Opzetten van een authentieke bron

Versie 1 – Maart 2019

FOD BOSA DG Digitale Transformatie

Federale overheidsdienst
Beleid en Ondersteuning
Service public fédéral
Stratégie et Appui

INHOUDSOPGAVE

Overzicht

Dit document beschrijft de typische activiteiten en aandachtspunten voor het opzetten van een authentieke bron. De informatie in dit document is bedoeld om andere overheidsdiensten te ondersteunen en het opzetten van authentieke bronnen te versnellen.

Iedere authentieke bron is echter uniek in verwachtingen, gebruik en opzet. De eigenaar van de bron blijft verantwoordelijk om de acties juist uit te voeren, en bijkomende acties te definiëren om te verzekeren dat de bron goed werkt, alle relevante wetgevingen nageleefd worden, en de verwachtingen van de stakeholders ingevuld worden.

Definities en verklaring van de gebruikte termen vindt u terug in sectie 5.

1 Wat is een authentieke bron?

1.1 Het begrip "Authentieke bron"

"Een authentieke bron is een gegevensbank waarin authentieke gegevens gehouden worden. Deze gegevens worden erkend als de unieke en oorspronkelijke gegevens over personen en rechtsfeiten." (Wet houdende oprichting en organisatie van een federale dienstenintegrator, 15 augustus 2012, Art. 2).

Een authentieke bron geldt als dé referentie om welbepaalde gegevens te bekomen en zij biedt specifieke garanties ten aanzien van de *juistheid*, de *volledigheid* en de *beschikbaarheid* van deze gegevens.

- Juistheid: Gegevens die worden opgevraagd uit een authentieke bron kunnen als correct en up-to-date worden beschouwd.
- Volledigheid: De authentieke bron bevat de volledige populatie van gegevens.
- Beschikbaarheid: De authentieke bron is op een vooraf bepaalde frequentie raadpleegbaar voor wie over de correcte machtigingen beschikt.

Het doel van een authentieke bron is om de administratieve verplichtingen van burgers en rechtspersonen te *vereenvoudigen* door te waarborgen dat gegevens die voor de overheid reeds beschikbaar zijn in een authentieke bron niet opnieuw moeten worden meegedeeld aan de federale overheidsdienst.

Een authentieke bron vervult aldus voor meerdere doeleinden een spilfunctie:

1. De natuurlijke en rechtspersonen hoeven deze gegevens in principe *éénmalig aan te leveren* aan deze bron;
2. Een authentieke bron wordt ontsloten voor andere overheidsdiensten, zodat zij deze gegevens opvragen bij deze bron, en zij *niet meer elk afzonderlijk* instaan voor het verzamelen van dezelfde informatie;

(Only-Once Wet, 5 mei 2014, Art. 2).

1.2 Wat zijn de voordelen van een authentieke bron?

Authentieke bronnen leveren voordelen voor zowel de instantie die als eigenaar van de bron optreedt, de gebruikers van de authentieke gegevens als voor de burgers/ondernemingen.

1. Kwaliteit van de data stijgt

Door de *garanties en procedures* is de kwaliteit van de gegevens in een authentieke bron reeds hoog. Bovendien zullen meer mensen dezelfde gegevens gebruiken, waardoor eventuele fouten sneller opgemerkt en gecorrigeerd worden, zodat de kwaliteit van de data verder toeneemt.

2. Duplicaten verminderen

De gegevens hoeven niet meer gedupliceerd te worden in lokale gegevensbanken bij verschillende instanties. Hierdoor kunnen de overheidsdiensten steeds beschikken over de *meest actuele gegevens*.

3. Administratiekosten dalen

Bij wijzigingen van de gegevens dient ment *slechts eenmalig één bron* aan te passen. Beheer, beveiliging, en onderhoud van de gegevens moeten slechts op één plaats te gebeuren.

4. Gegarandeerde beschikbaarheid

Door de garanties op beschikbaarheid, hebben alle gebruikers *duidelijk zicht op de periodes* gedurende de welke zij toegang hebben tot de gegevens.

5. Eenmalige ingave

Burgers en ondernemingen dienen *slechts éénmaal hun gegevens te bezorgen aan de overheid*. Nadien is de overheid verplicht om deze gegevens te ontsluiten en te hergebruiken.

6. Veiligheid stijgt

Door het duidelijk aanduiden van de *rollen* die verantwoordelijk zijn voor de veiligheid (DPO en veiligheidsadviseur) en *procedures* op te stellen voor de verwerking, opslag en uitwisseling van de gegevens, kan de veiligheid verhoogd worden en ongeautoriseerde toegang tot de gegevens vermeden worden.

