complexiteit verhoogt de kosten, verhult kwetsbaarheden en reduceert het overzicht en belemmert veranderingen.
Relatie met principes RoG	– Privacy-by-design & default – Security by design & default –
Toelichting	Het risico op onnodige complexiteit zal zich naar alle waarschijnlijkheid vooral voordoen bij het formuleren van de eisen (kwaliteit/omvang enz.) waaraan de gevraagde gegevensset moet voldoen door de dienstverlener. Zo kan de dienstverlener de burger overvragen, maar ook beveiligingseisen aan gegevenssets stellen die verder gaan dan het doel waarvoor deze gevraagd worden. In het Vertrouwensraamwerk worden afspraken gemaakt over gegevensset en de kwaliteitseisen, waarbij ook financiële instrumenten helpen bij de beantwoording van vragen over nut en noodzaak.

3.7.18 Stuur cyclisch op kwaliteit

NAP17	**Stuur cyclisch op kwaliteit**
Stelling	Maak cyclische sturing op de kwaliteit van de dienst mogelijk.
Rationale	Afnemers vragen overheidsorganisaties om transparantie ten aanzien van de geleverde kwaliteit van de dienst en de sturing daarop. De overheidsdienstverlener legt over deze sturing verantwoording af en geeft aan of zij 'in control' is. Voor alle diensten gelden leveringsvoorwaarden en kwaliteitscriteria (Quality of Service). Afspraken hierover zorgen ervoor dat overheidsdienstverlener en afnemer weten waar zij aan toe zijn en elkaar kunnen vertrouwen. Voor afnemers is het van belang om snel inzicht te kunnen krijgen in een pakket van maatregelen voor de borging van de kwaliteit. Dit is ook in het kader van samenwerking tussen organisaties van belang. Op basis van inzicht in deze maatregelen ontstaat vertrouwen en het vermogen om snel samenwerking te realiseren.

	De overheidsdienstverlener werkt daarom op methodische wijze aan de kwaliteit van de dienst. Dit veronderstelt een cyclische terugkoppeling of Plan-Do-Check-Act-cyclus (Deming-cirkel) op de kwaliteit van de dienst.
Relatie met principes RoG	–
Toelichting	In het Vertrouwensraamwerk worden afspraken gemaakt over het sturen op kwaliteit.

4 Functiemodel Regie op Gegevens

In dit hoofdstuk worden de bedrijfsfuncties die nodig zijn om regie op gegevens door burgers mogelijk te maken gegroepeerd in functionele domeinen en een functiemodel. Dit model beschrijft dus de "wat-vraag" (wat is nodig om…?) en niet de "hoe-vraag" (welke techniek is hiervoor nodig?).

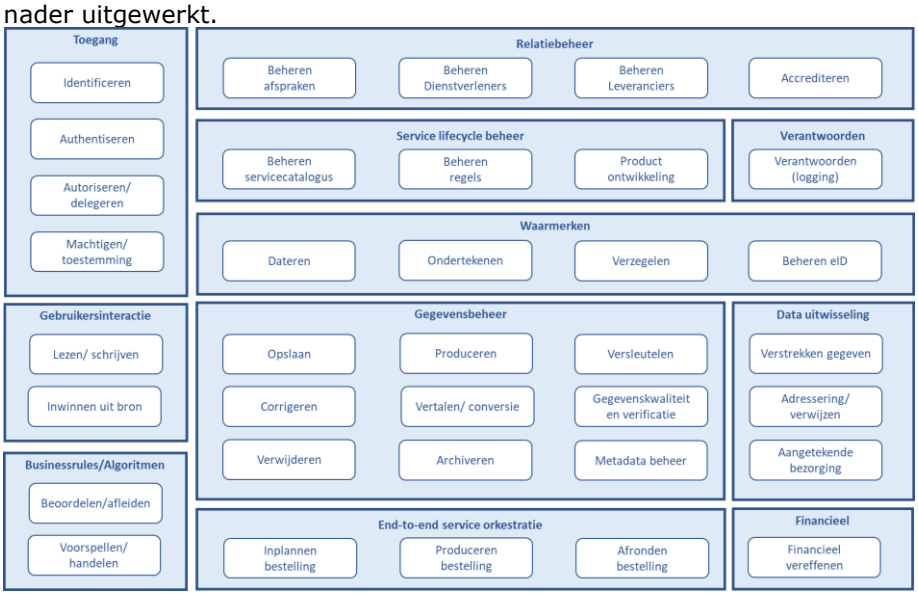
4.1 Functionele domeinen

De volgende functionele domeinen worden onderkend:

1. Toegang
2. Gebruikersinteractie
3. Businessrules/algoritmen
4. Gegevensbeheer
5. Waarmerken
6. Data-uitwisseling
7. Relatiebeheer
8. Service Lifecycle beheer
9. End-to-end Service orkestratie
10. Verantwoorden
11. Financieel

4.2 Functiemodel Regie op Gegevens

In het Business Functiemodel RoG worden per functiedomein de functies nader uitgewerkt.



Toegang	
Identificeren	Vaststellen wie een gebruiker, een andere computer of applicatie is.
Authentiseren	Authentiseren is de activiteit waarbij nagegaan wordt of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs.
Autoriseren/ delegeren	De vrager is bevoegd indien de bestelling overeen komt met de gemaakte afspraken (door wie, over wie, welk gegeven, waarom en wanneer). Controleren op vereiste toestemming maakt hier onderdeel van uit. Indien een persoon handelingsonbekwaam is omdat deze minderjarig, onder bewindvoering of curatele staat, treedt een vertegenwoordiger (ouder, voogd, bewindvoerder, curator) op in zijn naam. Deze vertegenwoordiger treedt in de plaats van de persoon.
Machtigen/ toestemming	Machtigen (*het verlenen van een volmacht*) heeft hier betrekking op het verlenen van toestemming aan een dienstverlener om in het kader van een offerte nader gespecificeerde gegevens die zich in de administratie van de overheid bevinden op te halen en rechtstreeks aan die dienstverlener te verstrekken. Onderdeel van machtigen is ook het beheren van de machtigingen (dus overzicht geven, verlenen, wijzigen en intrekken). Een tweede verschijningsvorm van volmacht verlening is de vertegenwoordiger (zoals schuldhulpverlener, echtscheidingsconsulent e.d.) die in opdracht van de vertegenwoordigde burger namens deze burger optreedt. De derde verschijningsvorm van volmacht verlening is de toestemming als grondslag uit de AVG tot het verwerken van persoonsgegevens.

Gebruikersinteractie	
Lezen/ schrijven	Het inzien van zijn gegevens in de administratie van een overheidsorganisatie om kennis te nemen van de inhoud. Schrijven heeft betrekking op de mogelijkheid om gegevens (bijv. een correctie) door te geven aan de bron of om een gegeven naar de eigen eWallet weg te schrijven.
Inwinnen uit de bron	Een gegeven wordt vanuit de omgeving van de bron in de eigen omgeving gebracht met als doel deze direct te gebruiken of op te slaan voor later gebruik.

Businessrules/ algoritmen	
Beoordelen/ afleiden	Aan de hand van vooraf opgestelde regels en een set gegevens wordt een conclusie getrokken.
Voorspellen/ handelen	Aan de hand van de analyse een gegevensset worden conclusies afgeleid, al dan niet gevolgd door handelen.

Beheren gegevens	
Opslaan	Gegevens die ingewonnen zijn kunnen voor later gebruik opgeslagen worden.
Corrigeren	Wanneer de burger kennis heeft van de onjuistheid van een gegeven in de administratie van de overheid, dan kan hij een verzoek tot correctie indienen. De overheid zal dit gegeven in onderzoek nemen en indien nodig aanpassen.
Verwijderen	Wanneer een gegeven niet meer geldig is, dan kan dit gegeven verwijderd worden. Verwijderen kan betekenen vernietigen maar ook een gegeven van een einddatum voorzien zodat op een later tijdstip de historie te achterhalen is. Archiveren wordt als een aparte functie onderkend.
Produceren	Gegevens worden binnen deze activiteiten gereed gemaakt voor verzending. Dit kan gebeuren tijdens het inwinnen maar ook tijdens de opslag of bij levering. Afhankelijk van het gegeven en de manier waarop deze vanuit de administratie beschikbaar is, bestaat het klaar maken voor levering uit het *verzamelen* van de benodigde gegevens, indien nodig *filteren* van de verzameling en *samenstellen* indien gegevens uit verschillende bronnen in één levering bijeengebracht moeten worden. Een mogelijke bewerking kan ook integreren/aggregeren zijn: gegevens in onderlinge samenhang gebracht op een zodanige manier dat deze verwerkt kunnen worden door de gebruiker. Waar de Verzamelen meer doelt op de logistiek van gegevens, doelt Integreren meer op de inhoud en onderlinge samenhang van gegevens (bijv. in tijd). Een andere mogelijke bewerking kan zijn het afleiden van conclusies: indien nodig worden op basis van regels conclusies getrokken en nieuwe gegevens (de conclusie) gegenereerd. Afleiden speelt een belangrijke rol binnen dataminimalisatie in het kader van privacybescherming.
Vertalen/ conversie	Indien gewenst kunnen gegevens vanuit het Nederlands vertaald worden naar andere talen en vice versa. Een andere vorm van bewerking is conversie van bijv. het ene bestands- of gegevensformaat naar een ander.

Archiveren	Indien gewenst kunnen gegevens opgeslagen worden voor later gebruik. Deze functie onderscheidt zich van de functie Opslaan Gegevens door het doel van de opslag: beschikbaar voor gebruik in het primaire proces versus beschikbaar voor verantwoording/reconstructie/onderzoek enz. achteraf.
Versleutelen	Als onderdeel van een bredere beveiligingsstrategie kunnen gegevens op verschillende momenten in het proces versleuteld worden. Breder geformuleerd kan deze functie *Beveiligen* genoemd worden, waarbij versleutelen een van de opties is.
Gegevenskwaliteit en verificatie	Waarborgen van de gegevenskwaliteit is een belangrijke voorwaarde voor ongestoord gebruik van die gegevens. Een van de manieren is validatie (met name op het aspect Juistheid). In de eIDAS-verordening 2021 is de verificatie van een aantal attributen aan de hand van authentieke bronnen expliciet opgenomen (art. 45 quinquies).
Metadata beheer	Gegevens worden gebruikt *in de context* van het proces waarvoor ze gebruikt worden. Om gegevens in een andere context te kunnen gebruiken, is het beheer van de metadata over die gegevens een belangrijke voorwaarde.

Waarmerken (vertrouwen)	
Elektronisch dateren	Een gegeven of set van gegevens wordt hiermee voorzien van een datum zodat vastgelegd is wat de datum van creëren/levering is. Komt overeen met *elektronische tijdstempel* uit eIDAS (amendement artikel 3 punt 16).
Elektronisch ondertekenen	Een gegeven of set van gegevens wordt hiermee voorzien van een elektronische verklaring van de afzender dat deze ook daadwerkelijk de afzender is. Komt overeen met *elektronische ondertekening* uit eIDAS.
Elektronisch verzegelen	Een gegeven of set van gegevens wordt hiermee voorzien van een elektronisch waarborg dat de set overeenkomt met de inhoud van de bron/verklaring van de afzender nadat deze door de afzender verzonden is (integriteit van de inhoud en afzender). Komt overeen met *elektronisch zegel* uit eIDAS.
Beheren eID	Een gegeven of een set van gegevens wordt hiermee voorzien van bewijs van de identiteit van de betrokkene. Komt overeen met *elektronische identiteitsbewijs* uit eIDAS.

Data uitwisseling	
Verstrekken gegeven	De gevraagde gegevens worden door de bron (i.c. overheid) conform afspraak aan de afnemer (burger of dienstverlener) verstrekt.
Adressering/ verwijzen	Een vorm van leveren van een gegeven kan ook zijn het verwijzen naar een bron waar het gewenste gegeven verkregen.
Aangetekend verzenden	Een bericht ("elektronisch pakketje") wordt met extra waarborgen verzonden (vooral: bewijs van ontvangst). Komt overeen met *elektronisch* aangetekende verzending uit eIDAS.

Relatiebeheer	
Beheren afspraken	Leveringen van gegevens van bron (i.c. overheid) naar dienstverlener geschiedt enkel op basis van afspraak. Deze afspraken moeten gemaakt, aangepast en beëindigd kunnen worden.
Beheren dienstverleners	Om een goede samenwerking te borgen, is het voor de leverancier noodzakelijk te weten wie zijn afnemers zijn en wat daar speelt (dus zowel operationeel, tactisch als strategisch relatiebeheer richting dienstverleners).
Beheren leveranciers	Om een goede samenwerking te borgen, is het voor de dienstverlener noodzakelijk te weten wie zijn leveranciers zijn en wat daar speelt (dus zowel operationeel, tactisch als strategisch relatiebeheer richting dienstverleners).
Accrediteren	Dit is de activiteit die de deelname van een dienstverlener en een leverancier aan een (sectoraal) ecosysteem beheert. Hieronder valt toelaten, wijzigen en verwijderen van deelnemers aan samenwerkingsverbanden/ ecosystemen alsmede toezicht op de naleving van de regels.

Service Lifecycle beheer	
Beheren servicecatalogus	Beheren catalogus is de activiteit die het actuele aanbod aan gegevens inclusief levervoorwaarden van de leverancier inzichtelijk maakt.
Beheren regels	Binnen de activiteit Beheren regels worden de afleidings- en samenstellingsregels (in relatie tot de gegevens) beheerd.
Productontwikkeling	Gegevens die niet in de catalogus opgenomen zijn of niet tegen de gewenste levervoorwaarden, kunnen binnen de activiteit Productontwikkeling leverbaar gemaakt worden (inclusief aanpassing van de levervoorwaarden). Het

	resultaat van productontwikkeling is een nieuw gegeven in de catalogus.

End-to-end Service orkestratie	
Intake bestelling	De bestelling wordt geregistreerd en aan de hand van de afspraak beoordeeld.
Inplannen bestelling	Indien nodig wordt de bestelling ingepland voor productie en levering (een bestelling kan meerdere periodieke leveringen bevatten).
Produceren bestelling	De bestelling wordt aan de hand van de specificaties gereed gemaakt voor levering.
Afronden bestelling	Na levering is de bestelling gereed. Registratie hiervan vindt plaats in een productiesysteem. Deze afronding kan ook de trigger zijn voor financieel afwikkelen.

Financieel vereffenen	
Financieel vereffenen	Indien overeengekomen vindt financiële vereffening plaats.

Verantwoorden	
Verantwoorden	De wet (waaronder AVG) en de betrokken organisaties zelf stellen eisen aan de registratie van alle relevante handelingen in het kader van delen van gegevens. Doel van deze registratie is verantwoording (naar de burger als ook intern) mogelijk te maken. Organisaties leggen verantwoording af aan de burger over de verwerking van zijn persoonsgegevens.

5 Gegevens

5.1 Waarde in het maatschappelijk verkeer

De eIDAS-verordening uit 2014 regelt, samengevat, de *identificatie* van een natuurlijke persoon (met erkenning van andere Europese inlogmiddelen) en de vertrouwensservices waarmee gegevens over die persoon elektronisch *gewaarmerkt* kunnen worden. Bij de evaluatie van deze verordening in 2020 bleek dat de spelers in de markt dit weliswaar een stap in de goede richting vonden, maar dat echte waarde van (persoons)gegevens pas gecreëerd wordt als het identificerende gegeven in relatie met de relevante gegevens over die persoon gewaarmerkt geleverd worden. Dus:

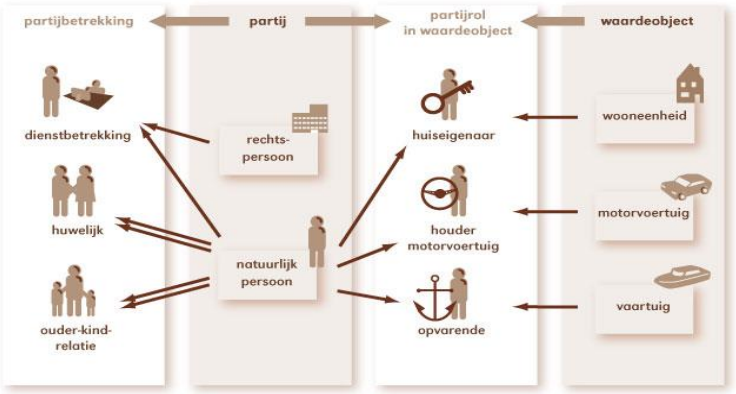
- persoon A heeft een zwemdiploma,
- persoon B is rijbevoegd,
- persoon C vormt geen risico voor Covid19-besmetting,
- persoon D is houder van een gekentekend voertuig

Omdat de huidige verordening op dit punt tekort schiet, wordt deze in het (voorstel voor) amendement van 2021 aangevuld met de mogelijkheid om identificerende gegevens (blauw) te koppelen aan kenmerken (groen) middels een relatie (rood). Deze kunnen vervolgens met behulp van de vertrouwensservices (zie domein 7 van het functiemodel) gewaarmerkt worden om garanties over inhoud en bron/afzender te geven. Het is deze drie-eenheid (identificerende gegevens, kenmerken en bron) die waarde creëert.

5.2 Informatiepositie

Het belang hiervan komt ook tot uiting in de informatiepositie van de burger. De doelstelling van Regie op Gegevens is - geheel in lijn met de Europese Datastrategie- de burger meer inzicht te geven in de persoonsgegevens die de overheid over hem heeft vastgelegd en hem tevens de mogelijkheid te geven om deze persoonsgegevens te gebruiken in transacties buiten de overheid. Voor het (her)gebruik van die gegevens binnen de overheid geldt al het *once-only*-principe.

Deze persoonsgegevens worden gebruikt in overeenkomsten met dienstverleners om de gewenste informatiepositie ten behoeve van die overeenkomst in te vullen. De informatiepositie van de burger wordt hier dus gedefinieerd als een set van gegevens betreffende die burger, nodig om de overeenkomst met de dienstverlener aan te kunnen gaan. Deze set beschrijft *de persoon* en de *relatie* met objecten en andere personen, e.e.a. in de *context* van de overeenkomst *waarin deze gebruikt wordt*.



Zo zal een informatiepositie (de gewenste gegevensset) ten behoeve van het aankopen van een huis een andere zijn dan een informatiepositie van diezelfde burger ten behoeve van een behandelovereenkomst met een arts. Dezelfde persoon, echter andere relevante gegevens. Conclusie: er is altijd een relatie te leggen tussen de informatiepositie (de gevraagde gegevensset) en het doel (de context) waarvoor deze gegevens gebruikt worden.

5.3 Informatiepositie per sector

De gebeurtenis in het leven van een burger bepaalt dus de overeenkomst die de burger met een dienstverlener wil aangaan om een product of dienst geleverd te krijgen. Op basis van de overeenkomst is vast te stellen welke gegevens nodig zijn om tot die overeenkomst te komen. Burger en dienstverlener kunnen het gesprek over welke gegevens nodig zijn aangaan op het moment dat de burger die dienst wil gaan afnemen.

Dat zal voor de meeste burgers niet eenvoudig zijn, dus ligt het voor de hand om deskundige vertegenwoordigers van burgers (zo spreekt bijvoorbeeld de Data Governance Act in artikel 9 lid 1 onder c over *gegevenscoöperaties*) vooraf hierover in gesprek te laten gaan met deskundige vertegenwoordigers van dienstverleners die namens een sector afspraken maakt over (onder meer) de gegevensset die verzameld wordt op het moment dat een burger zich meldt voor het afnemen van een dienst. Afspraken hierover kan dan onderdeel uitmaken van het Vertrouwensraamwerk waar betrokken partijen zich aan conformeren.

5.4 Identificatie aan de hand van persoonsidentificatiegegevens

Onderdeel van de informatiepositie van de persoon vormen de persoonsidentificatiegegevens (de blauwe gegevens uit paragraaf 5.1). Deze kunnen gedefinieerd worden als een unieke set persoonskenmerken dat op exact één individu betrekking heeft. Vaak is de enkele combinatie tussen *achternaam* en *geboortedatum* al voldoende om één individu uniek te identificeren. Voor die gevallen waarin dat niet toereikend is, is het toevoegen van één of enkele persoonskenmerken (bijv. voornaam, geboorteplaats) voldoende om in een populatie de anderen te uniek identificeren. Het Interoperabiliteitskader elektronische identificatie en vertrouwensdiensten (behorend bij eIDAS 2014) maakt voor een natuurlijk persoon onderscheid in een minimale pakket persoonsidentificatiegegevens en een set van mogelijke aanvullingen:

Vereisten betreffende het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of rechtspersoon op unieke wijze vertegenwoordigt, als bedoeld in artikel 11

1. Minimaal gegevenspakket voor een **natuurlijke persoon**

Het minimale gegevenspakket voor een natuurlijke persoon bevat al de volgende verplichte attributen:

a) huidige familienaam of familienamen;

b) huidige voornaam of voornamen;

c) geboortedatum;

d) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.