7. Toegankelijkheid

Wanneer de bron erkent wordt als authentieke bron, wordt deze toegevoegd aan het *overzicht op de website van FOD BOSA*. Alle gebruikers die deze gegevens nodig hebben voor hun eigen doeleinden, kunnen op deze manier *makkelijk* de eigenaar terugvinden en indien nodig *machtiging aanvragen* voor *toegang* bij de bevoegde instantie.

2 Hoe zet ik een authentieke bron op?

2.1 Wat zijn de voorwaarden voor het aanmaken van een authentieke bron, en hoe kan ik deze controleren?

1. *Business reden*: Voordat u een authentieke bron maakt, dient u te bekijken in welke mate uw gegevens gevraagd worden.

> 1. *Vraag uw stakeholders (andere overheidsdiensten) duidelijk te definiëren welke gegevens ze nodig hebben, en hoe vaak ze deze gegevens nodig zullen hebben.*
>
> 2. *Evalueer of de vraag van de stakeholders groot genoeg is om verdere stappen te zetten richting het authentiek maken van de gegevens en de bron.*

2. *Wettelijke criteria:* Een overheidsdienst kan een authentieke bron aanmaken, indien de gegevens voor de welke men een authentieke bron wil creëren, voldoen aan alle volgende 3 criteria:

    1. De registratie van het gegeven en de mededeling ervan aan diverse bestemmelingen vloeit voort uit opdrachten bij of krachtens een wet, een decreet of een ordonnantie toegewezen;
    2. Het gegeven is juist, volledig, beveiligd, en beschikbaar;
    3. De instantie belast met de inzameling en het beheer van de gegevens, geeft garanties ten aanzien van de juistheid, de volledigheid, veiligheid en de beschikbaarheid van het gegeven;

    Indien niet aan alle voorwaarden wordt voldaan (bijvoorbeeld juistheid en volledigheid is niet gegarandeerd) kan de bron niet als authentiek erkend worden.

> 3. Contacteer uw juridische dienst en vraag hun advies over de wettelijke opdrachten die van toepassing zijn op uw organisatie, en hoe de verzameling van de gegevens die u in de authentieke bron wilt opslaan hierin kadert. (*indien er geen wettelijk kader is voor het opslaan en verwerken van gegevens in de authentieke bron, dient dit eerst gecreëerd te worden)*
>
> 4. Doe een zelf-evaluatie over de gegevens die u in de authentieke bron wilt opslaan:
>
> - Hoe hebben we deze gegevens verzameld?
> - Hebben we de gegevens nog recent gevalideerd?
> - Hoe hebben we verzekerd dat de gegevens juist zijn?
> - Hoe hebben we verzekerd dat de gegevens volledig zijn?
> - Hebben we een gevalideerd proces om de gegevens te onderhouden en up-to-date te houden?
> - Hoe verzekeren we de veiligheid van de gegevens (bv dat de toegang beperkt is)?

3. *Eigenaarschap:* Vermits een authentiek gegeven slechts eenmaal kan worden opgeslagen, is het belangrijk om te controleren dat u “de eigenaar” bent van de gegevens en er niet al reeds een eigenaar is toegewezen.

5. Controleer op de lijst van authentieke bronnen, gepubliceerd door FOD BOSA DT (*https://dt.bosa.be/nl/gegevensuitwisseling/authentieke_bronnen/overzicht_authentieke_bronnen*), of er reeds andere bronnen zijn die dezelfde gegevens bevatten. Indien deze bron reeds bestaat, kan u geen eigenaar zijn.