Het minimale gegevenspakket voor een natuurlijke persoon **kan** één of meer van de volgende aanvullende attributen bevatten:

a) voornaam of voornamen en familienaam of familienamen bij geboorte;

b) geboorteplaats;

c) huidig adres;

d) geslacht.

Binnen de context van Regie op Gegevens wordt ervan uitgegaan dat de **overheid** de identiteit van een persoon aan de hand van identificerende gegevens vaststelt (en niet de burger zelf of een andere partij).

5.5 Attributen

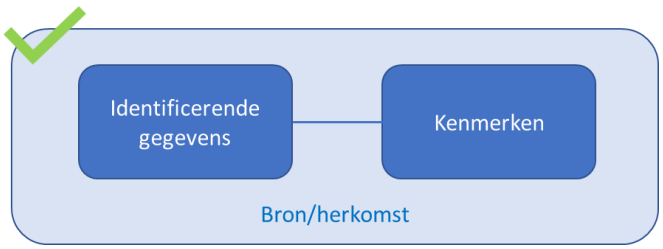
In paragraaf 5.1 werd al gewezen op het feit dat waarde gecreëerd wordt door de combinatie van identificerende gegevens, kenmerken en bron. Hierbij wordt met kenmerk (ook wel attribuut genoemd) bedoeld ieder gegeven dat een bewering doet over die persoon. De eIDAS-verordening definieert een attribuut als: *een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat*.

De overheid heeft een grote hoeveelheid en diversiteit aan beweringen over personen in zijn bronnen opgenomen. Deze bronnen bij de overheid zijn allereerst de basisregistraties, die oorspronkelijk bedoeld zijn om informatieposities rondom natuurlijke personen, rechtspersonen en locaties op te bouwen voor hoofdzakelijk intern overheidsgebruik. Ook zijn er vele informatieposities opgebouwd in sectorale registraties, bedoeld voor intern overheidsgebruik.

In de NORA zijn de Basisregistratie en Sectorregistraties als bouwblokken opgenomen (een overzicht van 145 registraties op basis van een inventarisatie uit 2017). Zowel de basisregistraties als sectorregistraties bevatten persoonsgegevens die mogelijk ontsloten dienen te worden. Naast deze registraties zijn er natuurlijk vele andere bronnen binnen de overheid waarin zich persoonsgegevens bevinden die voor ontsluiting in aanmerking komen. Er is ook een overzicht van datasets die in het kader van Open Data beschikbaar worden gesteld op data.overheid.nl.

5.6 Elektronisch attesteren van attributen

Een attest is een elektronisch bewijs, een verklaring die een bewering versterkt, ondersteunt, wettigt. Elektronisch attesteren van attributen is dus in deze context het combineren/koppelen van identificerende gegevens, bijbehorende kenmerken en bron om deze vervolgens te voorzien van waarmerk (timestamp, handtekening en verzegeling):



5.7 Verificatie van attributen aan de hand van authentieke bronnen

Een andere manier om hetzelfde effect te bereiken (een gewaarmerkte uitspraak over een eigenschap van een persoon) kan door middel van verificatie bij de authentieke bron:

Artikel 45 quinquies

Verificatie van attributen aan de hand van authentieke bronnen

1. De lidstaten waarborgen dat er, ten minste voor de in bijlage VI vermelde attributen, voor zover die attributen authentieke bronnen binnen de publieke sector gebruiken, maatregelen worden genomen zodat gekwalificeerde verleners van elektronische attesteringen van attributen op verzoek van de gebruiker langs elektronische weg de authenticiteit van het attribuut rechtstreeks kunnen verifiëren aan de hand van de relevante authentieke bron op nationaal niveau of via op nationaal niveau overeenkomstig nationaal of Unierecht erkende aangewezen intermediairs.
2. Binnen zes maanden na de inwerkingtreding van deze verordening en met inachtneming van de toepasselijke internationale normen legt de Commissie door middel van een uitvoeringshandeling betreffende de uitvoering van de Europese portemonnees voor digitale identiteit in de zin van artikel 6 bis, lid 10, minimale technische specificaties, normen en procedures vast met betrekking tot de catalogus van attributen en regelingen voor de attestering van attributen en verificatieprocedures voor gekwalificeerde elektronische attesteringen van attributen.

MINIMALE LIJST VAN ATTRIBUTEN

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

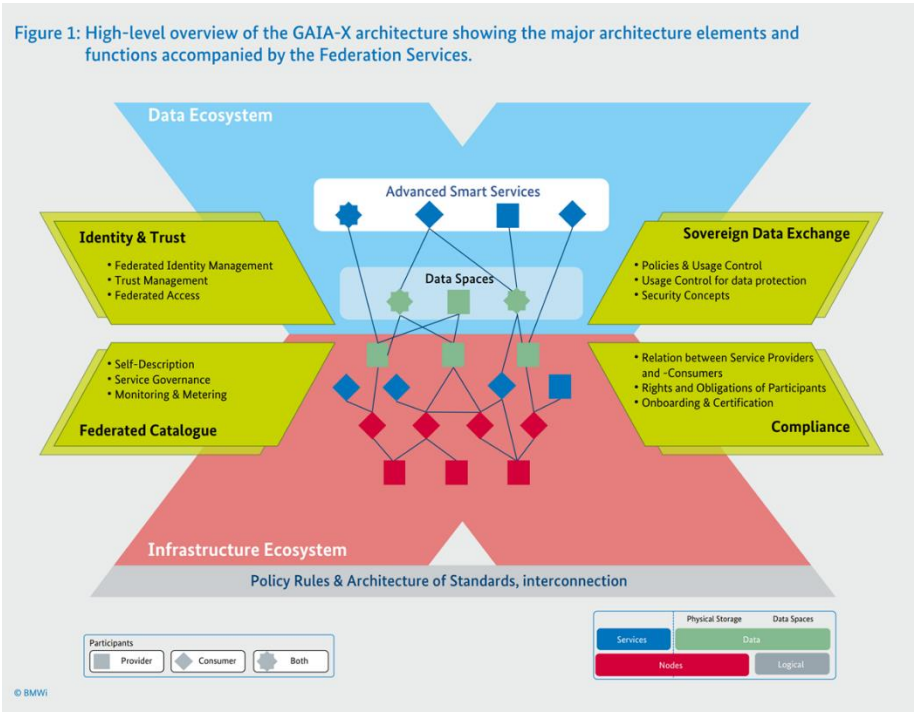
de **authenticiteit van de volgende attributen kunnen verifiëren**:

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

5.8 Ontwikkeling naar federatieve data infrastructuur

Een belangrijke ontwikkeling in het delen van gegevens in Europees verband is GAIA-X (gestart in 2020). Het Duits-Franse GAIA-X-initiatief richt zich op het realiseren van een pan-Europese 'federatieve data infrastructuur'. Omdat die in belangrijke mate moet gaan steunen op onderling verbonden cloud diensten wordt GAIA-X ook gezien als een belangrijk vehikel om veilige Europese cloud voorzieningen te realiseren. Vanuit Nederland is Normcommissie (NEN) hierbij betrokken. In de GAIA-X architectuur (2020) en verdere uitwerking (2021) wordt het onderstaand model uitgewerkt, waarbij wordt ingezet op een Europees federatief model op de onderdelen Identity en trust, Woordenboek, Soevereine Gegevensuitwisseling en Compliance:

Figure 1: High-level overview of the GAIA-X architecture showing the major architecture elements and functions accompanied by the Federation Services.



De visie op de **doorontwikkeling van het stelsel van basisregistraties** sluit naadloos op deze ontwikkeling aan:

"Het hiervoor genoemde doel van onderlinge verbonden stelsels kan worden gerealiseerd door het huidige stelsel van 10 basisregistraties verder te ontwikkelen tot een stelsel waarin steeds meer partijen samenwerken om hun sectorale basisdata op de stelselmanier te ontsluiten, dus met waarborgen voor het vertrouwen bij burgers, afnemers en data aanbieders. Hiermee groeit het stelsel van basisregistraties uit tot een bredere nationale datafederatie van hoogwaardige databronnen die daartoe gerechtigde gebruikers flexibel, naar behoefte, kunnen toepassen en die op Europees niveau aansluiting biedt op soortgelijke stelsels van andere landen."

"De NL-datafederatie is geen IT systeem en geen datapakhuis, maar een virtuele dataverzameling waarbij op registratieniveau of op sectorniveau het lokale aanbod volgens het principe van "data bij de bron" binnen het

federatieve stelsel wordt ontsloten. Daarbij zorgt het adopteren van stelselafspraken, stelselstandaarden en stelselfuncties in combinatie met het toepassen van dezelfde identificerende gegevens/koppelsleutels ervoor dat individuele databronnen een datastelsel worden en dat data tussen de op het NL-datafederatie aangesloten partijen kan stromen. Van deze federatie kunnen zowel private als publieke databronnen deel uitmaken." (Toekomstbeeld Stelsel van Basisregistraties v08c, p. 3 e.v.).

5.9 Gegevenswoordenboek

Gezien de omvang van het aantal mogelijk gewenste persoonsgegevens en bronnen is vindbaarheid van het juiste gegeven een uitdaging. Hiervoor bestaan al veel initiatieven waarop aangesloten kan worden. Het vinden van een gegeven begint met een eenduidige beschrijving van de betekenis van de gebruikte begrippen (waarbij bij voorkeur wordt gelinkt met de relevante wet- en regelgeving) in een gegevenswoordenboek. Daarnaast zijn aspecten als gegevenskwaliteit (juistheid, actualiteit enz.) en herkomst/bron van belang. Op Europees niveau wordt hiervoor verwezen naar EU thesauri terwijl BegrippenXL op nationaal niveau als ingang kan dienen. Daarnaast is er de bestaande (en beheerde) inventarisatie van Gegevenswoordenboeken (inmiddels meer dan 25, waaronder de Stelselcatalogus) in de NORA. Deze zijn/worden volgens de standaard JSON/Linked Data machineleesbaar en interpreteerbaar aangeboden.

5.10 Produceren van gegevens

Wat nu als de gegevens in de bron niet overeenkomen met de vraag van burger en/of dienstverlener maar dat de vraag wel af te leiden is uit de gegevens die wel beschikbaar zijn? Dan zijn bewerkingen met behulp van gegevensservices nodig. Naast de CRUD (create, read, update en delete) wordt worden de bewerkingen *verzamelen*, *integreren* en *afleiden* hier nader toegelicht.

5.10.1 Verzamelen

Gegevens worden binnen deze activiteiten gereed gemaakt voor levering (push of pull). Dit kan gebeuren tijdens het inwinnen ('doorlevering') maar ook tijdens de opslag of bij levering. Afhankelijk van het gegeven en de manier waarop deze vanuit de bron beschikbaar is, bestaat het klaar maken voor levering uit het verzamelen van de benodigde gegevens, indien nodig filteren van de verzameling en samenstellen indien gegevens uit verschillende bronnen in één levering bijeengebracht moeten worden. Uitgangspunt bij verzamelen is dat er geen bewerking aan het gegeven zelf gedaan wordt, m.a.w. de onderdelen worden verzameld, in een doos gestopt, gewaarmerkt en aangeboden voor verzending.

5.10.2 Integreren

Met integreren (aggregeren) worden gegevens in onderlinge samenhang gebracht op een zodanige manier dat deze verwerkt kunnen worden door de gebruiker. Waar de functie Verzamelen meer doelt op de logistiek van gegevens, doelt de functie Integreren meer op de inhoud en onderlinge samenhang van gegevens door middel van de regels in een informatiemodel (bijv. in tijd zoals bij 'omzet per maand' het geval zal zijn). In deze functie kunnen nieuwe gegevens ontstaan. Een voorbeeld van een voor de gebruiker in samenhang gebrachte gegevensset is natuurlijk het Kadaster (IMKAD) en andere basisregistraties.

5.10.3 Afleiden

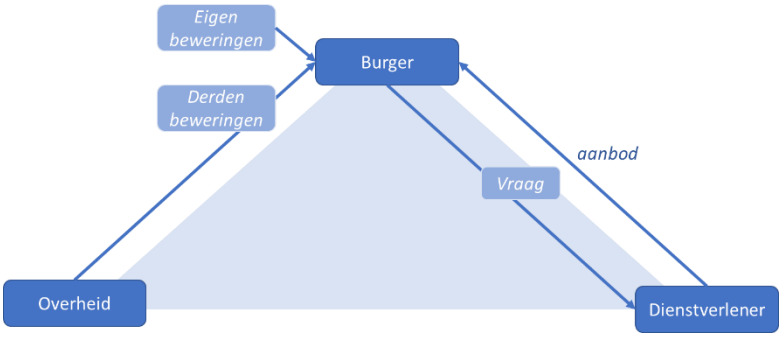
Afleiden gaat nog een stap verder dan integreren: binnen deze activiteit worden op basis van regels (algoritmen) conclusies getrokken en nieuwe gegevens (de conclusie) gegenereerd. Afleiden speelt een belangrijke rol binnen dataminimalisatie in het kader van privacybescherming.
Artikel 5 lid 1 sub c AVG stelt, als één van de 'beginselen inzake verwerking van persoonsgegevens', dat de gegevensverwerking toereikend is, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit laatste wordt ook het principe van dataminimalisatie genoemd en is daarmee onderdeel van de beperkende maatregelen op de inbreuk van de privacy van burgers. Ook binnen de Wet Digitale Overheid is privacy by design het uitgangspunt.
Binnen de context van RoG zijn hierbij globaal drie strategieën te onderkennen:
Alleen die gegevens die strikt noodzakelijk zijn voor het beantwoorden van de vraag (dataminimalisatie door filteren, hiervoor beschreven als een vorm van verzamelen).
Conclusie als gegeven en niet de gegevens die leiden tot de conclusie (dataminimalisatie door delen afleiden).
Cryptografisch bewijs over gegevens zonder de gegevens zelf te delen (dataminimalisatie door wiskundig bewijs, waaronder diverse Privacy Enhancing Technologies).
Transparantie naar de burger ten aanzien van het algoritme (naast de gegevens!) dat gebruikt wordt om de gewenste afleiding te doen is, één van de manieren om vertrouwen bij de burger te krijgen. Een van de manieren is de recente ontwikkeling van het Nationaal Algoritmen Register.

5.11 Eigenaarschap van Gegevens

Uitgangspunt is dat de gegevenseigenaar (vaak de bronhouder) verantwoordelijk is voor de kwaliteit van het gegeven uit die bron. Gegevens die rechtstreeks uit de bron komen, door de eigenaar zelf gewaarmerkt worden met behulp van vertrouwensservices en aan de burger ter beschikking gesteld worden, kunnen door die gegevenseigenaar gegarandeerd worden als 'overeenkomstig de bron'. Zodra dat waarmerken al door een ander dan de eigenaar wordt gedaan, dan zal die eigenaar die ander hierin al moeten vertrouwen wil die eigenaar de garantie kunnen blijven afgeven. Afspraken hierover kunnen in een vertrouwensraamwerk gemaakt worden.
Dit wordt al gecompliceerder wanneer tussen de weg van bron naar burger/dienstverlener bewerkingen (gegevensservices) plaatsvinden waarbij nieuwe gegevens ontstaan. Is de eigenaar van de brongegevens nog wel in staat om de kwaliteit van dat nieuwe gegeven te garanderen of ontstaat met het creëren van dit nieuwe gegeven ook een nieuwe eigenaar die verantwoordelijk is voor de gegevenskwaliteit? Ook hierover zullen afspraken gemaakt moeten worden in een vertrouwensraamwerk.

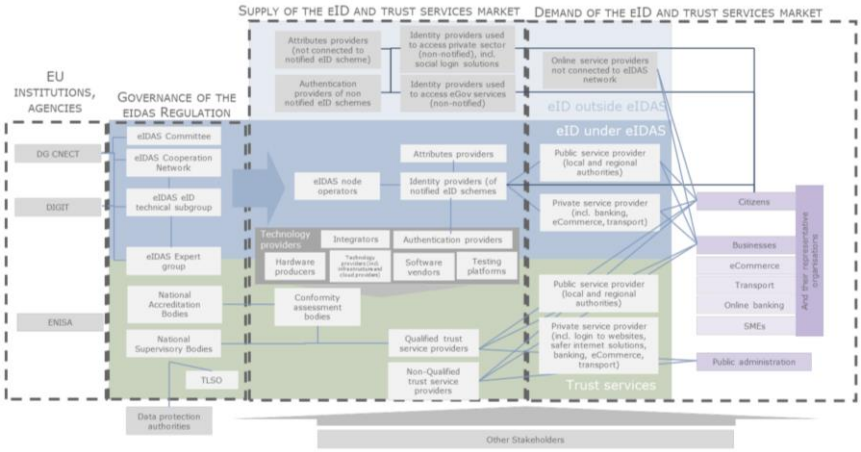
6 Proces

6.1 Actoren



1. **Burger**
   Onder burger wordt in deze context verstaan iedere natuurlijke persoon die ingezetene is in Nederland. Onder de categorie burger valt daarnaast ook de natuurlijke persoon die opgenomen is in het Register Niet-Ingezetenen RNI (niet-ingezetene met een relatie met de Nederlandse overheid). Burger is ook iedere Europese ingezetene die met een erkend Europees inlogmiddel toegang vraagt tot zijn persoonsgegevens.
   Een burger kan zich laten vertegenwoordigen door een wettelijke vertegenwoordiger (indien van toepassing) of door een gevolmachtigde vertegenwoordiger.
2. **Dienstverlener**
   Onder dienstverlener wordt in deze context verstaan iedere natuurlijke of rechtspersoon die een product of dienst aan een burger levert.
3. **Overheid (als bron)**
   Onder overheid wordt in deze context verstaan iedere overheidsorganisatie die een bron beheert waarin zich persoonsgegevens bevinden. De overheid als marktmeester valt buiten de scope van de referentiearchitectuur. Deze rol wordt uitgewerkt in wet- en regelgeving en het vertrouwensraamwerk.
4. **Intermediair**
   Onder intermediair wordt in deze context verstaan iedere natuurlijke of rechtspersoon die als tussenpersoon gegevens- en/of vertrouwensdiensten levert aan burger, dienstverlener of bronhouder (i.c. overheid).

Binnen het architectuurkader van eIDAS zijn deze actoren nader gespecificeerd in onderstaand overzicht van stakeholders en overzicht ecosysteem in eIDAS:



6.2 Triggers

- Huis kopen
- Auto huren
- Huis huren
- Zwangerschap
- Verzekering afsluiten
- Uitkering aanvragen
- Medische hulp ivm ziekte
- Reizen van A naar B
- …

Om invulling te geven aan het principe Burger Centraal wordt zoveel mogelijk de wereld van de burger als startpunt genomen voor de interactie tussen de actoren. Vanuit het perspectief van die burger is in de regel de aanleiding om persoonsgegevens uit een overheidsadministratie te willen ophalen een gebeurtenis in het leven van die burger naar aanleiding waarin deze producten of diensten geleverd wenst te krijgen van dienstverleners (of overheid). Deze gebeurtenissen kunnen zeer divers van aard zijn (zie kader) en starten iedere keer andere processen/interactiepatronen met andere actoren. Ook de gegevens die de burger per gebeurtenis nodig heeft om zijn product of dienst geleverd te krijgen, verschillen per gebeurtenis. De gebeurtenis start een dus specifiek proces/interactiepatroon en vereist een specifieke set aan gegevens, behorend bij die gebeurtenis.

6.3 Interactiepatronen

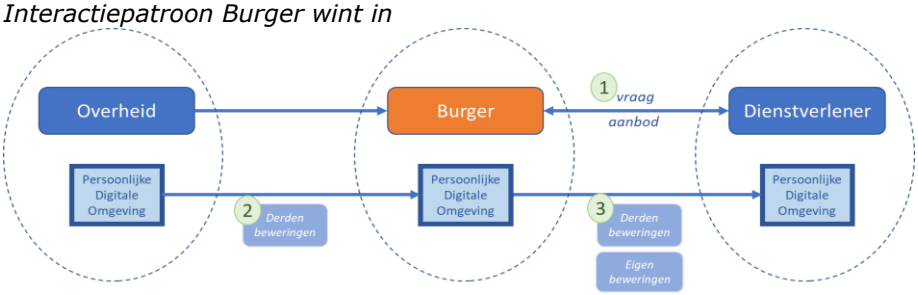
Om het persoonsgegeven van overheidsbron naar uiteindelijk de dienstverlener te krijgen, zijn in beginsel twee routes (de interactiepatronen) mogelijk, te weten:

1. De **burger wint het gegeven zelf in** bij de overheidsbron en levert deze vervolgens aan de dienstverlener of
2. De **dienstverlener wint het gegeven in** (met volmacht van de burger) bij de overheidsbron.

Enkele noties:

- Van belang is op te merken dat beide interactiepatronen uiteindelijk **hetzelfde resultaat** opleveren: het persoonsgegeven uit de overheidsbron worden aan de dienstverlener geleverd. Beide interactiepatronen stellen echter andere eisen (waaronder waarmerken en toestemming) en afhankelijk van de situatie kunnen dus keuzes gemaakt worden in de route om hetzelfde resultaat te bereiken.
- Daarnaast geldt het uitgangspunt dat de **burger vrij is om te kiezen** op welke wijze hij de gegevens wil delen. Hieronder worden de interactiepatronen nader uitgewerkt.

6.3.1 *Interactiepatroon Burger wint in*



1- De burger wil een product of dienst afnemen van de dienstverlener. Om een aanbod te kunnen doen heeft de dienstverlener (persoons)gegevens van/over de burger nodig.

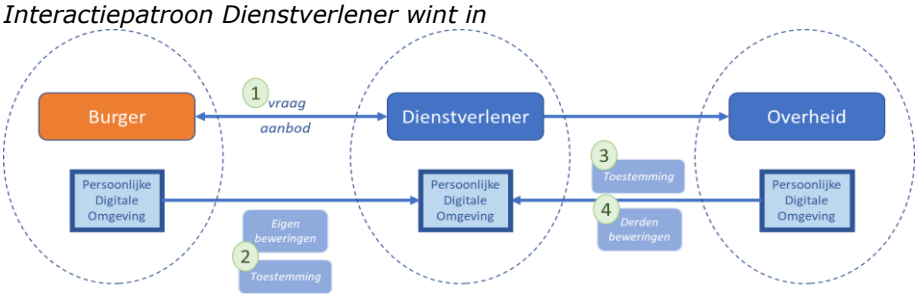
Een deel van die informatiepositie zal bestaan uit gegevens die de burger zelf kan/moet invullen (eigen beweringen) en een deel kan bestaan uit gegevens die (op verzoek van de dienstverlener) uit een andere bron afkomstig zal zijn, hier gedefinieerd als derdenbeweringen uit de bron van de overheid. Het deel van de informatiepositie dat de burger met eigen beweringen kan invullen, kan de burger direct aan de dienstverlener leveren.

2-
Voor derdenbeweringen zal de burger dit gegeven eerst uit de bron van de overheid moeten ophalen en in zijn eigen Persoonlijke Digitale Omgeving moeten brengen. Als hij nog over een geldig gegeven uit de overheidsbron in zijn eigen Persoonlijke Digitale Omgeving beschikt, dan kan hij deze natuurlijk direct gebruiken en is ophalen bij de overheid niet nodig.

3-
Als de burger de gevraagde gegevens voor de informatiepositie (dus derdenbeweringen en eigen beweringen) compleet heeft, kan hij deze aan de dienstverlener leveren zodat deze het aanbod kan doen.

Kenmerken van dit interactiepatroon zijn:
- De **positie van de burger**. Deze staat letterlijk tussen dienstverlener en de bron in en heeft *by design* volledig zicht en controle op de gegevens die vanuit de overheidsbron met de dienstverlener gedeeld worden.
- Geen **koppeling tussen uitvraag bij de bron en doel** waarvoor het gebruikt wordt: de burger hoeft niet aan de bronhouder te verantwoorden waarom/waarvoor het persoonsgegeven ingewonnen wordt.
- De wens van het **waarmerk**: de dienstverlener wil de garantie dat het gegeven uit de bron (de derdenbewering) ook daadwerkelijk van die bron afkomstig is en overeenkomt met die bron. Hier speelt de **vertrouwensservice** (trustservices uit eIDAS) een grote rol.
- Het onderwerp **toestemming** (niet zijnde wettelijke vertegenwoordiging) maakt geen onderdeel uit van dit interactiepatroon.

6.3.2 *Interactiepatroon Dienstverlener wint in*



1-
Ook dit interactiepatroon start met de relatie tussen dienstverlener en de burger. Om een aanbod te kunnen doen heeft de dienstverlener (persoons)gegevens van/over de burger nodig. Een deel van die informatiepositie zal bestaan uit eigen beweringen en (mogelijk) een deel uit derdenbeweringen.

2-
Het verschil met het vorige interactiepatroon is dat niet de burger de derdenbewering inwint, maar de dienstverlener aanbiedt om dat namens deze burger te doen. Het is dus de dienstverlener die zich bij de overheid digitaal meldt met het verzoek om een persoonsgegeven uit de bron van de overheid. De bronhouder zal vanwege zijn geheimhoudingsplicht deze gegevens alleen ter beschikking stellen indien de dienstverlener als gevolmachtigde van de burger optreedt, m.a.w. de dienstverlener toestemming heeft van de burger om namens hem de persoonsgegevens bij de overheid in te winnen.

3/4-
De dienstverlener wint met toestemming van de burger zijn persoonsgegevens (derdenbeweringen) in bij de overheid.

Kenmerken van dit interactiepatroon zijn:
- De **positie van de burger**. In dit interactiepatroon staat de dienstverlener tussen de burger en de bron in. Vanuit deze positie heeft de burger *by design* veel minder zicht en controle op de gegevens die vanuit de overheidsbron met de dienstverlener gedeeld worden. Om de burger toch vertrouwen te geven in zowel dienstverlener als overheid en hem uit vrij wil te bewegen gebruik te maken van deze dienst, zijn aanvullende maatregelen gericht op dit vertrouwen noodzakelijk.
- Het onderwerp **toestemming** maakt altijd onderdeel uit van dit interactiepatroon.
- **Koppeling tussen uitvraag bij de bron en doel** waarvoor het gebruikt wordt: de burger geeft toestemming aan de dienstverlener om gegevens namens hem in te winnen. De eis aan de toestemming is dat deze voldoende specifiek en afgebakend is (dus geen toestemming zoals dat nu bij bijv. *cookies* het geval is). Hierdoor kan de overheid mogelijk afleiden welke gegevens, waarvoor en aan wie geleverd worden.
- De wens van het **waarmerk is in dit interactiepatroon minder relevant**: de dienstverlener haalt namelijk zelf de gegevens rechtstreeks bij de vertrouwde bron en heeft daarmee al de nodige garanties op afzender en integriteit van het gegeven. Hier speelt de

vertrouwensservice (trustservices uit eIDAS) dus minder een rol. Natuurlijk staat het de dienstverlener vrij om tegen vergoeding extra vertrouwensservices zoals digitale handtekening en/of digitale seal te gebruiken.

- Het moment waarop de burger volmacht (toestemming) verleent en aan wie kan verschillen en leiden tot een **variant op bovenstaand interactiepatroon**. Het is namelijk ook mogelijk dat de burger zijn wilsuiting (toestemming tot het leveren van vooraf gedefinieerde persoonsgegevens aan vooraf gedefinieerde dienstverleners in vooraf gedefinieerde gevallen) aan de overheid kenbaar maakt **voordat** de dienstverlener een verzoek bij de overheid tot het leveren van specifieke persoonsgegevens voor deze burger doet. De overheid zal dan in zijn eigen administratie moeten nagaan of de specifieke toestemming van die burger bestaat om vervolgens dit gegeven met toestemming van die burger aan de dienstverlener te kunnen leveren.
- Een van de verschijningsvormen van dit interactiepatroon is verificatie zoals bedoeld in art. 45 quinquies eIDAS: de dienstverlener kan bij de juistheid van een gegeven controleren door deze te vergelijken met de bron. De dienstverlener heeft dat gegeven dus al (bijvoorbeeld omdat de burger dit verklaard heeft aan die dienstverlener) en vergelijkt deze met de bron. Het antwoord is dan ja of nee: het komt overeen of niet.

6.4 Use-cases

6.4.1 Vanuit de burger

De burger wil:

1. Een dienst afnemen van een dienstverlener
2. Inzage in zijn gegevens in een administratie van de overheid
3. Zijn gegevens in een administratie van de overheid kunnen corrigeren
4. Zijn gegevens digitaal (evt. gewaarmerkt) van de overheid in zijn PDO kunnen overnemen
5. Zijn gegevens kunnen bewaren in zijn PDO
6. Zijn gewaarmerkte gegeven kunnen actualiseren indien deze niet meer geldig is
7. Waarmerken aan een gegeven kunnen toevoegen
8. (Eigen) gegevens kunnen toevoegen aan zijn PDO
9. Gegevens kunnen wijzigen in zijn PDO
10. Gegevens kunnen verwijderen uit zijn PDO
11. Gegevens tussen verschillende PDO-en kunnen uitwisselen
12. Gegevens in zijn PDO (inclusief waarmerk) kunnen tonen aan personen
13. Gegevens digitaal kunnen leveren aan PDO’s van dienstverleners of diens beheerders
14. Een dienstverlener digitaal kunnen machtigen om gegevens in te winnen bij de overheid.
15. Deze digitale machtiging kunnen beheren.
16. Gegevens kunnen beveiligen
17. Kunnen attenderen indien de geldigheid (i.c. waarmerk) van een gegeven verloopt

6.4.2 *Vanuit de dienstverlener*

De dienstverlener wil:

1. Een PDO aan een burger beschikbaar kunnen stellen
2. Inzage in een PDO van een burger aan die burger kunnen geven
3. Gegevens digitaal kunnen ontvangen uit PDO-en van burgers
4. Burgers inzage geven in hun (door de dienstverlener beschikbaar gestelde) PDO
5. Burgers inzage geven in ontvangen leveringen van gegevens door de overheid (verantwoording)
6. Burgers gegevens laten beheren in hun (door de dienstverlener beschikbaar gestelde) PDO
7. Burgers de mogelijkheid geven fouten te herstellen
8. Inzicht geven in de in te winnen gegevens middels een gegevenscatalogus (inkoop)
9. Machtigingen van burgers digitaal kunnen ontvangen, opslaan en gebruiken
10. Een afspraak tot het leveren van gegevens met overheid kunnen maken
11. Een afspraak tot het leveren van gegevens met overheid kunnen beheren
12. Een bestelling tot het leveren van gegevens bij een overheid kunnen doen
13. Levering van gegevens door de overheid aan een PDO kunnen toevoegen
14. Gegevens kunnen beveiligen
15. Kunnen attenderen indien de geldigheid (i.c. waarmerk) van een gegeven verloopt

6.4.3 *Vanuit de overheid*

De overheid wil als bronhouder van persoonsgegevens:

1. Inzicht geven middels de gegevenscatalogus (verkoop) in de mogelijk te leveren gegevens
2. De gegevenscatalogus kunnen beheren
3. Nieuwe gegevens kunnen leveren (productontwikkeling)
4. Afleidingen o.b.v. algoritmen van dienstverleners kunnen doen
5. Een afspraak tot het leveren van gegevens met een dienstverlener kunnen maken
6. Een afspraak tot het leveren van gegevens met een dienstverlener kunnen beheren
7. Een bestelling tot het leveren van gegevens door een dienstverlener kunnen besturen
8. Een bestelling kunnen autoriseren
9. Gegevens aan een burger kunnen leveren in zijn PDO
10. Gegevens aan een dienstverlener kunnen leveren (indien afgesproken in een individueel) PDO
11. De burger inzage geven in zijn gegevens in een administratie van de overheid

12. De burger inzage geven in/ verantwoording afleggen over over de levering van die gegevens aan dienstverlener x op moment y voor doel/transactie z.
13. De burger zijn gegevens kunnen laten corrigeren
14. Gegevens van de burger digitaal kunnen waarmerken
15. Kunnen attenderen indien de geldigheid (i.c. waarmerk) van een gegeven verloopt
16. Gegevens kunnen beveiligen

7 Applicatie

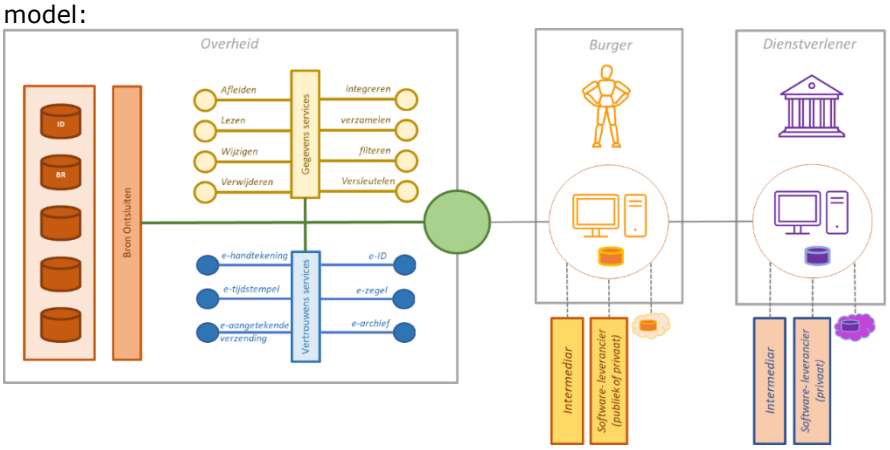
7.1 Applicatieservices Regie op Gegevens

Een interactiepatroon beschrijft het proces dat de levering van het persoonsgegeven uit de administratie van de overheid aan de dienstverlener realiseert. In dit proces worden de functies uit het functiemodel (de inrichtingsonafhankelijke bewerkingen) aaneen geregen om tot het gewenste resultaat te komen. In de servicegeoriënteerde benadering van deze referentiearchitectuur betekent dit dat het eindresultaat voor de burger gerealiseerd wordt door applicatie- en netwerkservices die door werkstroombesturing in de juiste volgorde aangeroepen worden. De belangrijkste services die bij het ontsluiten van persoonsgegevens uit bronnen bij de overheid een rol spelen zijn (naast werkstroombesturing):

1. Toegangsservice (groen)
2. Koppelvlakservices (groen)
3. Gegevensservices (geel)
4. Vertrouwensservices (blauw)
5. Bronontsluitingsservices (geel en rood)

7.2 Schets services *Burger wint in*

Toegepast op het interactiepatroon *Burger wint in* leidt dit tot het volgende model:



Aan de linkerkant de overheid als bron, in het midden de burger die contact maakt met de overheid om een gegeven in te zien, te corrigeren of in te winnen en aan de rechterkant de dienstverlener die een dienst gaat leveren aan de burger.

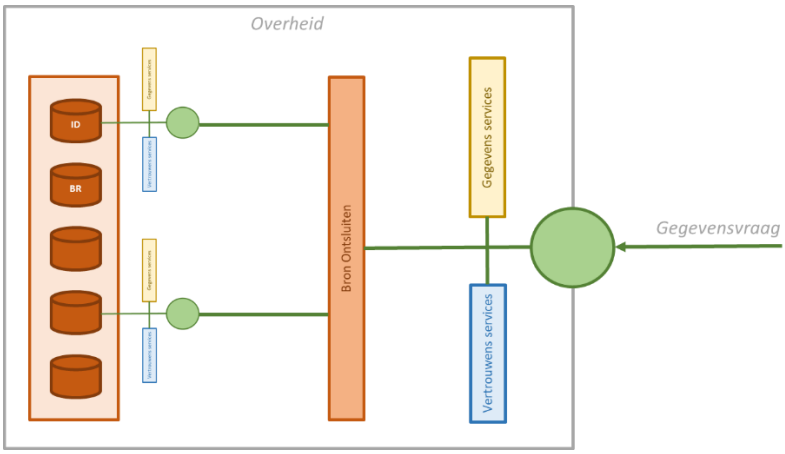
Zowel burger als dienstverlener kan hierbij:

- gebruik maken van een apparaat onafhankelijke toepassing (desktop/laptop/tablet/smartphone)
- met of zonder opslag (lokaal of in de cloud of geen lokale opslag maar altijd gegevens bij de bron)
- onder licentie gebruik maken van “eigen” software voor regiehandelingen (beschikbaar gesteld door private softwareleveranciers of vanuit de overheid) of

- gebruik maken van een “eigen” intermediair die namens de burger of dienstverlener overeengekomen gegevens- en/of vertrouwensdiensten levert.

Ter illustratie is de beschrijving van één *use case* (als variant op vele mogelijkheden) dan:
De burger logt vanuit zijn eigen Digitale Persoonlijke Omgeving met zijn eigen erkende inlogmiddel in bij de overheid (groene bol) en doet een leesactie op een gegeven in de bron (gele gegevensservice “lezen” i.c.m. rode bronontsluiting op de basisregistratie. Hij controleert het gegeven en besluit dat dit gegeven, voorzien van een waarmerk (blauwe vertrouwensservices e-Handtekening, e-Tijdsstempel, e-ID en e-Zegel) in te winnen (gele gegevensservice verzamelen) en in zijn eigen omgeving in de cloud te plaatsen. Vervolgens levert hij dit gewaarmerkte gegeven aan de dienstverlener.

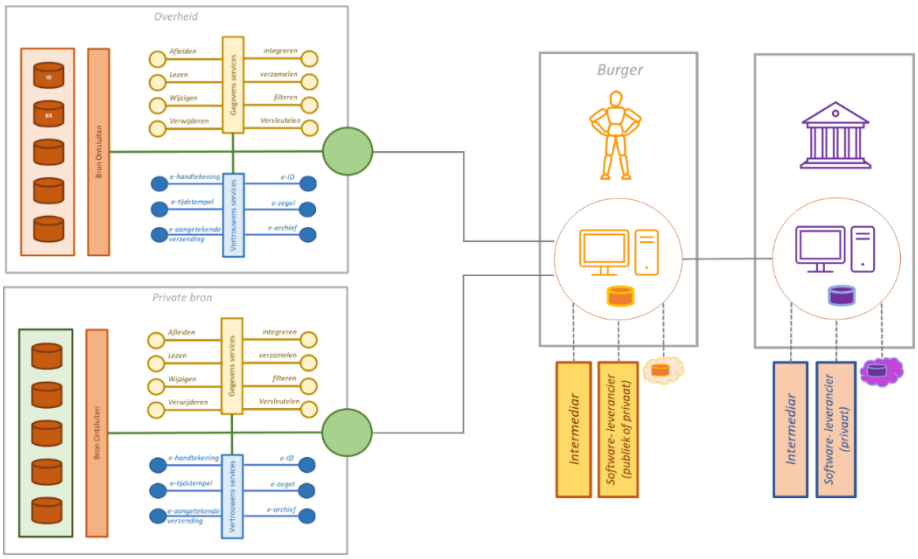
Als ingezoomd wordt op de overheid als bron, dan bestaat die bron uit een hele verzameling van bronnen, vaak verdeeld over net zoveel overheidsorganisaties. Bij het uitvragen van een persoonsgegeven aan een bron ontstaan er twee mogelijkheden:



- de gegevensvraag wordt gesteld aan het centrale aanspreekpunt (rechter groene stip) en het aanspreekpunt verzamelt bij de bronnen en (indien nodig) bewerkt en/of waarmerkt of
- de gegevensvrager gaat zelf direct naar de aanspreekpunten van de verschillende bronnen (linker groene stippen) om de gegevens te verzamelen en die iedere bron voor zich (noodzakelijkerwijs) dan bewerkt en/of waarmerkt.

Op het moment van schrijven (2022) is nog niet vastgesteld wat het voorkeursscenario is.

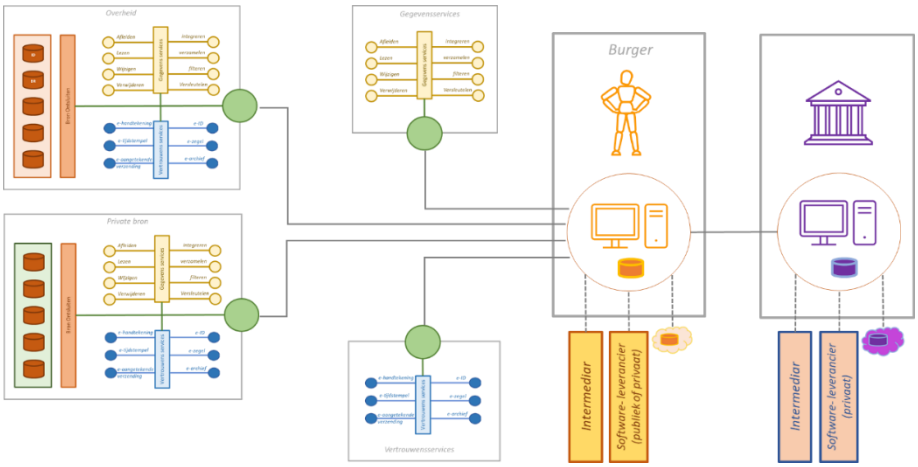
Het bovenstaande model geeft alleen de overheid als bron weer. Vanuit burgerperspectief zal de overheid vaak niet de enige bron zijn vanwaar uit gegevens ingewonnen worden. Ook private bronnen zullen hierin een rol gaan spelen (zoals ze dat nu al vaak doen). De toepassingen die de burger (of in zijn naam de intermediair) zal gaan gebruiken zullen dus zowel gegevens moeten kunnen inwinnen bij bronnen bij de overheid als bronnen bij private partijen. Deze gebruikerswens leidt tot het volgende uitbreiding:



In bovenstaand model zijn zowel de (gele) gegevensservices als de (blauwe) vertrouwensservices opgenomen in het domein van de publieke en de private bron. Dit betekent dat het gegeven of de gegevensset ***voordat*** dit het domein van de overheid of het domein van de private bron verlaat, middels gegevensservices bewerkt kan worden, bijvoorbeeld integratie t.b.v. het aanbrengen van samenhang of afleiding t.b.v. dataminimalisatie in het kader van de bescherming van de privacy.