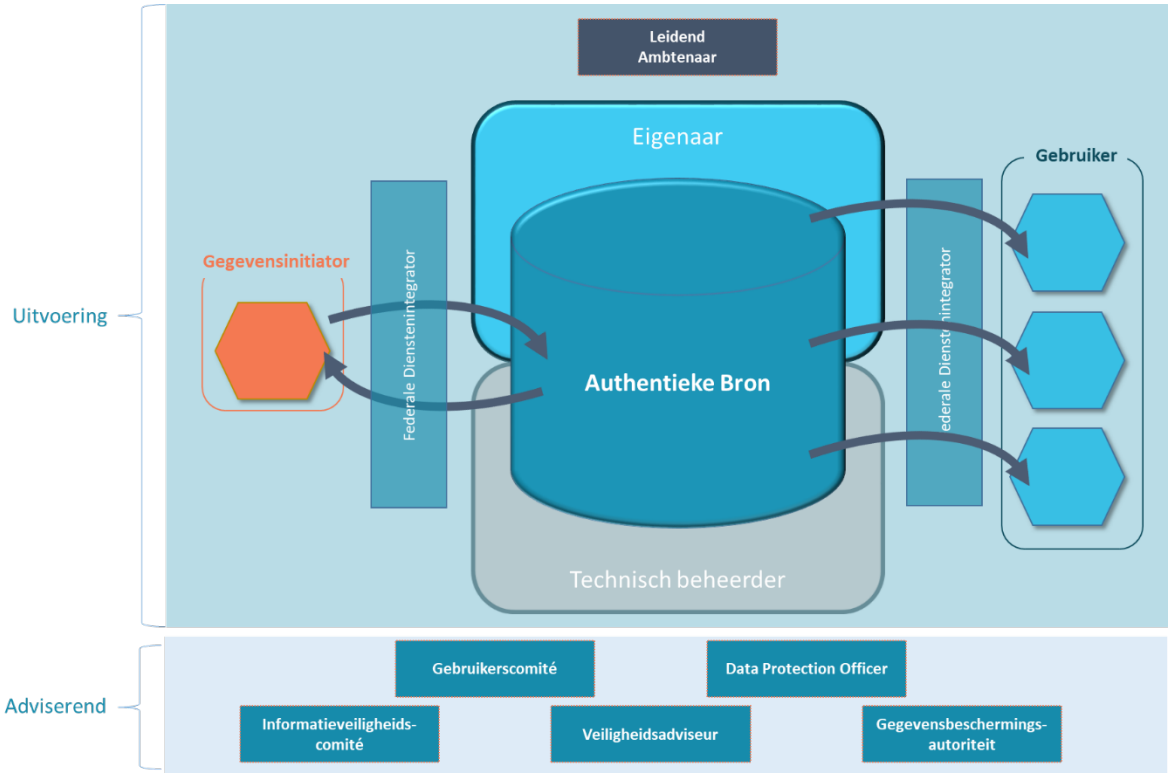
6. Indien er geen bron op de lijst van BOSA DT staat, dient u te verzekeren dat er geen andere overheidsdiensten gelijkaardige gegevens opslaan.

   U kan hiervoor contact opnemen met FOD BOSA DT (https://dtservices.bosa.be/nl/Contact/contactformulier) met de vraag of zij nog kennis hebben van andere (niet-authentieke) bronnen met dezelfde gegevens.
   U kan ook zelf rechtstreeks andere overheidsdiensten contacteren om te bevragen of zij gelijkaardige gegevens opslaan en als authentieke bron willen aanbieden.

   Indien u informatie ontvangt dat er andere bronnen zijn met dezelfde gegevens, dient u contact op te nemen met de eigenaars van die bronnen om overeen te komen wie de "eigenaar" van de gegevens is.

Wanneer de eigenaar is bepaald van een gegeven of reeks van gegevens kan deze instantie het proces starten ter erkenning van de authentieke bron. Voor meer details over het proces van de erkenning van een authentieke bron wordt verwezen naar Sectie 3: "Hoe maak ik een authentieke bron beschikbaar?".

2.2 Wat zijn de rollen & verantwoordelijkheden voor mijn authentieke bron?



Voor iedere authentieke bron zijn er verschillende rollen, zowel voor de governance (het aansturen van de authentieke bron) als voor de uitvoering.

Binnen de *uitvoering* dienen er steeds minimaal 4 rollen gedefinieerd te zijn:

- Gegevensinitiator
- Eigenaar
- Technisch beheerder
- Gebruiker

Daarnaast wordt er voor iedere bron een *governance* structuur opgesteld.

Enerzijds wordt er voor iedere authentieke bron een *gebruikerscomité* opgericht. Dit comité is voor elke authentieke bron uniek is en wordt samengesteld met de belangrijkste stakeholders (vertegenwoordigers van de belangrijkste gebruikers, de eigenaar, de technisch beheerder en de gegevensinitiatoren).

Daarnaast worden 2 rollen voorzien voor veiligheid en privacy: de *veiligheidsadviseur* en indien de authentieke bron persoonsgegevens bevat, dient ook een *Data Protection Officer* te zijn aangesteld. De veiligheidsadviseur en de Data Protection Officer kunnen op hun beurt beroep doen op de volgende 2 organen wanneer het om persoonsgegevens betreft:

- Informatieveiligheidscomité
- Gegevensbeschermingsautoriteit

Dit zijn officiële instanties die advies aan de DPO kunnen verschaffen omtrent privacy en veiligheid van de persoonsgegevens.

Hieronder vindt u een samenvattend overzicht van de typische activiteiten per rol. De exacte verantwoordelijkheden kunnen verschillend zijn voor iedere authentieke bron, en dienen tussen de partijen worden vastgelegd in een service level agreement (zie sectie 2.5: “Welke afspraken tussen de verschillende partijen kunnen opgezet worden?”).

2.2.1 Uitvoering

Er worden 4 grote fases van verwerking van persoonsgegevens geïdentificeerd door de Gegevensbeschermingsautoriteit *(Aanbeveling nr. 09/2012 van 23 mei 2012, Art. 6)*:

- Verwerving: Verzamelen van gegevens, en deze in correct formaat documenteren
- Validatie: Verzekeren dat de gegevens correct zijn
- Beheer: Beheren van het gebruik, toepassing, onderhoud, opslag van gegevens
- Uitwisseling van persoonsgegevens.

Hieronder een overzicht van welke rollen in deze fases betrokken zijn.

	Verwerving	Validatie	Beheer	Uitwisseling
Gegevensinitiator	X	X		X
Eigenaar	X	X	X	X
Technisch beheerder			X	X
Gebruiker				

Rol: Gegevensinitiator

Beschrijving:

De gegevensinitiator(en) is/zijn de verantwoordelijke personen voor de verwerving alsook de *invoering en validatie* van de *oorspronkelijke (authentieke) gegevens.* De gegevensinitiator fungeert als eerste aanspreekpunt voor burgers en ondernemingen.

Verantwoordelijkheden:

- Verwerven gegevens via burgers en ondernemingen
- Toevoegen van de ontbrekende gegevens in het systeem door middel van officiële documenten en/of elektronisch inlezen van gegevens
- Correct registreren van de nieuwe gegevens
- Wijzigen van de gegevens
- Controleren op juistheid en volledigheid
- Uitwisseling van de correcte gegevensbundels met de eigenaar via een vooraf gedefinieerde procedure die gespecifieerd wordt via een SLA met de eigenaar (zie Sectie 2.5: “Welke afspraken tussen de verschillende partijen kunnen opgezet worden?”)
- De registratie van een audit log volgens de bepalingen van de SLA

Rol: Eigenaar

Beschrijving:

De eigenaar heeft de *eindverantwoordelijkheid* over de gegevens. Dit betekent dat eigenaar ook de eindverantwoordelijkheid draagt over de juistheid, volledigheid, beschikbaarheid en beveiliging van de gegevens, alsook de *verwerking* en de *uitwisseling* van de gegevens met andere instanties. De eigenaar van een authentiek gegeven is de overheidsinstantie die voldoet aan alle onderstaande voorwaarden:

- De overheidsdienst heeft een wettelijke opdracht om de gegevens te verzamelen en te verwerken
- De overheidsdienst heeft, meer dan andere overheidsdiensten, gemakkelijke toegang tot de gegevens, en heeft reeds de meeste gegevens verzameld.

Verantwoordelijkheden:

- Verwerving van de gegevens via de gegevensinitiatorvia een vooraf gedefinieerde procedure die gespecifieerd wordt via een SLA met de gegevensinitiator (zie Sectie 2.5: “Welke afspraken tussen de verschillende partijen kunnen opgezet worden?”)
- Strategie opstellen voor het up-to-date brengen van gegevens samen met de gegevensinitiator.
- Eindverantwoordelijkheid over de juistheid, volledigheid, beschikbaarheid en beveiliging van de bron
- Uitwisseling van de correcte gegevensbundels met andere instanties via een vooraf gedefinieerd procedure (zie sectie 3: “Hoe maak ik een authentieke bron beschikbaar?”)
- De registratie van een audit log volgens de bepalingen van de SLA.

Rol: Technisch beheerder

Beschrijving:

De technisch beheerder van de (authentieke) gegevens is de instantie die verantwoordelijk is voor de *technische beleid* inzake het capteren, opslag en onderhoud van de gegevens en de ontsluiting naar zijn dienstenintegrator. De connectie met andere integratoren of instanties wordt gestuurd door de gekoppelde dienstenintegrator. Het technisch beleid gebeurt onder verantwoordelijkheid van de eigenaar van de bron.