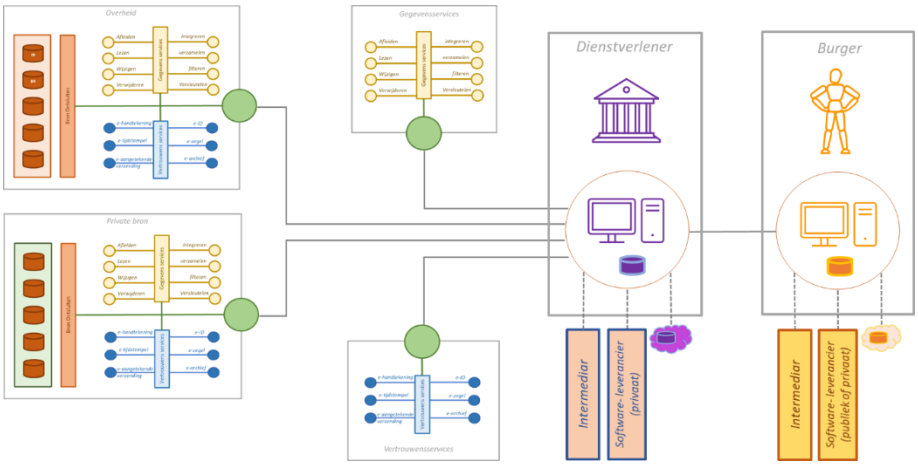
Het ligt voor de hand dat de burger bij het vullen van de concrete informatiepositie gebruik gaat maken van een combinatie van (persoons)gegevens uit zowel publieke als private bronnen (bijvoorbeeld bij het vaststellen van de actuele schuldenpositie) zodat de gegevensservice (bijvoorbeeld integratie of afleiding) moet plaatsvinden ***nadat*** de gegevens het domein van publieke en private bron heeft verlaten.

Als de gegevens bewerkt worden nadat ze het domein van overheid of private partij hebben verlaten, gaat dit zonder aanvullende maatregelen natuurlijk ten koste van het vertrouwen van de dienstverlener in de integriteit van de geleverde gegevens. Hij krijgt immers gegevens aangeleverd waarvan “het zegel verbroken is”. Waarmerken nadat de gegevens bewerkt zijn met behulp van vertrouwensservices zullen daarom in zo’n geval noodzakelijk zijn. Dit leidt tot het volgende aanvulling op het model (waarbij een veelheid aan varianten en combinaties mogelijk is):



7.3 Schets services *Dienstverlener wint in*

Voor het interactiepatroon *Dienstverlener wint in* is zo'n zelfde schets te maken. De betrokken gegevens- en vertrouwensservices zijn in beginsel dezelfde als bij het interactiepatroon *Burger wint in*, alleen speelt hier ook nog het toestemmingsvraagstuk (niet in de figuur opgenomen).

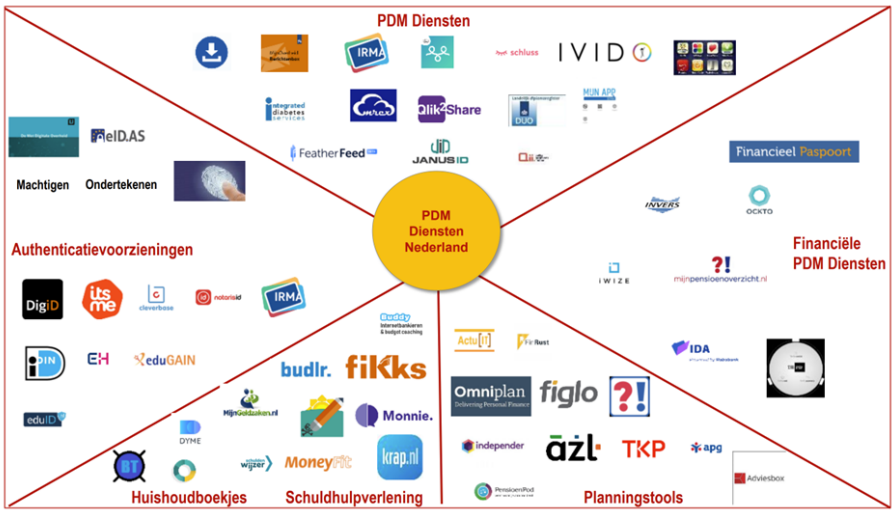


7.4 Persoonlijk digitale omgevingen

In deze referentiearchitectuur wordt gesproken over Persoonlijke digitale omgevingen (PDO). Hiermee wordt gedoeld op iedere digitale oplossing waar een burger (direct of indirect) controle over heeft: het is "zijn omgeving". Binnen Regie op Gegevens staat het beoogde effect (regie kunnen voeren over de eigen persoonsgegevens) centraal en minder de techniek. Iedere technische oplossing die invulling geeft aan dit beoogde effect, te weten regiehandelingen als inzage, correctie en delen van gegevens, past daarmee binnen de kaders van Regie op Gegevens.

In Europese wetgeving (bijv. eIDAS) wordt gesproken over Europese portemonnees voor digitale identiteit (*e-Wallet)* als technische oplossing voor burgers om regiehandelingen op hun eigen persoonsgegevens te kunnen uitvoeren. In de markt is het gebruikelijk geworden om te spreken over een Personal Data Management dienst (regiehandelingen) met bijbehorende PDM-oplossing. Hiervan zijn er inmiddels vele tientallen

beschikbaar, die alle regiehandelingen door de burger mogelijk maken. Overzichten zijn bijvoorbeeld te vinden hier (Innovalor) en hier (SIVI).



Figuur-5: PDM-Diensten Nederland inclusief authenticatievoorzieningen

7.5 Europese portemonnee voor digitale identiteit (eWallet)

In het voorgesteld (dus nog niet vastgesteld) amendement op de eIDAS-verordening wordt het idee van een *European Digital Identity Wallet* als oplossingsrichting van de in de evaluatie geschetste problemen uitgewerkt. In het oog springende noties in relatie tot Regie op Gegevens en PDM-oplossingen zijn:

1. **Uitgifte portemonnee** (Artikel 6 bis onder 2)

Europese portemonnees voor digitale identiteit worden uitgegeven:
(a) door een lidstaat;
(b) krachtens een mandaat van een lidstaat;
(c) onafhankelijk, maar erkend door een lidstaat.

2. **Functionaliteit** (Artikel 6 bis onder 3)

Met een Europese portemonnee voor digitale identiteit kunnen gebruikers:
(a) op een transparante en door de gebruiker traceerbare wijze veilig de nodige wettelijke persoonsidentificatiegegevens en elektronische attesteringen van attributen aanvragen, verkrijgen, opslaan, selecteren, combineren en delen, zodat zij zich online en offline kunnen authenticeren om openbare en particuliere onlinediensten te gebruiken;
(b) middels gekwalificeerde elektronische handtekeningen ondertekenen.

3. **Eisen aan de portemonnee (**Artikel 6 bis onder 4)

Portemonnees voor digitale identiteit zullen in het bijzonder:
(a) een gemeenschappelijke interface bieden:
1. voor gekwalificeerde en niet-gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde en niet-gekwalificeerde attesteringen van attributen of andere gekwalificeerde en niet-gekwalificeerde certificaten uitgeven met het oog op de afgifte van dergelijke attesteringen en certificaten aan de Europese portemonnee voor digitale identiteit;

2. voor vertrouwende partijen om persoonsidentificatiegegevens en elektronische attesteringen van attributen aan te vragen en te valideren;
3. om lokaal en zonder internettoegang voor de portemonnee, persoonsidentificatiegegevens, elektronische attestering van attributen of andere gegevens, zoals inloggegevens, aan vertrouwende partijen aan te bieden;
4. voor de gebruiker om met de Europese portemonnee voor digitale identiteit te kunnen communiceren en een "EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit" te kunnen weergeven;

(b) waarborgen dat verleners van vertrouwensdiensten van gekwalificeerde attesteringen van attributen geen informatie over het gebruik van die attributen kunnen ontvangen;
(c) 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;
(d) een mechanisme bieden waarmee de vertrouwende partij de gebruiker kan authenticeren en elektronische attesteringen van attributen kan ontvangen;
(e) waarborgen dat de in artikel 12, lid 4, punt d), bedoelde persoonsidentificatiegegevens uniek en permanent de daarmee verbonden natuurlijke of rechtspersonen vertegenwoordigen.

4. **Validatie van de inhoud** (Artikel 6 bis onder 5)

De lidstaten voorzien valideringsmechanismen voor de Europese portemonnees voor digitale identiteit, zodat:
(a) de authenticiteit en de geldigheid ervan kunnen worden geverifieerd;
(b) de vertrouwende partijen kunnen verifiëren dat de attesteringen van attributen geldig zijn;
(c) de vertrouwende partijen en gekwalificeerde verleners van vertrouwensdiensten de authenticiteit en de geldigheid van gekoppelde persoonsidentificatiegegevens kunnen verifiëren.

5. **Stelsel van elektronische identificatie** (Artikel 6 bis onder 6)

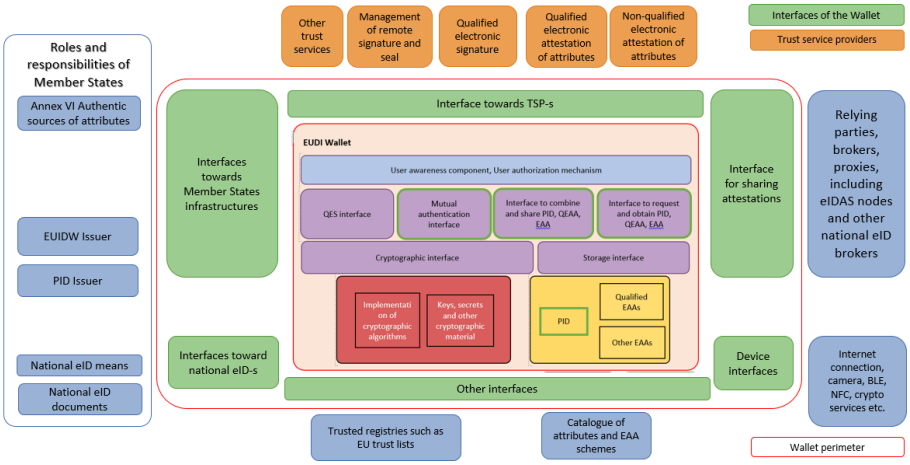
De Europese portemonnees voor digitale identiteit worden uitgegeven op grond van een aangemeld stelsel voor elektronische identificatie met een "hoog" betrouwbaarheidsniveau. Het gebruik van Europese portemonnees voor digitale identiteit is gratis voor natuurlijke personen.

6. **Eisen aan provider van portemonnee** (Artikel 6 bis onder 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, punten b) en c), is artikel 45 septies, lid 4, van overeenkomstige toepassing.

7.6 Overzicht van applicatiefuncties en interfases eWallet



8 Infrastructuur

Het is van belang om vast te stellen dat de doelstelling van Regie op Gegevens met bestaande technische middelen en procedures (wellicht niet altijd even efficiënt) gerealiseerd kunnen worden en gebeurt dan ook al. Gegevensuitwisseling via een email met een gewaarmerkte pdf is natuurlijk al lang mogelijk. Berichten met gegevens erin uitwisselen via SOAP met een XML-bericht over een beveiligde internetverbinding ook. Van meer recente datum (binnen de overheid) is gegevensuitwisseling over een beveiligde internetverbinding middels RESTful API's in JSON-formaat (of andere). De Nederlandse API-strategie voorziet in overheidsbreed ontwerp en standaarden.

Uitgangspunt voor het uitwisselen van gegevens binnen de overheid (en deels daarbuiten) is de Generieke Digitale Infrastructuur (GDI). Deze wordt geborgd in de Wet digitale overheid (Wdo) en bestaat uit standaarden, producten en voorzieningen die gezamenlijk gebruikt worden door overheden, publieke organisaties en in een aantal gevallen ook private partijen. De GDI bestaat uit herbruikbare digitale basisvoorzieningen, standaarden en producten. Hierdoor is het mogelijk om primaire processen doelmatig in te richten en te blijven ontwikkelen. De GDI vormt een dynamisch geheel dat in de toekomst – op basis van technologische ontwikkelingen of nieuwe inzichten – gewijzigd kan worden door het toevoegen van nieuwe generieke voorzieningen (of functionaliteiten van een voorziening) of door het uitfaseren van bestaande generieke voorzieningen.

De voorzieningen in de huidige GDI zijn ondergebracht in vier clusters. Elk cluster heeft een eigen functie:

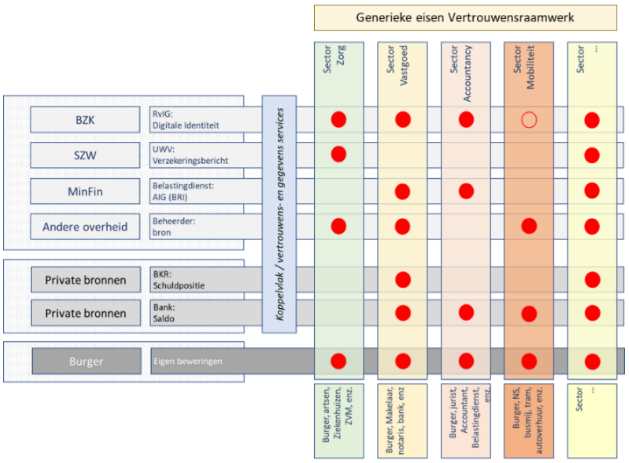
1. digitale identificatie en authenticatie (bv. eHerkenning en DigiD);
2. gegevens (basisregistraties en de bijbehorende stelselvoorzieningen);
3. interconnectiviteit (bv. netwerken en koppelstandaarden); en
4. dienstverlening (bv. het digitaal ondernemersplein en de berichtenbox).

De GDI vormt uiteindelijk geen op zichzelf staand geheel en maakt deel uit van een meer omvattende digitale nationale, Europese en zelfs deels mondiale infrastructuur, bestaande uit een ecosysteem van technologieën, protocollen, hardware, software en content.

9 Governance: vertrouwensraamwerk

In de inleiding is al gesteld dat, om de doelstellingen van Regie op Gegevens te realiseren, in de toekomstige oplossing twee fasen te onderkennen zijn, te weten:

1. ontsluiten (ter beschikking stellen) van de persoonsgegevens aan burgers (of met volmacht aan dienstverleners) uit bronnen van de overheid, eventueel met gebruik making van gegevensservices en vertrouwensservices;
2. gebruik van deze persoonsgegevens door burgers in hun relatie met dienstverleners (dus nadat ze door de overheid ter beschikking gesteld zijn).



In de tweede fase is de overheid partij in een in een samenwerking tussen publieke en private partijen waarin de overheidsbron een van de bronnen is binnen de sectorale samenwerking. Burgers, dienstverleners, publieke bronhouders, private bronhouders en diverse intermediairs zullen tot samenwerking moeten komen. Dit zal enerzijds plaatsvinden op basis van wettelijke kaders en verplichtingen en anderzijds binnen de vrije onderhandelingsruimte van partijen vallen. Doel is in ieder geval tot een vorm van samenwerking te komen waarin partijen elkaar kunnen vertrouwen: een vertrouwensraamwerk.

Een *Trust Framework* ('Vertrouwensraamwerk') is een algemene term die vaak wordt gebruikt om:

1. een juridisch afdwingbare reeks specificaties, regels en overeenkomsten te beschrijven die
2. een meerpartijenstelsel regelen dat is opgezet voor een gemeenschappelijk doel,
3. ontworpen voor het uitvoeren van specifieke transacties tussen een groep van deelnemers,
4. en gebonden aan een gemeenschappelijke reeks vereisten.

Voorbeelden van systemen met meerdere partijen die vertrouwensraamwerk gebruiken, zijn onder meer creditcardsystemen (zoals Visa of MasterCard), elektronische betalingssystemen (zoals SWIFT

of NA-CHA), het domeinnaamregistratiesysteem (ICANN) en identiteitssystemen.

Een vertrouwensraamwerk bestaat dus uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en zorgaanbieders op een veilige en efficiënte manier kunnen samenwerken. Partijen die deelnemen committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken. Een canvas voor zo'n vertrouwensraamwerk voor het delen van gegevens is uitgewerkt in Data Sharing Canvas. Binnen Regie op Gegevens wordt het vertrouwensraamwerk uitgewerkt in het *Vertrouwensraamwerk Regie op Gegevens*.

Bijlage A Definities

Begrip	Definitie
Dienstverlener	De dienstverlener is iedere private partij die een dienst levert.
Attribuut	een eigenschap, kenmerk of kwaliteit van een natuurlijke of rechtspersoon of een entiteit, in elektronisch formaat
Attest	Een attest is een elektronisch bewijs, een verklaring die een bewering versterkt, ondersteunt, wettigt.
Elektronische attestering van attributen	een attestering in elektronisch formaat aan de hand waarvan attributen kunnen worden geauthenticeerd
Vertrouwensraamwerk	een juridisch afdwingbare reeks specificaties, regels en overeenkomsten te beschrijven die een meerpartijenstelsel regelen dat is opgezet voor een gemeenschappelijk doel, ontworpen voor het uitvoeren van specifieke transacties tussen een groep van deelnemers, en gebonden aan een gemeenschappelijke reeks vereisten.
Europese portemonnee voor digitale identiteit	een product en dienst die de gebruiker in staat stelt identiteitsgegevens, inloggegevens en attributen met betrekking tot zijn/haar identiteit 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
Burger	Onder burger wordt hier verstaan iedere natuurlijke persoon die ingezetene is in Nederland (zoals opgenomen in de BRP) en iedere natuurlijke persoon die opgenomen is in het Register Niet-Ingezetenen RNI (niet-ingezetene met een relatie met de Nederlandse overheid).
Overheid	Iedere overheidsorganisatie die persoonsgegevens over een burger administreert die door die burger ingezien mogen worden.
Overeenkomst	Een overeenkomst is een meerzijdige rechtshandeling, waarbij een of meer partijen jegens een of meer andere een verbintenis aangaan (art. 6:213 lid 1 BW).

Offerte	De overeenkomst komt tot stand door een aanbod en de aanvaarding daarvan (art. 6:217 lid 1 BW). De offerte is het aanbod.
Afspraak	De afspraak is een overeenkomst tussen een dienstverlener en een overheidsorganisatie waarin deze zich verbindt om onder bepaalde voorwaarden (zoals een geldige machtiging) bepaalde gegevens over een burger conform bepaalde leveringsvoorwaarden aan die dienstverlener te leveren.
Bestelling	Een bestelling is verzoek op basis van een afspraak tot het leveren van bepaalde gegevens over een bepaalde burger.
Machtiging	Een toestemming van de burger aan de dienstverlener om namens hem gegevens over hem in te winnen bij de overheid.
Persoonsgegeven	Een persoonsgegeven is alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 4 AVG). Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens.
Bijzonder gegeven	Bijzondere persoonsgegevens zijn gegevens over iemands: • ras of etnische afkomst; • politieke opvattingen; • godsdienst of levensovertuiging; • lidmaatschap van een vakbond; • genetische of biometrische gegevens met oog op unieke identificatie; • gezondheid; • seksuele leven; • strafrechtelijk verleden. Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is.
Gevoelige gegevens	*Gevoelige gegevens* is geen officieel AVG-begrip, maar kent wel AVG-verplichtingen vanwege risico's voor de betrokkene.
Persoons identificerende gegevens	Gegevens die het mogelijk maken de *identiteit* van een persoon te achterhalen, te weten geslachtsnaam, voornamen, geboortedatum en woonplaats (vgl. o.a. definitie uit Donorwet kunstmatige bevruchting)

Identificeerbaar	Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Eigen bewering	Onder bewering wordt hier de neutrale en niet-geverifieerde status van een gegeven verstaan en deze kan dus waar of niet waar zijn. Een eigen bewering is een bewering die de burger zelf doet.
Derden bewering	Een derden bewering is een bewering die (in deze context) de overheid over een burger doet.
Feit	Zodra een bewering geverifieerd en/of geaccepteerd is, krijgt dit gegeven de status van feit en is daarmee uitgangspunt voor het vervolg van het proces
Waarmerk	Een waarmerk is een extra kenmerk van (een set van) gegeven(s) waaruit blijkt dat de uitgever van het waarmerk (meestal na onderzoek) de juistheid van het gegeven onderschrijft ("voor waar aanmerkt").
Algoritme	Een algoritme is een set instructies om een bepaalde taak uit te voeren. Aan de hand van data die in het algoritme worden ingevoerd, wordt in verschillende stappen toegewerkt naar het beoogde eindresultaat, bijvoorbeeld het toekennen van een toeslag. Op basis van dat resultaat kan men dan actie ondernemen (toeslag wel of niet toekennen). De precieze stappen die worden doorlopen verschillen per algoritme. In het algemeen geldt dat deze stappen variabelen bevatten, bijvoorbeeld de hoogte van het inkomen als relevante factor voor het toekennen van de toeslag. Er bestaan verschillende typen algoritmes. Het algoritme voor het toekennen van een toeslag heeft doorgaans het karakter van een eenvoudige beslisboom (rule based) met een beperkt aantal variabelen en drempelwaarden, bijvoorbeeld dat om voor een toeslag in aanmerking te komen het inkomen lager dient te zijn dan bedrag x. Een algoritme kan ook meer complex zijn en bijvoorbeeld op basis van een aantal casussen voorspellingen doen over nog niet bekende gevallen (case based) of gebruikt worden voor gezichts- of objectherkenning. We betreden dan de wereld van machine learning, deep learning, zelflerende algoritmes en kunstmatige intelligentie.
Brongegeven	Brongegeven is het gegeven zoals deze zich in de administratie van de overheid bevindt.

Afgeleid gegeven	Een afgeleid gegeven is een gegeven dat verkregen wordt door de toepassing van regels (algoritmen) op brongegevens of andere afgeleide gegevens. Afgeleid gegeven en conclusie worden hier als synoniem gebruikt.
Gegevenscatalogus	Een gegevenscatalogus is een beschrijving van zowel bron- als afgeleide gegevens die door de (in casu) overheid geleverd kunnen worden. Deze beschrijving bevat tenminste per gegeven de metadata, context, semantiek, uitspraken over kwaliteit en levercondities. Een voorbeeld van zo'n gegevenscatalogus is de Stelselcatalogus.
Persoonlijke Digitale Omgeving	Een persoonlijke digitale omgeving is in deze context iedere digitale toepassing met toegangsfunctie waar een burger of dienstverlener gegevens in kan plaatsen en beheren.
Vertegenwoordiger	Burgers kunnen zich (vrijwillig of gedwongen, middellijk of onmiddellijk) laten vertegenwoordigen door iedere andere burger (particulier of professioneel).

Bijlage B Overzicht van relevante EU wet- & regelgeving

VERKLARINGEN

18 november 2009 - Verklaring van Malmö over moderniseren van publieke administraties en cross-border diensten eServices, eProcurement en eID

6 oktober 2017 - Verklaring van Tallinn over eGovernment

8 december 2020 - Verklaring van Berlijn over de digitale samenleving en een waarde gebaseerde digitale overheid

26 januari 2022 (CONCEPT) - Europese verklaring over digitale rechten en beginselen voor het digitale decennium

STRATEGIEËN

11 december 2019 – De Europese Green Deal

19 februari 2020 - Een Europese datastrategie

19 februari 2020 – De digitale toekomst van Europa vormgeven

16 december 2020 – Een Europese strategie voor cybersecurity

02 februari 2022 – Een Europese strategie voor Standaardisatie

RICHTLIJNEN

Richtlijn 2000/31/EG
08 juni 2000 - Bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt

Richtlijn 2000/31/EG
08 juni 2000 - Bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (Richtlijn inzake elektronische handel)

Richtlijn 2002/58/EG
12 juli 2002 - Verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (ePrivacy)

Richtlijn 2006/123/EG
12 december 2006 – Diensten op de interne markt

Richtlijn 2007/2/EG
14-03-2007 - Oprichting van een infrastructuur voor ruimtelijke informatie in de Europese Gemeenschap

Richtlijn 2008/114/EG
08 december 2008 - De identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren

Richtlijn 2011/83/EU
25 oktober 2011 - Consumentenrechten

Richtlijn 2013/40/EU
12 augustus 2013 - Aanvallen op informatiesystemen

Richtlijn 2014/24/EU
26 februari 2014 - Het plaatsen van overheidsopdrachten

Richtlijn 2014/25/EU
24 februari 2014 - Het plaatsen van opdrachten in de sectoren water- en energievoorziening, vervoer en postdiensten

Richtlijn 2015/1535
09 september 2015 - Een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij

Richtlijn 2015/2366
25 november 2015 - Betalingsdiensten in de interne markt (PSD 2)

Richtlijn 2016/680
27 april 2016 - Bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens

Richtlijn 2016/943
08 juni 2016 - Bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan

Richtlijn 2016/1148
06 juli 2016 - Maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS)

Richtlijn 2019/882
14 april 2019 - Toegankelijkheidsvoorschriften voor producten en diensten

Richtlijn 2019/1024
20 juni 2019 - Open data en het hergebruik van overheidsinformatie

Richtlijn in voorbereiding
16 december 2020 (CONCEPT) - De veerkracht van kritieke entiteiten (NIS2)

Richtlijn in voorbereiding
Aangekondigd - Richtlijn Data Governance

VERORDENINGEN

Verordening (EU) 910/2014
23 juli 2014 - Elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS)

Verordening (EU) 2016/679
27 april 2016 - Algemene Verordening Gegevensbescherming (AVG | GDPR)

Verordening (EU) 2018/1724
02 oktober 2018 - Oprichting van één digitale toegangspoort voor informatie, procedures en diensten voor ondersteuning en probleemoplossing (Single Digital Gateway)

Verordening (EU) 2018/1725
23 oktober 2018 - 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

Verordening (EU) 2018/1807
14 november 2018 - Vrije verkeer van niet-persoonsgebonden gegevens

Verordening (EU) 2019/881
17 april 2019 - De certificering van de cyberbeveiliging van informatie- en communicatietechnologie

Verordening in voorbereiding
25 oktober 2020 - Data Governance Verordening (DGA)

Verordening in voorbereiding
10 januari 2017 (CONCEPT) - Eerbiedigen van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie (ePrivacy Act)

Verordening in voorbereiding
24 september 2020 (CONCEPT) – Markten in cryptoactiva (MiCA)

Verordening in voorbereiding
03 juni 2021 (CONCEPT) - Verordening Europees Kader voor een digitale identiteit (eIDAS-2)

Verordening in voorbereiding
21 april 2021 (CONCEPT) - Verordening inzake Artificiële Intelligentie (AI-act)

Verordening in voorbereiding

15 december 2021 (CONCEPT) - Verordening inzake Digitale Diensten (DSA)

Verordening in voorbereiding
15 december 2021 (CONCEPT) - Verordening inzake Digitale Markten (DMA)

Verordening in voorbereiding
23 februari 2022 (CONCEPT) - Data Verordening (DA)

Bijlage C Korte toelichting per Europese regeling

Algemene verordening gegevensbescherming (AVG)
Onderwerp en toepassingsgebied
De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. De beginselen en regels betreffende de bescherming van natuurlijke personen bij de verwerking van hun persoonsgegevens dienen, ongeacht hun nationaliteit of verblijfplaats, in overeenstemming te zijn met hun grondrechten en fundamentele vrijheden, met name met hun recht op bescherming van persoonsgegevens. Deze verordening beoogt bij te dragen aan de totstandkoming van een ruimte van vrijheid, veiligheid en recht en van een economische unie, alsook tot economische en sociale vooruitgang, de versterking en de convergentie van de economieën binnen de interne markt en het welzijn van natuurlijke personen. Deze verordening stelt regels vast betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens. Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. Het vrije verkeer van persoonsgegeven in de Europese Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

Status

Titel
Verordening 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

EU-code
Verordening (EU) 2016/679

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2012/11/FINAL	25 januari 2012	**Goedgekeurde handeling**	DG JUST
	Datum inwerkingtreding: 27 april 2016		

ePrivacyverordening
Onderwerp en toepassingsgebied
Artikel 7 van het Handvest van de grondrechten van de Europese Unie beschermt het grondrecht van eenieder op eerbiediging van zijn privéleven, zijn familie- of gezinsleven, zijn woning en zijn communicatie. Eerbiediging van de privacy van de communicatie is een essentieel onderdeel van dit recht. De vertrouwelijkheid van de elektronische communicatie zorgt ervoor dat de informatie die tussen partijen worden uitgewisseld en de externe aspecten van die communicatie, waaronder het tijdstip waarop de informatie is verzonden, van waar, naar wie, niet aan anderen worden meegedeeld dan aan de partijen die bij de communicatie

betrokken zijn. Het beginsel van vertrouwelijkheid moet van toepassing zijn op huidige en toekomstige communicatiemiddelen, met inbegrip van gesprekken, internettoegang, applicaties voor instant messaging, emailverkeer, internettelefoon en persoonlijke berichten die via de sociale media worden verzonden. Deze verordening voorziet in regels betreffende de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke en rechtspersonen in de levering en het gebruik van elektronische communicatiediensten, en in het bijzonder het recht op eerbiediging van het privéleven en de communicatie en de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Deze verordening waarborgt het vrije verkeer van elektronische communicatiegegevens en elektronische communicatiediensten in de Europese Unie, dan niet mag worden beperkt of verboden om redenen die verband houden met het eerbiedigen van het privéleven en de communicatie van natuurlijke en rechtspersonen en de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. De bepalingen van deze verordening vormen een specificatie van en een aanvulling op Verordening (EU) 2016/679, de Algemene Verordening Gegevensbescherming.

Status

Titel

Verordening met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG

EU-code

-

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2017/10/FINAL	10 januari 2017	**Eerste lezing door de Raad**	DG CNECT
	Datum inwerkingtreding:		
	-		

Data verordening | Data Act (DA)

Onderwerp en toepassingsgebied

De afgelopen jaren hebben datagestuurde technologieën alle sectoren van de economie grondig getransformeerd. Met name van de verspreiding van producten die verband houden met het internet der dingen heeft het volume en de potentiële waarde van data voor consumenten, bedrijven en de samenleving vergroot. Hoogwaardige en interoperabele data uit verschillende domeinen vergroten het concurrentievermogen en de innovatie en zorgen voor duurzame economische groei. Dezelfde dataset kan voor verschillende doeleinden onbeperkt worden gebruikt en hergebruikt, zonder dat dit invloed heeft op de kwaliteit of kwantiteit ervan. Deze verordening stelt geharmoniseerde regels vast voor het beschikbaar stellen van data die zijn gegenereerd door het gebruik van een product of een gerelateerde dienst door de gebruiker van dat product of die dienst, het beschikbaar stellen van data door datahouders aan data-ontvangers, en het beschikbaar stellen van data door datahouders aan overheidsinstanties of EU-instellingen, -agentschappen of -orgaan, indien er een uitzonderlijke noodzaak bestaat voor de uitvoering van een taak van algemeen belang.

Status

Titel
Verordening betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data

EU-code
-

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2022/68/FINAL	23 februari 2022	**Eerste lezing door de Raad**	DG CNECT

Datum inwerkingtreding:
-

Datagovernance verordening | Data Governance Act (DGA)

Onderwerp en toepassingsgebied

Het Verdrag betreffende de werking van de Europese Unie (VWEU) voorziet in de totstandbrenging van een interne markt en de invoering van een systeem waardoor wordt verzekerd dat de mededinging binnen de interne markt niet wordt vervalst. De vaststelling van gemeenschappelijke regels en praktijken in de lidstaten met betrekking tot de ontwikkeling van een kader inzake datagovernance draagt bij tot he bereiken van die doelstellingen, met volledige inachtneming van de grondrechten. Het moet ook de versterking van de open strategische autonomie van de Europese Unie waarborgen, en tegelijk het internationale vrije verkeer van gegevens bevorderen. Deze verordening bevat voorwaarden voor het hergebruik, in de Europese Unie, van bepaalde gegevenscategorieën die in het bezig zijn van openbare lichamen. Deze verordening bevat verder een meldings- en toezichtskader voor het aanbieden van gegevensdelingsdiensten en een kader voor vrijwillige registratie van entiteiten die voor altruïstische doeleinden beschikbaar gestelde gegevens verzamelen en verwerken.

Status

Titel
Verordening betreffende Europese datagovernance

EU-code
Verordening (EU) 2022/868

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2022/767/FINAL	23 november 2022	**In afwachting van kennisgeving**	DG CNECT

Datum inwerkingtreding:
23 juni 2022

Wet inzake digitale diensten | Digital Services Act (DSA)

Onderwerp en toepassingsgebied
Diensten van de informatiemaatschappij en met name tussenhandelsdiensten zijn een belangrijk onderdeel geworden van de economie en het dagelijks leven van de burgers van de Europese Unie. Nieuwe en innovatieve bedrijfsmodellen en diensten, zoals sociale onlinenetwerken en -marktplaatsen, hebben het mogelijk gemaakt voor zakelijke gebruikers en consumenten om op nieuwe manieren informatie te verstrekken en te verkrijgen en transacties te verrichten. Een

meerderheid van de burgers van de Europese Unie maakt nu dagelijks gebruik van deze diensten. De digitale transformatie en het toegenomen gebruik van deze diensten hebben echter ook nieuwe risico's en uitdagingen met zich meegebracht, zowel voor individuele gebruikers als voor de samenleving als geheel. Deze verordening stelt geharmoniseerde regels vast over het aanbieden van tussenhandelsdiensten op de interne markt. Deze verordening bepaald een kader voor de voorwaardelijke vrijstelling van aansprakelijkheid van aanbieders van tussenhandelsdiensten, de regels over verplichtingen inzake gepaste zorgvuldigheid op maat van bepaalde specifieke categorieën van aanbieders van tussenhandelsdiensten en regels over de uitvoering en handhaving van deze verordening, ook met betrekking tot de samenwerking van en coördinatie tussen bevoegde autoriteiten.

Status

Titel

Verordening betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG

EU-code

-

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2022/825/FINAL	15 december 2020	**Eerste lezing door het Parlement**	DG CNECT
	Datum inwerkingtreding:		
	-		

Wet inzake digitale markten| Digital Markets Act (DMA)

Onderwerp en toepassingsgebied

Digitale diensten in het algemeen en onlineplatforms in het bijzonder spelen een steeds belangrijkere rol in de economie, met name op de interne markt, doordat zij in de Europese Unie nieuwe zakelijke kansen bieden en grensoverschrijdende handel vergemakkelijken. Deze verordening stelt geharmoniseerde regels vast voor betwistbare en eerlijke markten in de digitale sector van de hele Europese Unie waarop poortwachters aanwezig zijn. Deze verordening is van toepassing op kernplatformdiensten die door poortwachters worden verleend of aangeboden aan zakelijke gebruikers die in de Europese Unie zijn gevestigd, of aan eindgebruikers die in de Europese Unie zijn gevestigd of zich aldaar bevinden, ongeacht de plaats van vestiging of de verblijfplaats van de poortwachters en ongeacht het recht dat anders op de dienstverlening van toepassing zou zijn.

Status

Titel

Verordening over betwistbare en eerlijke markten in de digitale sector

EU-code

-

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2022/842/FINAL	16 december 2020	**Eerste lezing door het Parlement**	DG CNECT
	Datum inwerkingtreding:		
	-		

Elektronische identificatie & vertrouwensdiensten voor elektronische transacties eIDAS

Onderwerp en toepassingsgebied

Het opbouwen van vertrouwen in de online-omgeving is essentieel voor economische en sociale ontwikkeling. Een gebrek aan vertrouwen, met name ten gevolge van een ogenschijnlijk gebrek aan rechtszekerheid, leidt ertoe dat consumenten, bedrijven en overheden aarzelen om transacties elektronisch uit te voeren en van nieuwe diensten gebruik te maken. Deze verordening heeft tot doel het vertrouwen in elektronische transacties in de interne markt te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten, e-business en elektronische handel in de Unie te verhogen. Deze verordening stelt de voorwaarden vast waaronder lidstaten elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen erkennen die onder een aangemeld stelsel voor elektronische identificatie van een andere lidstaat vallen. Verder stelt deze verordening regels vast voor vertrouwensdiensten, met name voor elektronische transacties, en stelt een juridisch kader vast voor elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, diensten voor elektronisch aangetekende bezorging en certificatendiensten voor websiteauthenticatie.

Status

Titel

Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

EU-code

Verordening (EU) 910/2014

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2012/238/FINAL	04 juni 2012	**Goedgekeurde handeling**	DG INFSO
	Datum inwerkingtreding:		
	23 juli 2014		

Een Europees kader voor een digitale identiteit| eIDAS

Onderwerp en toepassingsgebied

In de mededeling '*De digitale toekomst van Europa vormgeven*' van de Commissie van 19 februari 2020 wordt een herziening van Verordening (EU) nr. 910/2014 aangekondigd om de doeltreffendheid ervan te verbeteren, de voordelen ervan voor particulieren uit te breiden en betrouwbare digitale identiteiten voor alle Europeanen te bevorderen. In zijn conclusies van 1-2 oktober 2020 heeft de Europese Raad de Commissie opgeroepen tot de ontwikkeling van een EU-breed kader voor beveiligde openbare elektronische identificatie, inclusief interoperabele digitale handtekeningen, om mensen controle over hun online identiteit en -gegevens te geven en toegang tot openbare, particuliere en grensoverschrijdende digitale diensten mogelijk te maken. Een meer geharmoniseerde benadering van digitale identificatie moet de risico's en de kosten van de huidige versnippering vanwege uiteenlopende nationale oplossingen verkleinen en de eengemaakte markt versterken door burgers, andere ingezetenen krachtens nationaal recht en ondernemingen zich op een gemakkelijke en uniforme manier in de hele Unie online te laten identificeren. Iedereen moet veilig toegang kunnen hebben tot openbare en particuliere diensten en kunnen vertrouwen op een verbeterd ecosysteem voor vertrouwensdiensten en op geverifieerde identiteitsbewijzen en attesteringen van attributen, zoals een universitair diploma, die overal in de Unie wettelijk worden erkend en aanvaard. Het Europese kader voor een digitale identiteit beoogt een verschuiving van het gebruik van nationale digitale-identiteitsoplossingen naar de levering van elektronische attesteringen van attributen die op Europees niveau geldig zijn. Aanbieders van elektronische attesteringen van attributen moeten profiteren van duidelijke en uniforme regels en overheidsdiensten moeten kunnen vertrouwen op elektronische documenten in een bepaald formaat. Deze verordening is gericht op het goede functioneren van de interne markt, en op het bieden van een adequaat niveau van beveiliging van elektronische identificatiemiddelen en vertrouwensdiensten. Deze verordening stelt de voorwaarden vast waaronder de lidstaten elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen aanbieden en erkennen die onder een aangemeld stelsel voor elektronische identificatie van een andere lidstaat vallen. Ook stelt deze verordening regels voor vertrouwensdiensten, met name voor elektronische transacties. Verder stelt deze verordening 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, het beheer van middelen voor het aanmaken van elektronische handtekeningen en zegels op afstand, en elektronische registers. Tenslotte stelt deze verordening de voorwaarden voor de uitgifte van Europese portemonnees voor digitale identiteit door de lidstaten.