Verantwoordelijkheden:

De technische beheerder zorgt onder meer voor:

1. Bepalen en opzetten van technische structuur van de bron
2. Bepalen en opzetten van *datamodel*
3. *Bepalen* van de *interfaces* naar de authentieke bron
4. *Omzetting* naar de correcte *structuur* van de gegevens (bijvoorbeeld XSD of XML)
5. Correcte *verrijking* van de *gegevens* met andere gegevens van de eigenaar, indien dit door middel van een systeem wordt uitgevoerd.

De connectie met andere integratoren of instanties wordt gestuurd door de gekoppelde dienstenintegrator.

Rol: Gebruiker

Iedere natuurlijke persoon of rechtspersoon, met inbegrip van ondernemingen, instellingen, verenigingen en alle onderdelen van de overheid zelf, die de machtiging bezitten om de authentiek gegevens te raadplegen en voor eigen doeleinden te gebruiken.

Een machtiging kan een toelating zijn van het bevoegde orgaan (Informatiebeveiligingscomité of Minister van Binnenlandse Zaken) of gebaseerd zijn op een protocol opgesteld tussen de eigenaar en de gebruiker.

Voorbeelden:

Bron	Gegevensinitiator(en)	Eigenaar	Technisch beheerder
Rijksregister	• Gemeentes	• FOD IBZ	• FOD IBZ
Kruispuntbank van Ondernemingen	• Ondernemingsrechtbank • Ondernemingsloket • RSZ	• FOD Economie	• FOD Economie
Landencodes	• AD Statistiek	• FOD Buitenlandse zaken	• FOD Economie

2.2.2 Governance

Rol: Gebruikerscomité

Beschrijving:

Het gebruikerscomité handelt als overkoepelend orgaan verantwoordelijk voor de *goede werking* van het proces van gegevenswerving en –uitwisseling. Het zorgt ervoor dat alle belangrijke *stakeholders inspraak* hebben in de werking en het beleid van de authentieke bron. Dit sluit aan bij het advies van de Gegevensbeschermingsautoriteit (Aanbeveling nr 09/2012 van 23 mei 2012). Voor elke authentieke bron hoort men een gebruikerscomité op te richten.

Verantwoordelijkheden:

1. Afstemming omtrent gemeenschappelijke verplichtingen, zoals deze opgenomen zijn in de Service Level Agreements tussen de betrokken partijen;
2. Afstemming omtrent het gebruik van de verschillende systemen die gebruikt worden voor de verwerving, de validatie, het beheer en de uitwisseling van de gegevens met de betrokken partijen;
3. Het verlenen van advies voor de optimalisatie van het proces van gegevensverwerving tot gegevensuitwisseling;
4. Afstemming omtrent de samenwerking tussen de stakeholders of de werking van de gehanteerde systemen.

Rol: Data Protection Officer (DPO)

Beschrijving:

Een Data Protection Officer wordt als *deskundige* aangesteld op het gebied van gegevensverwerking met oog op de *privacy* en *veiligheid* van *persoonsgegevens.*

Een overheidsinstantie is verplicht een DPO in te schakelen conform artikel 37, 1, a) van de Europese Verordening 2016/679.

Een privéorgaan dat persoonsgegevens verwerkt voor rekening van een federale overheid, of waaraan een federale overheid persoonsgegevens doorgeeft, wijst een functionaris voor gegevensbescherming aan indien de verwerking van deze gegevens een hoog risico kan inhouden.

Verantwoordelijkheden:

De DPO is – in overeenstemming met de GDPR-wetgeving - verantwoordelijk voor:

1. *Informeren* en *adviseren* van de gegevensbeheerders en –verwerkers (gegevensinitiatoren, eigenaars en technisch beheerders);
   a. Gegevens mogen enkel gebruikt worden volgens de doelstelling waarvoor deze verzameld werden.;
   b. Niet meer gegevens opslaan dan wat nodig is voor het doel waarvoor ze worden opgeslagen;
   c. Gegevens mogen niet langer bewaard worden dan nodig.
2. *Controleren* op naleving van gegevensbeschermingsmaatregelen opgelegd door de Europese en Belgische wetgeving inzake gegevensbescherming.

3. *Eerste contactpunt* omtrent veiligheid en privacy van persoonsgegevens.
4. Beheer van de formaliteiten die komen kijken bij de gegevensverwerking, zoals het opstellen van een *protocolakkoord*. De veiligheidsadviseurs van beide partijen maken een overeenkomst op omtrent de uitwisseling van gegevens. Bij een conflict, kan men het informatieveiligheidscomité consulteren.