Status

Titel

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

EU-code

-

Commissievoorstel code:	Datum voorstel:	Status:	EU-DG
COM/2021/281/FINAL	03 juni 2021	**Eerste lezing door de Raad**	DG CNECT

Datum inwerkingtreding:

-

Bijlage D Rechten en plichten burgers per EU-regeling

Burger		
Natuurlijk persoon		
Regeling	Artikel	Rechten/plichten
AVG	7, lid 3	Recht zijn toestemming voor de verwerking van zijn persoonsgegevens ten alle tijde in te trekken
	13, lid 2, c)	Recht de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid.
	13, lid 2, d)	Recht om toestemming te allen tijde in te trekken
	13, lid 2, e)	Recht een klacht in te dienen bij een toezichthoudende autoriteit
	15, lid 1	Recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van de persoonsgegevens en 8 informatie-typen.
	15, lid 2	Recht om in kennis te worden gesteld van de passende waarborgen inzake de doorgifte aan een derde land of een internationale organisatie.
	16	Recht om onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen
	16	Recht om vervolledigend van onvolledige persoonsgegevens te verkrijgen.
	17	Recht op gegevenswissing (recht op vergetelheid)
	18	Recht op beperking van de verwerking
	20	Recht op overdraagbaarheid van gegevens
	21	Recht op bezwaar
	22	Recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit.
	77	Recht om klacht in te dienen bij een toezichthoudende autoriteit
	79	Recht om een doeltreffende voorziening in rechte in te stellen tegen de verwerkingsverantwoordelijke of een verwerker
	80	Recht op het opdrachtgeven aan een externe om namens hem een klacht in te dienen.
ePrivacy	9, lid 3	Recht om toestemming voor de verwerking van elektronische communicatiegegevens te allen tijde in te trekken
	10, lid 2	Plicht om voor de voortzetting van de installatie van software een privacy-instelling te aanvaarden.
	16, lid 2	Recht om duidelijk en expliciet in de gelegenheid gesteld te zijn om kosteloos en op gemakkelijke wijze bezwaar te maken tegen het gebruik van elektronische contactgegevens t.b.v. direct marketing.
	22	Recht op schadevergoeding en aansprakelijkheid

DA	Art. 14, lid 1	Plicht: Een datahouder stelt op verzoek data ter beschikking aan een overheidsinstantie of een EU-instelling, -agentschap of -orgaan wanneer is aangetoond dat er een uitzonderlijke noodzaak bestaat om de gevraagde data te gebruiken.
	Art 18, lid 1t/m 6	Plicht: datahouder die een verzoek om toegang tot data ontvangt bij noodsituaties, stelt de data onverwijld ter beschikking van de verzoekende overheidsinstantie of EU-instelling, -agentschap of -orgaan. Recht: de datahouder kan het verzoek afwijzen of verzoeken om wijziging van het verzoek, en dit binnen vijf werkdagen na ontvangst van een verzoek om de data die noodzakelijk zijn om te reageren op een algemene noodsituatie, en binnen 15 werkdagen in andere gevallen van uitzonderlijke noodzaak, om een van de volgende redenen: de data zijn niet beschikbaar, het verzoek voldoet niet aan de voorwaarden van artikel 17, lid 1 en 2. In geval van een verzoek om data die nodig zijn om te reageren op een algemene noodsituatie, kan de datahouder het verzoek ook afwijzen of vragen om wijziging ervan, indien de datahouder de gevraagde data reeds heeft verstrekt in antwoord op een eerder ingediend verzoek met hetzelfde doel door een andere overheidsinstantie of een andere EU-instelling, -agentschap of -orgaan en de datahouder niet in kennis is gesteld van de vernietiging van de data.
	Art. 20, lid 1	Plicht: data die beschikbaar worden gesteld met als doel te reageren op een algemene noodsituatie overeenkomstig artikel 15, punt a), worden kosteloos verstrekt.
	Art. 32, lid 1	Recht: om individueel of, in voorkomend geval, collectief een klacht in te dienen bij de relevante bevoegde autoriteit indien zij van mening zijn dat hun rechten uit hoofde van deze verordening zijn geschonden.
	Art. 32, lid 2.	Recht: de bevoegde autoriteit waarbij de klacht is ingediend, stelt de klager in kennis van het verloop van de procedure en van het genomen besluit
DGA	2 onder 6	"gegevensgebruiker": een *natuurlijke persoon* of rechtspersoon die rechtmatige *toegang* heeft tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens en gemachtigd is die gegevens voor commerciële of niet-commerciële doeleinden te gebruiken;
	2 onder 8	"toegang": verwerking door een gegevensgebruiker van gegevens die zijn verstrekt door een gegevenshouder, overeenkomstig specifieke technische, juridische of organisatorische voorschriften, zonder dat dit noodzakelijkerwijs gepaard gaat met het doorgeven of downloaden van die gegevens;
	24	klachtrecht
	25	Recht op een doeltreffende voorziening in rechte
DSA	Art 2 c	"consument": een natuurlijke persoon die handelt voor doeleinden die buiten zijn bedrijfs-, handels- of beroepsactiviteit vallen;
	Artikel 9	*Bevelen om informatie te verstrekken* 1. Wanneer aanbieders van tussenhandelsdiensten een door de relevante nationale gerechtelijke of administratieve autoriteiten op basis van het van toepassing zijnde EU-recht of intern recht overeenkomstig het EU-recht uitgegeven bevel ontvangen om specifieke informatie te verstrekken over een of meerdere specifieke afnemers van de dienst, brengen zij de uitgevende autoriteit onmiddellijk op de hoogte van de ontvangst van het bevel en van het gevolg dat zij hieraan hebben gegeven.
	Artikel 12	*Algemene voorwaarden* 1. Aanbieders van tussenhandelsdiensten nemen informatie over eventuele beperkingen die zij aan het gebruik van hun dienst opleggen met betrekking tot door de afnemers van de dienst verstrekte informatie, op in hun algemene voorwaarden 2. ….de rechten en gewettigde belangen van alle betrokken partijen, waaronder de van toepassing zijnde, in het Handvest verankerde grondrechten van de afnemers van de dienst.
	Artikel 13	*Rapportageverplichtingen inzake transparantie voor aanbieders van tussenhandelsdiensten* • de inhoudsmoderatie die is uitgevoerd op eigen initiatief van de dienstverleners, met inbegrip van het aantal en de soort genomen maatregelen die een invloed hebben op

		de beschikbaarheid, zichtbaarheid en toegankelijkheid van door de afnemers van de dienst verstrekte informatie en • de mogelijkheid van de afnemers om informatie te verstrekken, ingedeeld per soort reden en grondslag om deze maatregelen te nemen;
	Artikel 15	*Motivering* 1. Wanneer een aanbieder van hostingdiensten besluit toegang tot specifieke, door de afnemers van de dienst verstrekte informatie te verwijderen of uit te schakelen, …, brengt hij de afnemer, ten laatste op het ogenblik van de verwijdering of uitschakeling van toegang, op de hoogte van het besluit en geeft hij een duidelijke en specifieke motivering voor dat besluit. f. informatie over de beroepsmogelijkheden waarover de afnemer van de dienst met betrekking tot het besluit beschikt, met name via interne klachtenafhandelingsmechanismen, buitengerechtelijke geschillenbeslechting en hoger beroep
	Artikel 17	*Intern klachtenafhandelingssysteem* 1. Onlineplatforms verstrekken afnemers van de dienst gedurende een periode van ten minste zes maanden na het in dit lid genoemde besluit, toegang tot een doeltreffend intern klachtenafhandelingssysteem, dat het elektronisch en gratis indienen mogelijk maakt van klachten tegen de volgende besluiten die het onlineplatform heeft genomen op basis van het feit dat de door de afnemers verstrekte informatie illegale inhoud is of onverenigbaar is met zijn algemene voorwaarden:
	Artikel 18	*Buitengerechtelijke geschillenbeslechting* Afnemers van de in artikel 17, lid 1, bedoelde diensten mogen een overeenkomstig lid 2 gecertificeerd orgaan voor buitengerechtelijke geschillenbeslechting kiezen om geschillen met betrekking tot deze besluiten op te lossen, waaronder klachten die niet konden worden opgelost via het in dat artikel bedoelde interne klachtenafhandelingssysteem. Als het orgaan het geschil in het voordeel van de afnemer van de dienst beslecht, betaalt het onlineplatform de afnemer alle vergoedingen en andere redelijke uitgaven terug die de afnemer heeft betaald of moet betalen in verband met de geschillenbeslechting.
	Artikel 20	*Maatregelen en bescherming tegen misbruik* 1. Onlineplatforms schorten, voor een redelijke periode en na een voorafgaande waarschuwing, de verlening van hun diensten op aan afnemers van de dienst die frequent manifest illegale inhoud verstrekken. 2. Onlineplatforms schorten, voor een redelijke periode en na een voorafgaande waarschuwing, de verwerking op van berichten en klachten …. 3. Onlineplatforms beoordelen geval per geval en tijdig, zorgvuldig en objectief of een afnemer, persoon, entiteit of klager zich schuldig maakt aan het in de leden 1 en 2 vermelde misbruik
	Artikel 22	*Traceerbaarheid van handelaren* 1. Wanneer een onlineplatform consumenten in staat stelt op afstand gesloten overeenkomsten met handelaren aan te gaan, zorgt het ervoor dat handelaren zijn diensten alleen kunnen gebruiken ter promotie van berichten over of voor het aanbieden van producten of diensten aan consumenten in de EU als het onlineplatform vóór het gebruik van zijn diensten de volgende informatie heeft verkregen: 2.
DMS	Art.5 c)	de poortwachter laat zakelijke gebruikers toe aanbiedingen aan eindgebruikers die via de kernplatformdienst zijn verworven, te promoten en contracten met deze eindgebruikers te sluiten, ongeacht of zij daarvoor gebruikmaken van de kernplatformdiensten van de poortwachter, en laat eindgebruikers toe om via de kernplatformdiensten van de poortwachter toegang te krijgen tot en gebruik te maken van inhoud, abonnementen, functies of andere artikelen door middel van de softwaretoepassing van een zakelijke gebruiker, wanneer deze artikelen door de eindgebruikers van de desbetreffende zakelijke gebruiker zijn gekocht zonder gebruik te maken van de kernplatformdiensten van de poortwachter;
	Art.6 h)	de poortwachter zorgt voor effectieve portabiliteit van gegevens die zijn gegenereerd door de activiteit van een zakelijke gebruiker of eindgebruiker, en stelt met name instrumenten ter beschikking aan eindgebruikers om de gegevensportabiliteit te vergemakkelijken, in overeenstemming met Verordening (EU) 2016/679 <AVG>, onder meer door continue toegang in real time te bieden;

	Art.6 i)	de poortwachter biedt zakelijke gebruikers of door een zakelijke gebruiker gemachtigde derden kosteloos en op doeltreffende, hoogwaardige wijze continue en in real time toegang tot en gebruik van geaggregeerde of niet- geaggregeerde gegevens die worden verstrekt voor of gegenereerd in het kader van het gebruik van de betrokken kernplatformdiensten door die zakelijke gebruikers en de eindgebruikers die betrokken zijn bij de producten of diensten die door die zakelijke gebruikers worden geleverd; de poortwachter maakt de toegang tot en het gebruik van persoonsgegevens alleen mogelijk indien deze rechtstreeks verband houden met het gebruik door de eindgebruiker van producten of diensten die door de betrokken zakelijke gebruiker worden aangeboden via de betrokken kernplatformdienst, en wanneer de eindgebruiker voor een dergelijke uitwisseling toestemming geeft in de zin van Verordening (EU) 2016/679 <AVG>;
eIDAS	-	-
eIDAS 2 (*Europees kader voor digitale identiteit*)	Artikel 6, bis, 6	Het gebruik van Europese portemonnees voor digitale identiteit is gratis voor natuurlijke personen.
	Artikel 6, bis, 7	De gebruiker heeft volledige controle over de Europese portemonnee voor digitale identiteit.
	Artikel 6, bis, 10	De Europese portemonnee voor digitale identiteit wordt toegankelijk gemaakt voor personen met een handicap overeenkomstig de toegankelijkheidsvoorschriften van bijlage I bij Richtlijn (EU) 2019/882.

Bijlage E Rechten en plichten bronhouders per EU-regeling

Bronhouder		
Regeling	Artikel	Rechten/plichten
AVG	2, lid d	Verordening niet van toepassing i.h.k.v. voorkoming, onderzoek, opsporing, vervolging van strafbare feiten
	9, lid 2, f)	Recht om de verwerking te doen van bijzondere categorieën van persoonsgegevens indien noodzakelijk voor de instelling, uitoefening of onderbouwing van de rechtsverordening of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.
	7, lid 1	Plicht van de *verwerkingsverantwoordelijke* om aan te tonen dat de *betrokkene* (RoG: burger) toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.
	7, lid 2	Plicht om het verzoek om toestemming in begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te presenteren met duidelijk onderscheid tussen andere aangelegenheden.
	7, lid 3	Plicht om bij het vragen om toestemming aangeven dat een betrokkene zijn toestemming kan intrekken.
	7, lid 3	Plicht om het proces van het intrekken van toestemming even eenvoudig te maken als het geven van toestemming.
	8, lid 2	Plicht om te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.
	9, lid 1	Verbod om persoonsgegevens te verwerken waaruit e.e.a. blijken of uit kan worden afgeleid, tenzij toestemming, noodzakelijke verwerking.
	11	Verwerking waarvoor identificatie niet is vereist
	12	Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene
	13	Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld
	14	Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen
	17, lid 1	Plicht om persoonsgegevens zonder onredelijke vertraging te wissen.
	19	Plicht kennisgeving inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking.
	20	Plicht om persoonsgegevens die verkregen zijn in een gestructureerde, gangbare en machineleesbare vorm te verstrekken aan de betrokkene
	21	Plicht om verwerking van persoonsgegevens te staken indien de betrokkene bezwaar heeft gemaakt.
	22	Plicht om passende maatregelen te nemen t.b.v. het recht op menselijke tussenkomst, recht om standpunt kenbaar te maken en recht om het besluit aan te vechten
	24	1. Plicht om passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd. Plicht om een passend gegevensbeschermingsbeleid te hebben voor de maatregelen.
	25	1. Plicht om passende technische en organisatorische maatregelen te treffen t.b.v. pseudonimisering, minimalisatie van gegevensverwerking en de nodige waarborgen ter naleving van de voorschriften uit de verordening. Plicht om technische en organisatorische maatregelen te treffen om persoonsgegevens te verwerken voor elk specifiek doel van de verwerking.

	26	Plicht om de betrokkene te informeren wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen,
	27	Plicht om een vertegenwoordiger aan te stellen/te machtigen in geval van een niet in de EU gevestigde verweringsverantwoordelijke of verwerker.
	28	Bepalingen t.b.v. de verwerker
	29	Plicht om uitsluitend in opdracht van de verwerkingsverantwoordelijke te verwerken
	30	Plicht om een register van (alle categorieën van) de verwerkingsactiviteiten bij te houden die t.b.v. de verwerkingsverantwoordelijke worden verricht.
	31	Plicht om, desgevraagd, samen te werken met de toezichthoudende autoriteit.
	32	Plicht om passende technische en organisatorische maatregen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.
	33	Plicht om plaatsgevonden inbreuken te melden aan de toezichthoudende autoriteit, informatie te verstrekken en alle inbreuken te documenteren.
	34	Plicht om de betrokkene te informeren over een inbreuk
	35	Plicht om voor de verwerking een beoordeling uit te voeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.
	36	Plicht om voorafgaande raadpleging te doen bij de toezichthoudende autoriteit in geval van een hoog risico indien er geen maatregelen worden genomen.
	37	Plicht om een functionaris voor gegevensbescherming aan te wijzen, bekend te maken en contactgegevens te delen met de toezichthoudende autoriteit
	38	Plicht om de positie van de functionaris voor gegevensbescherming te borgen
	42, lid 6	De verwerkingsverantwoordelijke of de verwerker die zijn verwerking aan het certificeringsmechanisme onderwerpt, verstrekt het certificeringsorgaan, of, waar van toepassing, aan de bevoegde toezichthoudende autoriteit de voor de uitvoering van de certificeringsprocedure noodzakelijke informatie en verleent het orgaan of de autoriteit toegang tot zijn verwerkingsactiviteiten.
	HFDST V	Plicht om te voldoen aan de voorwaarden die gesteld zijn aan doorgiften van persoonsgegevens aan een derde land of een internationale organisatie.
	46	Plicht om passende waarborgen te bieden en betrokkenen te beschikken over afdwingbare rechten en doeltreffende rechtsmiddelen om doorgifte van persoonsgegevens aan een derde land of internationale organisaties te laten plaatsvinden.
	60, lid 10	Plicht om de nodige maatregelen te treffen n.a.v. een besluit van de toezichthoudende autoriteit en de getroffen maatregelen mee te delen aan de toezichthoudende autoriteit.
ePrivacy	-	-
DA	Artikel 8 lid 1 t/m 5	1. Plicht: Wanneer een datahouder verplicht is data aan een ontvanger van data beschikbaar te stellen,. doet hij dit onder eerlijke, redelijke en niet-discriminerende voorwaarden en op transparante wijze overeenkomstig de bepalingen van dit hoofdstuk en hoofdstuk IV. 2. Een datahouder komt met een ontvanger van data de voorwaarden voor het beschikbaar stellen van de data overeen. Een contractuele bepaling betreffende de toegang tot en het gebruik van de data of de aansprakelijkheid en rechtsmiddelen voor de inbreuk op of de beëindiging van datagerelateerde verplichtingen is niet bindend indien zij voldoet aan de voorwaarden van artikel 13 of indien zij de toepassing uitsluit van, afwijkt van of de gevolgen wijzigt van de rechten van de gebruiker uit hoofde van hoofdstuk II. 3. Een datahouder mag bij het beschikbaar stellen van data geen onderscheid maken tussen vergelijkbare categorieën ontvangers van data, met inbegrip van partnerondernemingen of verbonden ondernemingen, zoals gedefinieerd in artikel 3 van de bijlage bij Aanbeveling 2003/361/EG, van de datahouder. Wanneer een ontvanger van data van mening is dat de voorwaarden voor het beschikbaar stellen van de data discriminerend zijn, dient de datahouder aan te tonen dat er geen sprake is van discriminatie. 4. Een datahouder stelt de data niet op exclusieve basis ter beschikking aan een ontvanger van data, tenzij de gebruiker daarom uit hoofde van hoofdstuk II verzoekt.

		5. Van houders en ontvangers van data wordt niet verlangd dat zij informatie verstrekken die verder gaat dan wat nodig is om na te gaan of wordt voldaan aan de contractuele voorwaarden die zijn overeengekomen voor het beschikbaar stellen van data, of aan hun verplichtingen uit hoofde van deze verordening of andere toepasselijke EU-wetgeving of nationale wetgeving tot uitvoering van het EU-recht.
	Artikel 3	Verplichting om door het gebruik van producten of gerelateerde diensten gegenereerde data toegankelijk te maken Producten worden zodanig ontworpen en vervaardigd, en gerelateerde diensten worden zodanig verleend, dat de door het gebruik ervan gegenereerde data standaard gemakkelijk, veilig en, waar relevant en passend, rechtstreeks toegankelijk zijn voor de gebruiker.
	Art. 14, lid 1	Een datahouder stelt op verzoek data ter beschikking aan een overheidsinstantie of een EU-instelling, -agentschap of -orgaan wanneer is aangetoond dat er een uitzonderlijke noodzaak bestaat om de gevraagde data te gebruiken.
	Art. 15, lid 1 en 2	Een uitzonderlijke noodzaak om data te gebruiken in de zin van dit hoofdstuk wordt geacht te bestaan wanneer er sprake is van een van de volgende omstandigheden: (a) wanneer de gevraagde data noodzakelijk zijn om te reageren op een algemene noodsituatie; (b) wanneer het verzoek om data beperkt is in tijd en reikwijdte en noodzakelijk is om een algemene noodsituatie te voorkomen of om het herstel na een algemene noodsituatie te ondersteunen; (c) wanneer het gebrek aan beschikbare data de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan belet een specifieke taak van algemeen belang te vervullen waarin de wet uitdrukkelijk voorziet; en (1) de overheidsinstantie of de EU-instelling, het EU-agentschap of het EU-orgaan niet in staat is geweest dergelijke data met alternatieve middelen te verkrijgen, onder meer door de data op de markt tegen markttarieven aan te kopen of door gebruik te maken van bestaande verplichtingen om data beschikbaar te stellen, en de vaststelling van nieuwe wetgevingsmaatregelen de tijdige beschikbaarheid van de data niet kan waarborgen; of (2) het verkrijgen van de data volgens de procedure van dit hoofdstuk de administratieve lasten voor datahouders of andere ondernemingen aanzienlijk zou verminderen.
	Art. 18, lid 3	Plicht: Indien persoonsgegevens moeten worden verstrekt om het verzoek om data van een overheidsinstantie of een EU-instelling, -agentschap of -orgaan in te willigen, levert de datahouder redelijke inspanningen om de data te pseudonimiseren, voor zover aan het verzoek kan worden voldaan met gepseudonimiseerde data.
DGA	2 lid 11	"openbaar lichaam": de nationale, regionale en lokale overheidsinstanties en publiekrechtelijke instellingen of samenwerkingsverbanden bestaande uit één of meer van deze overheidsinstanties of één of meer van deze publiekrechtelijke instellingen;
	2 lid 12	"publiekrechtelijke instellingen": instellingen die de volgende kenmerken hebben: (a) zij zijn opgericht voor het specifieke doel te voorzien in behoeften van algemeen belang, en zijn niet van industriële of commerciële aard; (b) zij bezitten rechtspersoonlijkheid; (c) zij worden merendeels door de nationale, regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen gefinancierd; of hun beheer staat onder toezicht van deze instanties of instellingen; of zij hebben een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, de regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen zijn aangewezen;
	4	Verbod op exclusiviteitsregelingen
	5 lid 1	Voorwaarden voor hergebruik: Openbare lichamen die krachtens het nationale recht bevoegd zijn om de toegang tot een of meer in artikel 3, lid 1, bedoelde