Rol: Veiligheidsadviseur

Beschrijving:

Een veiligheidsadviseur adviseert en begeleidt betreffende alle aspecten van informatieveiligheid. Een veiligheidsadviseur wordt als *deskundige* aangesteld op het gebied van gegevensverwerking met oog op de *veiligheid* van *gegevens.*

Verantwoordelijkheden:

1. *Informeren* en *adviseren* van de gegevensbeheerders en –verwerkers;
2. In *samenspraak* met de *technisch beheerder* verzekeren dat de *verwerving, validatie, beheer en de uitwisseling* van de gegevens op een *veilige* manier gebeurt.

Gegevensbeschermingsautoriteit

Beschrijving:

De Gegevensbeschermingsautoriteit is de Belgische overheidsinstelling die toeziet op de *bescherming van de privacy* bij de verwerking van persoonsgegevens. De Gegevensbeschermingsautoriteit is sedert het in voege treden van de GDPR wetgeving in mei 2018 de opvolger van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), beter bekend onder de benaming van “Privacy commissie” (Wet tot oprichting van de Gegevensbeschermingsautoriteit, 3 december 2017).

Verantwoordelijkheden:

- Advies verlenen omtrent privacy en veiligheid bij de verwerking van persoonsgegevens.

Informatieveiligheidscomité (IVC)

Beschrijving:

Het informatieveiligheidscomité is een onafhankelijk orgaan dat bepaalt welke *persoonsgegevens gedeeld* mogen worden en onder welke *veiligheidsvoorwaarden*.

Het IVC bestaat uit een kamer voor de sociale zekerheid en gezondheid en een kamer voor de federale overheid.

(Wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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, 5 september 2018)

Opgelet! Toegang tot gegevens van het Rijksregister of tot gegevens zoals bedoeld in art. 5§2 van de wet op het Rijksregister, evenals het gebruik van het Rijksregisternummer, dienen worden aangevraagd bij de FOD Binnenlandse Zaken (artikel 5 van de wet van 08/08/1983 tot regeling van een Rijksregister van de natuurlijke personen).

Verantwoordelijkheden:

- Machtiging verlenen omtrent de uitwisseling van persoonsgegevens tussen de authentieke bron en de gebruikers.

7. Ken de uitvoeringsrollen van de authentieke bron toe aan specifieke (delen van) organisaties:
   - Gegevensinitiator(en)
   - Eigenaar
   - Technisch beheerder
   - Gebruiker(s)
8. Bepaal wie de rol van veiligheidsadviseur en DPO (indien nodig) zal opnemen.
9. Stel het gebruikerscomité samen, en bepaal hoe die zal opereren (frequentie, agenda, …)
10. Zorg dat de afspraken over de verantwoordelijkheden van iedere partij duidelijk zijn, en vastgelegd worden in SLA's en gebruikersovereenkomsten (zie sectie 2.5: "Welke afspraken tussen de verschillende partijen kunnen opgezet worden?")

2.3 Hoe kies ik een datamodel voor mijn authentieke bron?

Overheidsinstanties mogen slechts éénmalig gegevens bij burgers of bedrijven opvragen *(Only-Once Wet, 5 mei 2014),* waarna deze gegevens tussen de verschillende overheidsdiensten *gedeeld worden voor hergebruik*.

Een authentieke bron bevat enkel *ruwe data*, zonder enige vorm van business logica. Interpretatie van de gegevens en toevoegen van specifieke business logica gebeurt buiten de bron door de eigenaar of de dienstenintegratoren. De eigenaar van de bron kan eventueel wel bijkomende services met business logica aanbieden naast de generieke data.

Het is daarom belangrijk dat het "datamodel" van de authentieke bron goed beschreven is, en dat dit ook gepubliceerd wordt, zodat de andere overheidsinstanties hier rekening mee kunnen houden.

Het datamodel beschrijft *hoe de gegevens in een gegevensbron opgeslagen worden*, en hoe deze gegevens zich tegenover elkaar verhouden. Het datamodel wordt typisch opgesteld door een functionele analist of een IT architect, alvorens de gegevensbron ontwikkeld wordt.

In de beschrijving van het datamodel, is het aanbevolen om volgende elementen te evalueren:

1. Geldigheidsperiode;
2. Inhoud van de gegevens;
3. Nomenclatuur: taalgebruik, naamgevingen, afkortingen …;
4. Technische vereisten;
5. Uniciteit

Daarnaast kunnen nog veel andere elementen worden opgenomen, afhankelijk van de gegevens en de noden van uw bron.