		gegevenscategorieën met het oog op hergebruik te verlenen of te weigeren, maken de *voorwaarden* voor het toestaan van dat hergebruik openbaar.
	5 lid 2	De voorwaarden voor hergebruik moeten non-discriminerend, evenredig en objectief gerechtvaardigd zijn voor wat betreft de gegevenscategorieën, het doel van het hergebruik en de aard van de gegevens waarvoor hergebruik wordt toegestaan. Deze voorwaarden mogen niet worden gebruikt om de mededinging te beperken.
	5 lid 3-8	Aanvullende bepalen t.a.v voorwaarden
	5 lid 9-13	Voorwaarden t.a.v. doorgifte aan derde landen
	6	Mogelijkheid om vergoedingen te vragen
	8	Inrichting centraal informatiepunt (verplichting voor lidstaten!)
DSA	Artikel 1	*Onderwerp en toepassingsgebied* 1. In deze verordening worden geharmoniseerde regels vastgelegd over het aanbieden van tussenhandelsdiensten op de interne markt. In deze richtlijn is met name het volgende bepaald: (a) een kader voor de voorwaardelijke vrijstelling van aansprakelijkheid van aanbieders van tussenhandelsdiensten optreden; (b) regels over verplichtingen inzake gepaste zorgvuldigheid op maat van bepaalde specifieke categorieën van aanbieders van tussenhandelsdiensten;
	Artikel 7	*Geen algemene verplichtingen inzake toezicht of actieve vaststelling van feiten* Aan aanbieders van tussenhandelsdiensten wordt geen algemene verplichting opgelegd om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief op zoek te gaan naar feiten of omstandigheden die op illegale activiteiten duiden.
	Artikel 8	*Bevelen om tegen illegale inhoud op te treden* 1. Bij ontvangst van een … uitgegeven bevel om tegen specifieke illegale inhoud op te treden, brengen aanbieders van tussenhandelsdiensten de uitgevende autoriteit onverwijld op de hoogte van het gevolg dat aan de bevelen is gegeven, met vermelding van de ondernomen actie en het ogenblik waarop de actie is ondernomen.
	Artikel 9	*Bevelen om informatie te verstrekken* *1. Wanneer aanbieders van tussenhandelsdiensten een … uitgegeven bevel ontvangen om specifieke informatie te verstrekken over een of meerdere specifieke afnemers van de dienst, brengen zij de uitgevende autoriteit onmiddellijk op de hoogte van de ontvangst van het bevel en van het gevolg dat zij hieraan hebben gegeven.*
	Artikel 10	*Contactpunten* Aanbieders van tussenhandelsdiensten voorzien in een centraal contactpunt ... 2. Aanbieders van tussenhandelsdiensten stellen de informatie ter beschikking die nodig is om hun centrale contactpunt gemakkelijk te identificeren en ermee te communiceren. 3. Aanbieders van tussenhandelsdiensten vermelden in de in lid 2 bedoelde informatie de officiële taal of talen van de EU die kan of kunnen worden gebruikt om met hun contactpunt te communiceren
	Artikel 13	*Rapportageverplichtingen inzake transparantie voor aanbieders van tussenhandelsdiensten* 1. Aanbieders van tussenhandelsdiensten publiceren, ten minste een keer per jaar, duidelijke, gemakkelijk te begrijpen en gedetailleerde rapporten over eventuele inhoudsmoderatie die zij tijdens de betrokken periode hebben uitgevoerd. Deze rapporten bevatten met name informatie over het volgende, waar van toepassing:
DMA	-	-
eIDAS	Artikel 13	Verleners van vertrouwensdiensten zijn aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade.
	Artikel 14	Vertrouwensdiensten die door in een derde land gevestigde verlener van vertrouwensdiensten worden verstrekt moeten worden erkend op grond van een

		overeenkomst tussen de Europese Unie en het betrokken derde land of internationale organisatie.
	Artikel 15	Wanneer het haalbaar is vertrouwensdiensten of eindgebruiker producten die worden gebruik bij de verlening van deze diensten toegankelijk maken voor personen met een handicap.
	Artikel 19	Verleners van vertrouwensdiensten moeten treffende passende technische en organisatorische maatregelen treffen om risico's te beheren in verband met de veiligheid van de door hen verleende vertrouwensdiensten.
	Artikel 20	Verleners van vertrouwensdiensten moeten eens in de 24 maanden onderwerpen worden aan een audit door een conformiteitsbeoordelingsorgaan.
	Artikel 23	Gekwalificeerde verleners van diensten kunnen het vertrouwensmerk van de EU gebruiken om de vertrouwensdiensten op eenvoudige, herkenbare en duidelijke manier aan te geven.
	Artikel 24	Eisen aan gekwalificeerde verleners van vertrouwensdiensten
eIDAS 2 (*Europees kader voor digitale identiteit*)	Artikel 6, bis, 7	De afgever van de Europese portemonnee voor digitale identiteit verzamelt geen informatie over het gebruik van de portemonnee die niet noodzakelijk si 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.
	Artikel 7, ter,	Vertrouwde partijen voor Europese portemonnees voor digitale identiteit.
	Artikel 12, ter, 2	Indien particuliere vertrouwende partijen die diensten verlenen krachtens nationaal of Unierecht, sterke gebruikersauthenticatie voor online-identificatie moeten gebruiken, of indien sterke gebruikersauthenticatie vereist is op grond van een contractuele verbintenis, waaronder op het gebied van vervoer, energie, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie, aanvaarden particuliere vertrouwende partijen ook het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig artikel 6 bis zijn afgegeven.
	Artikel 12, ter, 3	Indien zeer grote onlineplatforms, als gedefinieerd in artikel 25, lid 1, van Verordening [referentie verordening inzake digitale diensten (DSA)] verlangen dat gebruikers zich authenticeren om toegang tot onlinediensten te krijgen, aanvaarden ze ook het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig artikel 6 bis zijn afgegeven; zij het uitsluitend op vrijwillig verzoek van de gebruiker en met inachtneming van de minimaal benodigde attributen voor de specifieke onlinedienst waarvoor authenticatie vereist is, zoals een bewijs van leeftijd.
	Artikel 13, lid 1, 1 (vervanging)	Onverminderd lid 2 zijn verleners van vertrouwensdiensten aansprakelijk voor schade die opzettelijk of uit onachtzaamheid wordt veroorzaakt aan natuurlijke of rechtspersonen vanwege een niet-naleving van de verplichtingen krachtens deze verordening of de verplichtingen inzake het risicobeheer op het gebied van cyberbeveiliging krachtens artikel 18 van Richtlijn XXXX/XXXX [NIS2].
	Artikel 14	Artikel 14 wordt vervangen.
	Artikel 15	Artikel 15 wordt vervangen.
	Artikel 20	De conformiteitsbeoordeling moet ook bevestigen dat voldaan wordt aan vereisten uit de NIS2-richtlijn.
	Artikel 24	Wijzigingen en toevoegingen in de eisen aan gekwalificeerde verleners van vertrouwensdiensten.
	Artikel 28	Eisen voor een gekwalificeerde dienst voor het beheer van middelen voor het aanmaken van elektronische handtekeningen op afstand
	Artikel 45, sexies	Verleners van gekwalificeerde elektronische attesteringen van attributen bieden een interface met de afgegeven Europese portemonnees voor digitale identiteit.

	Artikel 45, septies	Aanvullende voorschriften voor de levering van diensten voor elektronische attestering van attributen.

Bijlage F Rechten en plichten regiedienstaanbieders per EU-regeling

Regiedienstaanbieder		
Regeling	Artikel	Rechten/plichten
AVG	2, lid d	Verordening niet van toepassing i.h.k.v. voorkoming, onderzoek, opsporing, vervolging van strafbare feiten
	9, lid 2, f)	Recht om de verwerking te doen van bijzondere categorieën van persoonsgegevens indien noodzakelijk voor de instelling, uitoefening of onderbouwing van de rechtsverordening of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.
	7, lid 1	Plicht van de *verwerkingsverantwoordelijke* om aan te tonen dat de *betrokkene* (RoG: burger) toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.
	7, lid 2	Plicht om het verzoek om toestemming in begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te presenteren met duidelijk onderscheid tussen andere aangelegenheden.
	7, lid 3	Plicht om bij het vragen om toestemming aangeven dat een betrokkene zijn toestemming kan intrekken.
	7, lid 3	Plicht om het proces van het intrekken van toestemming even eenvoudig te maken als het geven van toestemming.
	8, lid 2	Plicht om te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.
	9, lid 1	Verbod om persoonsgegevens te verwerken waaruit e.e.a. blijken of uit kan worden afgeleid, tenzij toestemming, noodzakelijke verwerking.
	11	Verwerking waarvoor identificatie niet is vereist
	12	Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene
	13	Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld
	14	Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen
	17, lid 1	Plicht om persoonsgegevens zonder onredelijke vertraging te wissen.
	19	Plicht kennisgeving inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking.
	20	Plicht om persoonsgegevens die verkregen zijn in een gestructureerde, gangbare en machineleesbare vorm te verstrekken aan de betrokkene
	21	Plicht om verwerking van persoonsgegevens te staken indien de betrokkene bezwaar heeft gemaakt.
	22	Plicht om passende maatregelen te nemen t.b.v. het recht op menselijke tussenkomst, recht om standpunt kenbaar te maken en recht om het besluit aan te vechten
	24	2. Plicht om passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd. 3. Plicht om een passend gegevensbeschermingsbeleid te hebben voor de maatregelen.
	25	2. Plicht om passende technische en organisatorische maatregelen te treffen t.b.v. pseudonimisering, minimalisatie van gegevensverwerking en de nodige waarborgen ter naleving van de voorschriften uit de verordening. 3. Plicht om technische en organisatorische maatregelen te treffen om persoonsgegevens te verwerken voor elk specifiek doel van de verwerking.

	26	Plicht om de betrokkene te informeren wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen,
	27	Plicht om een vertegenwoordiger aan te stellen/te machtigen in geval van een niet in de EU gevestigde verweringsverantwoordelijke of verwerker.
	28	Bepalingen t.b.v. de verwerker
	29	Plicht om uitsluitend in opdracht van de verwerkingsverantwoordelijke te verwerken
	30	Plicht om een register van (alle categorieën van) de verwerkingsactiviteiten bij te houden die t.b.v. de verwerkingsverantwoordelijke worden verricht.
	31	Plicht om, desgevraagd, samen te werken met de toezichthoudende autoriteit.
	32	Plicht om passende technische en organisatorische maatregen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.
	33	Plicht om plaatsgevonden inbreuken te melden aan de toezichthoudende autoriteit, informatie te verstrekken en alle inbreuken te documenteren.
	34	Plicht om de betrokkene te informeren over een inbreuk
	35	Plicht om voor de verwerking een beoordeling uit te voeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.
	36	Plicht om voorafgaande raadpleging te doen bij de toezichthoudende autoriteit in geval van een hoog risico indien er geen maatregelen worden genomen.
	37	Plicht om een functionaris voor gegevensbescherming aan te wijzen, bekend te maken en contactgegevens te delen met de toezichthoudende autoriteit
	38	Plicht om de positie van de functionaris voor gegevensbescherming te borgen
	42, lid 6	De verwerkingsverantwoordelijke of de verwerker die zijn verwerking aan het certificeringsmechanisme onderwerpt, verstrekt het certificeringsorgaan, of, waar van toepassing, aan de bevoegde toezichthoudende autoriteit de voor de uitvoering van de certificeringsprocedure noodzakelijke informatie en verleent het orgaan of de autoriteit toegang tot zijn verwerkingsactiviteiten.
	HFDST V	Plicht om te voldoen aan de voorwaarden die gesteld zijn aan doorgiften van persoonsgegevens aan een derde land of een internationale organisatie.
	46	Plicht om passende waarborgen te bieden en betrokkenen te beschikken over afdwingbare rechten en doeltreffende rechtsmiddelen om doorgifte van persoonsgegevens aan een derde land of internationale organisaties te laten plaatsvinden.
	60, lid 10	Plicht om de nodige maatregelen te treffen n.a.v. een besluit van de toezichthoudende autoriteit en de getroffen maatregelen mee te delen aan de toezichthoudende autoriteit.
ePrivacy	5	Verbod op elke interferentie met elektronische communicatiegegevens, zoals door het afluisteren, aftappen, opslaan, controleren, scannen of anderszins onderscheppen, controleren of verwerken van elektronische communicatiegegevens door andere personen dan de eindgebruikers, tenzij toegestaan door deze verordening.
	6	Toegestane verwerkingen van elektronische communicatiegegevens
	7	Opslag en wissen van elektronische communicatiegegevens
	8, lid 1	Verbod (met uitzonderingen) op het gebruik van verwerkings- en opslagcapaciteit van eindapparatuur en het verzamelen van gegevens uit eindapparatuur van eindgebruikers, onder meer over de software en de hardware, anders dan door de betrokken eindgebruiker.
	8, lid 2	Verbod (met uitzonderingen) op het verzamelen van gegevens uit eindapparatuur om een aansluiting op andere apparatuur en/of netwerkuitrusting mogelijk te maken.
	10, lid 1	Plicht om bij software de optie te bieden om derden te verhinderen informatie in de eindapparatuur van de eindgebruiker op te slaan of reeds op die eindapparatuur opgeslagen informatie te verwerken

	10, lid 2	Plicht om bij de installatie van software de eindgebruiker te informeren over de opties in de privacy-instellingen
	11, lid 2	Plicht om interne procedures in te voeren voor de afhandeling van verzoeken om toegang tot elektronische communicatiegegevens van eindgebruikers op basis van een krachtens lid 1 vastgestelde wetgevende handeling. Plicht om de bevoegde toezichthoudende instantie op verzoek informatie te verstrekken over deze procedures, het aantal ontvangen verzoeken, de aangevoerde wettelijke motivering en het antwoord daarop.
	12 & 13	Bepalingen betreffende de weergave en beperking van de identificatie van het oproepende en het opgeroepen nummer.
	14	Plicht om geavanceerde maatregelen te ontwikkelen om de ontvangst van ongewenste oproepen door eindgebruikers te beperken en de opgeroepen eindgebruiker kosteloos van een aantal mogelijkheden te voorzien.
	15	Bepalingen betreffende de aanbieders van algemeen beschikbare telefoongidsen.
	16, lid 1	Plicht om toestemming te hebben van eindgebruikers voor de verzending van direct marketingberichten.
	16, lid 3	Plicht om aspecten kenbaar te maken indien gebruik gemaakt wordt van elektronische communicatiediensten door de doeleinden van direct marketing.
	16, lid 6	Plicht om eindgebruikers te informeren over de commerciële aard van de communicatie.
	17	Plicht om eindgebruikers te informeren over een bijzonder risico dat de veiligheid van elektronische communicatienetwerken en -diensten kan aantasten.
DA	Art. 5, lid 1	Op verzoek van een gebruiker of van een namens een gebruiker optredende partij stelt de datahouder de door het gebruik van een product of gerelateerde dienst gegenereerde data onverwijld en zonder kosten voor de gebruiker ter beschikking aan een derde partij, met dezelfde kwaliteit als die waarover de datahouder beschikt en, indien van toepassing, continu en in realtime.
	Art. 5 lid 3	Van de gebruiker of derde partij wordt geen informatie verlangd die verder gaat dan wat nodig is om de gebruiker of derde partij als zodanig te verifiëren overeenkomstig lid 1. De datahouder bewaart geen informatie over de toegang van de derde partij tot de gevraagde data die verder gaat dan nodig is voor de goede uitvoering van het toegangsverzoek van de derde partij en voor de beveiliging en het onderhoud van de data-infrastructuur.
	Art. 5, lid 7	Het verzuim van de datahouder en de derde partij om regelingen voor het doorgeven van de data overeen te komen, mag de uitoefening van de rechten van de betrokkene uit hoofde van Verordening (EU) 2016/679 en met name het recht op overdraagbaarheid van data uit hoofde van artikel 20 van die verordening, niet belemmeren, beletten of verstoren.
	Art. 6, lid 1	Een derde partij verwerkt de hem overeenkomstig artikel 5 ter beschikking gestelde data uitsluitend voor de doeleinden en onder de voorwaarden die met de gebruiker zijn overeengekomen, en met inachtneming van de rechten van de betrokkene wat persoonsgegevens betreft, en wist de data wanneer zij niet langer noodzakelijk zijn voor het overeengekomen doel.
	Art. 6, lid 3	De derde partij mag niet: (a) de gebruiker op enigerlei wijze dwingen, misleiden of manipuleren door de autonomie, besluitvorming of keuzes van de gebruiker te ondermijnen of te beperken, onder meer door middel van een digitale interface met de gebruiker; (b) de ontvangen data gebruiken voor de profilering van natuurlijke personen in de zin van artikel 4, lid 4, van Verordening (EU) 2016/679, tenzij dit noodzakelijk is om de door de gebruiker gevraagde dienst te verlenen;

	Art. 11, lid 2	Een ontvanger van data die met het oog op het verkrijgen van data onjuiste of valse informatie aan de datahouder heeft verstrekt, bedrieglijke of dwingende middelen heeft ingezet of kennelijke leemten in de technische infrastructuur van de datahouder ter bescherming van de data heeft misbruikt, de data die ter beschikking zijn gesteld voor ongeoorloofde doeleinden heeft gebruikt of deze data zonder toestemming van de datahouder aan een andere partij heeft verstrekt, doet onverwijld het volgende, tenzij de datahouder of de gebruiker anderszins instructies geeft: (a) de door de datahouder beschikbaar gestelde data en kopieën daarvan vernietigen; (b) een einde maken aan het produceren, aanbieden, in de handel brengen of gebruiken van goederen, afgeleide data of diensten die zijn geproduceerd op basis van de via die data verkregen kennis, of aan het invoeren, uitvoeren of opslaan van inbreukmakende goederen voor die doeleinden, en inbreukmakende goederen vernietigen.
	Art. 11, lid 3	Lid 2, punt b), is niet van toepassing in de volgende gevallen: a) het gebruik van de data heeft de datahouder geen ernstige schade berokkend; b) het zou onevenredig zijn, gezien de belangen van de datahouder
DGA	7 lid 1	De lidstaten wijzen een of meer bevoegde organen aan, die sectoraal kunnen zijn, om de openbare lichamen te ondersteunen bij het verlenen van toegang tot het hergebruik van de in artikel 3, lid 1, bedoelde gegevenscategorieën.
	7 lid 3	De bevoegde organen mogen ook gemachtigd worden om toegang te verlenen voor het hergebruik van de in artikel 3, lid 1, bedoelde gegevenscategorieën, krachtens het Unierecht of het nationale recht dat voorziet in het verlenen van die toegang.
	9	Voor het aanbieden van de volgende **gegevensdelingsdiensten** geldt een kennisgevingsprocedure: (a) bemiddelingsdiensten tussen gegevenshouders die rechtspersonen zijn en potentiële gebruikers van de gegevens, met inbegrip van het beschikbaar stellen van technische of andere middelen om dergelijke diensten mogelijk te maken; die diensten kunnen bilaterale of multilaterale gegevensuitwisseling omvatten, alsook de oprichting van platforms of databanken die de uitwisseling of gezamenlijke exploitatie van gegevens mogelijk maken, en de oprichting van specifieke infrastructuur voor de interconnectie tussen gegevenshouders en gegevensgebruikers; (b) bemiddelingsdiensten tussen datasubjecten die hun persoonsgegevens beschikbaar willen stellen en potentiële gegevensgebruikers, met inbegrip van het beschikbaar stellen van technische of andere middelen om dergelijke diensten mogelijk te maken, bij de uitoefening van de bij Verordening (EU) 2016/679 voorziene rechten; (c) diensten van gegevenscoöperaties, d.w.z. diensten ter ondersteuning van datasubjecten, eenmansbedrijven of micro-, kleine en middelgrote ondernemingen die lid zijn van de coöperatie of die de coöperatie de bevoegdheid verlenen om te onderhandelen over voorwaarden voor gegevensverwerking alvorens zij daarmee instemmen, om geïnformeerde keuzes te maken alvorens in te stemmen met gegevensverwerking, en om het mogelijk te maken mechanismen op te zetten voor de uitwisseling van standpunten over het doel en de voorwaarden van gegevensverwerking, die het beste de belangen van datasubjecten of rechtspersonen vertegenwoordigen.
	11	Voor de in artikel 9, lid 1, bedoelde verlening van gegevensdelingsdiensten gelden de volgende voorwaarden: (1) de aanbieder mag de gegevens waarvoor hij diensten verleent niet voor andere doeleinden gebruiken dan de beschikbaarstelling ervan aan gegevensgebruikers; gegevensdelingsdiensten moeten in een afzonderlijke juridische entiteit worden ondergebracht;