11. Verzamel de verwachtingen van uw stakeholders: welke informatie over uw gegevens *hebben zij nodig?*

12. Vraag uw IT architect of analist van de gegevensbron om de beschrijving van het datamodel op te maken, in functie van de vragen die u heeft gekregen van uw stakeholders. Vertrek vanuit interoperabiliteit-raamwerken (zoals het European Interoperability Framework) om maximale compatibiliteit en uitwisseling mogelijk te maken.

2.4 Waarom en hoe maak ik een privacy audit log en audit trail?

2.4.1 Privacy audit log

In een authentieke bron zitten unieke gegevens, die gedeeld worden met de hele overheid, en die gebruikt worden in officiële processen en communicatie van de overheid. Daarom is het belangrijk dat er steeds kan gecontroleerd worden wanneer en hoe gegevens gebruikt en gewijzigd werden, en dat deze informatie *tegenstelbaar* is.

Daarom dient de finaliteit en proportionaliteit van de gegevens in een authentieke bron steeds geborgd te zijn:

- De *finaliteit* omvat een welbepaald, uitdrukkelijk omschreven en gemachtigd doeleinde.
- De *proportionaliteit* betekent dat de gegevens toereikend, ter zake dienend en niet overmatig mogen zijn, uitgaande van het doeleinde waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt. De data mag ook niet langer worden bewaard dan strikt noodzakelijk voor het gemachtigde doeleinde.

Om te controleren dat iedere authentieke bron de *toepasbare wetgeving naleeft*, moeten alle betrokken partijen een privacy audit log opzetten.

Een *privacy audit log* is een log die automatisch wordt gegeneerd door het systeem en bestaat uit informatie omtrent de *raadpleging* of de *aanmaak, aanpassing & verwijdering* van *gegevens*. Deze log wordt gemaakt door ieder systeem dat betrokken is in de opzet en uitvoering van de authentieke bron. Deze informatie zorgt ervoor dat je per systeem steeds kan nagaan welke consultatie of manipulatie van gegevens zich heeft voorgedaan. De log capteert typisch de volgende informatie over de raadpleging of de wijziging:

1. Het uniek gebruikers ID (wie);
2. Datum en tijd (wanneer);
3. Type van raadpleging/wijziging;
4. Oude waarde en nieuwe waarde van het gegeven (wat);

Naast deze informatie, dienen de betrokken partijen te bepalen welke overige informatie nog in de privacy audit log moet opgenomen worden.

Een privacy audit log moet typisch voor 10 jaar beschikbaar blijven. Vermits de gegevens in de privacy audit log ook persoonsgegevens kunnen zijn, moeten deze nadien verwijderd worden. Voor iedere authentieke bron moet echter individueel worden bepaald hoe lang gegevens beschikbaar moeten blijven, in functie van wettelijke vereisten.

2.4.2 Privacy audit trail

Door de audit logs van alle systemen van de partijen in de ketting (gebruikersorganisatie, dienstenintegrator, beheerder van de bron) samen te leggen kan een privacy audit trail worden gereconstrueerd die weergeeft welke eindgebruiker op welk moment en in welke context een specifieke opvraging heeft uitgevoerd.

Dergelijke audit trail zorgt ervoor dat de transacties die via de dienstenintegrator worden uitgevoerd, kunnen worden gereconstrueerd ter naleving van de wettelijke verplichting omtrent persoonsgegevens. Iedere ketenpartner (gegevensinitiator, eigenaar en gebruiker) blijft wel verantwoordelijk voor de audit logs op zijn eigen systemen.

13. Bespreek met de gegevensinitiator, de eigenaar en de gebruiker van de authentieke bron, hoe de audit logs worden opgezet, welke informatie daarin opgeslagen wordt, en hoe een audit trail kan gemaakt worden. Houdt hierbij rekening met volgende punten:

- **Beveiliging**: Zorg dat iedere privacy audit log is beveiligd en niet kan worden aangepast, verwijderd of uitgezet. Enkel een bevoorrechte gebruiker (bv. Administrator) van het systeem kan de gegevens in de audit log aanpassen, verwijderen of uitzetten bij het volgen van een gecontroleerde procedure. Deze acties worden tevens ook bijgehouden door het systeem;

- **Beschikbaarheid**: De audit trail moet tot 10 jaar gereconstrueerd worden (tenzij er andere wettelijke vereisten zijn). In geval van onderzoek, moeten de gegevens op aanvraag binnen 24u geleverd kunnen worden. De gegevens die de privacy audit log bevat, moeten kunnen worden afgedrukt of geëxporteerd. De gegevens van de audit trail moeten verwijderd worden nadat de wettelijke bewaartermijn verstreken is.