		(2) de metagegevens die bij de levering van de gegevensdelingsdienst zijn verzameld, mogen alleen worden gebruikt voor de ontwikkeling van die dienst; (3) de aanbieder ziet erop toe dat de procedure voor toegang tot zijn dienst eerlijk, transparant en niet-discriminerend is voor zowel gegevenshouders als gegevensgebruikers, ook wat de prijzen betreft; (4) de aanbieder faciliteert de uitwisseling van de gegevens in het formaat waarin hij de gegevens ontvangt van de gegevenshouder en converteert de gegevens alleen naar specifieke formaten om de interoperabiliteit binnen en tussen sectoren te verbeteren, indien de gegevensgebruiker daarom verzoekt, indien het Unierecht hem daartoe verplicht of om de harmonisering met internationale of Europese gegevensnormen te waarborgen; (5) de aanbieder beschikt over procedures ter voorkoming van frauduleuze of onrechtmatige praktijken met betrekking tot de toegang tot gegevens door partijen die via hun diensten toegang wensen te krijgen; (6) de aanbieder zorgt voor een redelijke continuïteit bij de levering van zijn diensten en, in het geval van diensten die zorgen voor de opslag van gegevens, voor voldoende garanties die gegevenshouders en gegevensgebruikers in staat stellen toegang te krijgen tot hun gegevens in geval van insolventie; (7) de aanbieder neemt passende technische, juridische en organisatorische maatregelen ter voorkoming van doorgifte van of toegang tot niet-persoonsgebonden gegevens die krachtens het Unierecht onwettig is; (8) de aanbieder neemt maatregelen om een hoog niveau van beveiliging te waarborgen bij de opslag en doorgifte van niet-persoonsgebonden gegevens; (9) de aanbieder beschikt over procedures om ervoor te zorgen dat de mededingingsregels van de Unie en de lidstaten worden nageleefd; (10) de aanbieder die diensten aanbiedt aan datasubjecten handelt in het belang van de datasubjecten bij het faciliteren van de uitoefening van hun rechten, met name door datasubjecten advies te verstrekken over potentieel gebruik van de gegevens en de standaardvoorwaarden voor dergelijk gebruik; 1. (11)wanneer een aanbieder instrumenten ter beschikking stelt om instemming te verkrijgen van datasubjecten of toestemming om door rechtspersonen beschikbaar gestelde gegevens te verwerken, specificeert hij het rechtsgebied of de rechtsgebieden waarin het gebruik van de gegevens zal plaatsvinden.
DSA		
DMS	Art.5 a)	de poortwachter combineert geen persoonsgegevens die afkomstig zijn van deze kernplatformdiensten met persoonsgegevens van andere diensten die door de poortwachter worden aangeboden of met persoonsgegevens van diensten van derden, en meldt eindgebruikers niet aan op andere diensten van de poortwachter teneinde persoonsgegevens te combineren, tenzij de eindgebruiker de specifieke keuze heeft gekregen en toestemming heeft verleend in de zin van Verordening (EU) 2016/679 <AVG> ;
	Art.5 f)	de poortwachter verplicht zakelijke gebruikers of eindgebruikers niet zich te abonneren op of zich te registreren bij andere kernplatformdiensten die overeenkomstig artikel 3 zijn geïdentificeerd of die voldoen aan de drempels van artikel 3, lid 2, punt b), als voorwaarde voor toegang tot, inschrijving op of registratie op een van hun overeenkomstig dat artikel geïdentificeerde kernplatformdiensten;
	Art.6 a)	wanneer een poortwachter de concurrentie aangaat met zakelijke gebruikers, onthoudt hij zich van het gebruik van gegevens die niet openbaar beschikbaar zijn en die worden gegenereerd door activiteiten van die zakelijke gebruikers, alsook van de eindgebruikers van die zakelijke gebruikers of van zijn kernplatformdiensten, of die worden verstrekt door die zakelijke gebruikers van zijn kernplatformdiensten of door de eindgebruikers van die zakelijke gebruikers;

	Art.6 b)	de poortwachter laat eindgebruikers toe voorgeïnstalleerde softwaretoepassingen op zijn kernplatformdienst te verwijderen, onverminderd de mogelijkheid voor een poortwachter om dergelijke verwijdering te beperken met betrekking tot softwaretoepassingen die essentieel zijn voor de werking van het besturingssysteem of van het apparaat en die in technisch opzicht niet op zichzelf door derden kunnen worden aangeboden;
	Art.6 e)	de poortwachter legt geen technische beperking op aan het vermogen van eindgebruikers om over te stappen en zich te abonneren op andere softwaretoepassingen en diensten waartoe toegang kan worden verkregen via het besturingssysteem van de poortwachter, ook wat betreft de keuze van de aanbieder van internettoegang voor eindgebruikers;
eIDAS	Artikel 13	Verleners van vertrouwensdiensten zijn aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade.
	Artikel 14	Vertrouwensdiensten die door in een derde land gevestigde verlener van vertrouwensdiensten worden verstrekt moeten worden erkend op grond van een overeenkomst tussen de Europese Unie en het betrokken derde land of internationale organisatie.
	Artikel 15	Wanneer het haalbaar is vertrouwensdiensten of eindgebruikerproducten die worden gebruik bij de verlening van deze diensten toegankelijk maken voor personen met een handicap.
	Artikel 19	Verleners van vertrouwensdiensten moeten treffende passende technische en organisatorische maatregelen treffen om risico's te beheren in verband met de veiligheid van de door hen verleende vertrouwensdiensten.
	Artikel 20	Verleners van vertrouwensdiensten moeten eens in de 24 maanden onderwerpen worden aan een audit door een conformiteitsbeoordelingsorgaan.
	Artikel 23	Gekwalificeerde verleners van diensten kunnen het vertrouwensmerk van de EU gebruiken om de vertrouwensdiensten op eenvoudige, herkenbare en duidelijke manier aan te geven.
	Artikel 24	Eisen aan gekwalificeerde verleners van vertrouwensdiensten
eIDAS 2 (*Europees kader voor digitale identiteit*)	Artikel 6, bis, 7	De afgever van de Europese portemonnee voor digitale identiteit verzamelt geen informatie over het gebruik van de portemonnee die niet noodzakelijk si 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.
	Artikel 7, ter,	Vertrouwde partijen voor Europese portemonnees voor digitale identiteit.
	Artikel 12, ter, 2	Indien particuliere vertrouwende partijen die diensten verlenen krachtens nationaal of Unierecht, sterke gebruikersauthenticatie voor online-identificatie moeten gebruiken, of indien sterke gebruikersauthenticatie vereist is op grond van een contractuele verbintenis, waaronder op het gebied van vervoer, energie, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie, aanvaarden particuliere vertrouwende partijen ook het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig artikel 6 bis zijn afgegeven.
	Artikel 12, ter, 3	Indien zeer grote onlineplatforms, als gedefinieerd in artikel 25, lid 1, van Verordening [referentie verordening inzake digitale diensten (DSA)] verlangen dat gebruikers zich authenticeren om toegang tot onlinediensten te krijgen, aanvaarden ze ook het gebruik van Europese portemonnees voor digitale identiteit die overeenkomstig artikel 6 bis zijn afgegeven; zij het uitsluitend op vrijwillig verzoek van de gebruiker en met inachtneming van de minimaal benodigde attributen voor de specifieke onlinedienst waarvoor authenticatie vereist is, zoals een bewijs van leeftijd.

	Artikel 13, lid 1, 1 (vervanging)	Onverminderd lid 2 zijn verleners van vertrouwensdiensten aansprakelijk voor schade die opzettelijk of uit onachtzaamheid wordt veroorzaakt aan natuurlijke of rechtspersonen vanwege een niet-naleving van de verplichtingen krachtens deze verordening of de verplichtingen inzake het risicobeheer op het gebied van cyberbeveiliging krachtens artikel 18 van Richtlijn XXXX/XXXX [NIS2].
	Artikel 14	Artikel 14 wordt vervangen.
	Artikel 15	Artikel 15 wordt vervangen.
	Artikel 20	De conformiteitsbeoordeling moet ook bevestigen dat voldaan wordt aan vereisten uit de NIS2-richtlijn.
	Artikel 24	Wijzigingen en toevoegingen in de eisen aan gekwalificeerde verleners van vertrouwensdiensten.
	Artikel 28	Eisen voor een gekwalificeerde dienst voor het beheer van middelen voor het aanmaken van elektronische handtekeningen op afstand
	Artikel 45, sexies	Verleners van gekwalificeerde elektronische attesteringen van attributen bieden een interface met de afgegeven Europese portemonnees voor digitale identiteit.
	Artikel 45, septies	Aanvullende voorschriften voor de levering van diensten voor elektronische attestering van attributen.

Bijlage G Overzicht actoren/rollen in Europese wetgeving

Verordening	Titel	Artikel | #	Term	Definitie
Verordening (EU) 2016/679	AVG	Artikel 4 |7	**Betrokkene**	Een geïdentificeerde of identificeerbare natuurlijke persoon
Verordening (EU) 2016/679	AVG	Artikel 4 |7	**Verwerkingsverantwoordelijke**	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen
Verordening (EU) 2016/679	AVG	Artikel 4 |8	**Verwerker**	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt
Verordening (EU) 2016/679	AVG	Artikel 4 |9	**Ontvanger**	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn
Verordening (EU) 2016/679	AVG	Artikel 4 |10	**Derde**	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken
Verordening (EU) 2016/679	AVG	Artikel 4 |17	**Vertegenwoordiger**	Een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening
Verordening (EU) 2016/679	AVG	Artikel 4 |18	**Onderneming**	Een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en

				persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen
Verordening (EU) 2016/679	AVG	Artikel 4 |19	**Concern**	Een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend
Verordening (EU) 2016/679	AVG	Artikel 4 |21	**Toezichthoudende autoriteit**	Een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie
Verordening (EU) 2016/679	AVG	Artikel 4 |22	**Betrokken toezichthoudende autoriteit**	Een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat: a. de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd; b. de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of c. bij die toezichthoudende autoriteit een klacht is ingediend
Verordening (EU) 2016/679	AVG	Artikel 4 |26	**Internationale organisatie**	Een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen
Voorstel Verordening COM(2017) 10	ePrivacy	Artikel 4 |2.b	**Eindgebruiker**	*Verwijzing naar Richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie:* Een gebruiker die geen openbaar elektronische communicatienetwerk of voor het publiek beschikbare elektronische communicatiediensten aanbiedt.
Voorstel Verordening COM(2022) 68	Data Act	Artikel 2 | 5	**Gebruiker**	Een natuurlijke of rechtspersoon die een product in eigendom heeft, huurt of leaset of een dienst ontvangt
Voorstel Verordening COM(2022) 68	Data Act	Artikel 2 | 6	**Datahouder**	Een rechtspersoon of natuurlijke persoon die overeenkomstig deze verordening, het toepasselijke EU-recht of de nationale wetgeving tot uitvoering van het EU-recht, of, in het geval van niet-persoonsgebonden data en door controle over het technische ontwerp van het product en de bijbehorende diensten, het recht of de verplichting heeft om bepaalde data beschikbaar te stellen
Voorstel Verordening COM(2022) 68	Data Act	Artikel 2 | 7	**Ontvanger van data**	Een rechtspersoon of natuurlijke persoon die handelt voor doeleinden die verband houden met zijn handels-, bedrijfs-, ambachts- of beroepsactiviteit, die niet de gebruiker van een product of gerelateerde dienst is en aan wie data beschikbaar worden gesteld door de datahouder, met inbegrip van een derde partij op verzoek van de gebruiker aan de datahouder of in overeenstemming met een wettelijke verplichting uit hoofde van EU-recht of nationale wetgeving tot omzetting van het EU-recht.

Voorstel Verordening COM(2022) 68	Data Act	Artikel 2 | 8	**Bedrijf (of onderneming)**	Iedere natuurlijke persoon of rechtspersoon die handelt volgens onder deze verordening vallende overeenkomsten en praktijken, voor doeleinden die gerelateerd zijn aan diens handels-, bedrijfs-, ambachts- of beroepsactiviteit
Voorstel Verordening COM(2022) 68	Data Act	Artikel 2 | 9	**Overheidsinstantie**	Nationale, regionale en lokale autoriteiten van de lidstaten, publiekrechtelijke instellingen van de lidstaten of samenwerkingsverbanden bestaande uit één of meer van deze autoriteiten of één of meer van deze instellingen;
Voorstel Verordening COM(2020) 767	DGA	Artikel 2 | 5	**Gegevens houder**	Een rechtspersoon die of datasubject dat, overeenkomstig het toepasselijke Unierecht of nationaal recht, het recht heeft om toegang te verlenen tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens waarover hij/het zeggenschap heeft, en deze te verspreiden.
Voorstel Verordening COM(2020) 767	DGA	Artikel 2 | 6	**Gegevens gebruiker**	Een natuurlijke persoon of rechtspersoon die rechtmatige toegang heeft tot bepaalde persoonsgegevens of niet-persoonsgebonden gegevens en gemachtigd is die gegevens voor commerciële of niet-commerciële doeleinden te gebruiken.
Voorstel Verordening COM(2020) 767	DGA	Artikel 2 | 11	**Openbaar lichaam**	De nationale, regionale en lokale overheidsinstanties en publiekrechtelijke instellingen of samenwerkingsverbanden bestaande uit één of meer van deze overheidsinstanties of één of meer van deze publiekrechtelijke instellingen.
Voorstel Verordening COM(2020) 767	DGA	Artikel 2 | 12	**Publiekrechtelijke instellingen**	Instellingen die de volgende kenmerken hebben: a. zij zijn opgericht voor het specifieke doel te voorzien in behoeften van algemeen belang, en zijn niet van industriële of commerciële aard; b. zij bezitten rechtspersoonlijkheid; c. zij worden merendeels door de nationale, regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen gefinancierd; of hun beheer staat onder toezicht van deze instanties of instellingen; of zij hebben een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, de regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen zijn aangewezen.
Voorstel Verordening COM(2020) 767	DGA	Artikel 2 | 13	**Overheidsondernemi ng**	Elke onderneming waarover openbare lichamen direct of indirect een dominante invloed kunnen uitoefenen op basis van eigendom van of financiële deelneming in die onderneming, of de regels die op die onderneming van toepassing zijn; openbare lichamen worden geacht een dominante invloed uit te oefenen in elk van de volgende gevallen waarin die lichamen, direct of indirect: a. de meerderheid van het geplaatste kapitaal van de onderneming bezitten, of

				b. over de meerderheid van de stemrechten beschikken die zijn verbonden aan de door de onderneming uitgegeven aandelen, of c. meer dan de helft van de leden van het bestuurs-, leidinggevend of toezichthoudend orgaan van de onderneming kunnen aanwijzen.
Voorstel Verordening COM(2020) 767	DGA	Artikel 2 | 15	**Vertegenwoordiger**	Elke in de Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om voor rekening van een aanbieder van gegevensdelingsdiensten of een entiteit die, voor doeleinden van algemeen belang, gegevens verzamelt die door niet in de Unie gevestigde natuurlijke personen of rechtspersonen ter beschikking zijn gesteld op basis van gegevensaltruïsme, te handelen, waartoe een nationale bevoegde autoriteit zich kan wenden in plaats van tot de aanbieder van gegevensdelingsdiensten of entiteit, wat de verplichtingen van de aanbieder van gegevensdelingsdiensten of entiteit uit hoofde van deze verordening betreft.
Voorstel Verordening COM(2020) 825	DSA	Artikel 2 | b	**Afnemer van de dienst**	Een natuurlijke persoon of rechtspersoon die gebruikmaakt van de betrokken tussenhandelsdienst.
Voorstel Verordening COM(2020) 825	DSA	Artikel 2 | c	**Consument**	Een natuurlijke persoon die handelt voor doeleinden die buiten zijn bedrijfs-, handels- of beroepsactiviteit vallen.
Voorstel Verordening COM(2020) 825	DSA	Artikel 2 | e	**Handelaar**	Iedere natuurlijke persoon of iedere privaatrechtelijke dan wel publiekrechtelijke rechtspersoon die, ook via een andere persoon die in zijn naam of voor zijn rekening optreedt, handelt in het kader van de uitoefening van zijn handels-, bedrijfs-, ambachts- of beroepsactiviteit.
Voorstel Verordening COM(2020) 825	DSA	Artikel 2 | h	**Onlineplatform**	Een aanbieder van een hostingdienst die, op verzoek van een afnemer van de dienst, informatie opslaat en verspreidt bij het publiek, tenzij die activiteit een kleine en louter bijkomende functie van een andere dienst is en om objectieve en technische redenen niet kan worden gebruikt zonder die andere dienst, en de integratie van de functie in de andere dienst geen manier is om de toepasbaarheid van deze verordening te omzeilen.
Voorstel Verordening COM(2020) 825	DSA	Artikel 2 | l	**Coördinator voor digitale diensten van vestiging**	De coördinator voor digitale diensten van de lidstaat waar de aanbieder van een tussenhandelsdienst is gevestigd of waar zijn juridische vertegenwoordiger verblijft of is gevestigd.
Voorstel Verordening COM(2020) 825	DSA	Artikel 2 | m	**Coördinator voor digitale diensten van bestemming**	De coördinator voor digitale diensten van een lidstaat waar de tussenhandelsdienst wordt verleend.

Voorstel Verordening COM(2020) 842	DMA	Artikel 2 | 1	**Poortwachter**	Een overeenkomstig artikel 3 aangewezen aanbieder van kernplatformdiensten. Moet voldoen aan door EU gestelde randvoorwaarden als dataportabiliteit. Een aanbieder van kernplatformdiensten wordt als poortwachter aangewezen indien deze: een aanzienlijke impact heeft op de interne markt; een kernplatformdienst exploiteert die voor zakelijke gebruikers als een belangrijke toegangspoort fungeert om eindgebruikers te bereiken; en met betrekking tot haar activiteiten een stevig verankerde en duurzame positie inneemt of naar verwachting in de nabije toekomst een dergelijke positie zal innemen.
Voorstel Verordening COM(2020) 842	DMA	Artikel 2 | 16	**Eindgebruiker**	Elke natuurlijke of rechtspersoon die gebruikmaakt van kernplatformdiensten anders dan als zakelijke gebruiker
Voorstel Verordening COM(2020) 842	DMA	Artikel 2 | 17	**Zakelijke gebruiker**	Een natuurlijke of rechtspersoon die in commerciële of professionele hoedanigheid gebruikmaakt van kernplatformdiensten ten behoeve van of in het kader van het aanbieden van goederen of diensten aan eindgebruikers.
Voorstel Verordening COM(2020) 842	DMA	Artikel 2 | 22	**Onderneming**	Alle verbonden bedrijven of verbonden ondernemingen die een groep vormen in de vorm van directe of indirecte zeggenschap over een bedrijf of onderneming door een ander en die een economische activiteit uitoefenen, ongeacht hun rechtsvorm en de wijze waarop zij worden gefinancierd.
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 6	**Vertrouwde partij**	Een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst.
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 7	**Openbare instantie**	Een staat, regionale of lokale overheden, publiekrechtelijke instellingen en samenwerkingsverbanden bestaand uit één of meer van deze overheidsinstanties of een of meer van deze publiekrechtelijke instellingen, of een private entiteit die door ten minste een van deze autoriteiten, publiekrechtelijke instellingen of verenigingen is gemachtigd tot het verlenen van openbare diensten, wanneer zij in die hoedanigheid optreden
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 8	**Publiekrechtelijke instelling**	Een instelling volgens de definitie in punt 4 van artikel 2, lid 1, van Richtlijn 2014/24/EU van het Europees Parlement en de Raad.
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 9	**Ondertekenaar**	Een natuurlijke persoon die een elektronische handtekening aanmaakt.
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 18	**Conformiteits-beoordelingsinstantie**	Een instantie omschreven in artikel 2, punt 13, van Verordening (EG) nr. 765/2008, die in overeenstemming met die verordening geaccrediteerd is om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten.
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 19	**Verlener van een vertrouwensdienst**	Een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten.

Verordening (EU) 910/2014	eIDAS	Artikel 2 | 20	**Gekwalificeerde verlener van vertrouwensdiensten**	Een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen.
Verordening (EU) 910/2014	eIDAS	Artikel 2 | 24	**Aanmaker van een zegel**	Een rechtspersoon die een elektronisch zegel aanmaakt.
Voorstel Verordening COM(2021) 281	eIDAS 2.0	***Geen andere actoren-termen dan eIDAS (EU) 910/2014.***		