- **Privacy**: Idealiter wordt de burger *ook de mogelijkheid* geboden *om op te* zoeken wie en waarvoor *zijn* of *haar* gegevens heeft geraadpleegd in de voorbije maanden (vb. via een webapplicatie als 'Mijn Dossier' voor het Rijksregister). De eigenaar van de authentieke bron kan zelf de procedure en infrastructuur kiezen waarmee hij dit op een beveiligde manier en met respect voor de privacy dit kan verwezenlijken.

2.5 Welke afspraken tussen de verschillende partijen kunnen opgezet worden?

Om tevreden gebruikers te hebben, is het belangrijk om de verwachtingen op voorhand juist te zetten, en deze zo duidelijk mogelijk te maken in formele afspraken. Deze kunnen opgenomen worden in gebruikersovereenkomsten of Service level Agreements (SLA's).

De gebruikersovereenkomst bepaalt *de rechten en verplichtingen* om de authentieke bron te gebruiken. Deze bevat typisch:

- Beschrijving van de dienst
- Voorwaarden voor het gebruik van de dienst (kosten, doeleinden, volumes, etc.)
- Afspraken rond veiligheid (bv machtigingen, audit trail, …)

Een voorbeeld van een gebruikersovereenkomst is de "gebruikersovereenkomst FSB" (via https://dtservices.bosa.be/nl/services/fsb/aanvraag-van-een-fsb-webservice-fsb-certificaat/ik-vraag-toegang-tot-een-bestaande-fsb)

Een *Service Level Agreement (SLA)* is een *overeenkomst* ter coördinatie van de *informatie-uitwisseling* tussen de 2 betrokken partijen. Deze kan worden opgenomen in de gebruikersovereenkomst, of kan afzonderlijk worden afgesloten. Een SLA omvat een aantal voorwaarden en componenten waaraan beide partijen zich houden. Een SLA kan opgesteld worden tussen de eigenaar en de gebruiker of tussen de eigenaar en de partij verantwoordelijk voor het ontsluiten van de bron (dienstenintegrator).

Onderstaande onderdelen worden idealiter opgenomen in een dergelijke SLA:

1. **Aard van de gegevens:**
   - Naam van de gegevens;
   - Korte beschrijving van de gegevens;
   - Doelstelling voor het bewaren van deze gegevens.
2. **Procedures:**
   - Procedures die verzekeren dat de typische kenmerken (juistheid, volledigheid, beveiliging en beschikbaarheid) van een authentieke bron gewaarborgd zijn bij de verwerving, validatie en uitwisseling van de authentieke gegevens;
   - Procedures die verzekeren dat een correctie of een update van een gegeven, via een vooraf gedefinieerde proces worden gevalideerd en aangepast.
3. **Rollen en verantwoordelijkheden:**
   - De rol van de Gegevensinitiator;
   - De rol van de Eigenaar;
   - De rol van de Technisch Beheerder;
   - De rol van het Gebruikerscomité;
   - (zie Sectie 2.2: "Wat zijn de rollen & verantwoordelijkheden voor mijn authentieke bron?");
4. **Privacy audit log:**
   - Definiëring van wie verantwoordelijk is voor het registreren van de privacy audit log voor elke betrokken partij alsook wie verantwoordelijk is voor de reconstructie van de audit trail bij opvraging. (zie Sectie 2.4: "Waarom en hoe maak ik een privacy audit log en audit trail?")
5. **Technische vereisten:**
   - Change & release management;
     - Proces bepalen voor het voorstellen van wijzigingen;
     - Onderhoud van de systemen (b.v. Vooraf bepaalde momenten voor updates of upgrades).

- Beschikbaarheid van de systemen (b.v. 24/7 of enkel tijdens de kantooruren);
- Mogelijkheden tot connecties met de systemen (b.v. web-based);
- Performantie van de systemen (b.v. responstijd in x milliseconden);
- Capaciteitsbeperkingen van de systemen (b.v. aantal actieve gebruikers per minuut);
- De opvolging van meldingen van incidenten op de systemen en de reactietijd die wordt voorzien (bv. Incidenten met hoge prioriteit moeten binnen 4 uur opgelost worden.).

Bovenstaande onderdelen zijn echter richtlijnen, men kan het gebruikerscomité raadplegen voor advies omtrent andere belangrijke aspecten die dienen opgenomen worden in deze overeenkomst.

14. Bevraag in het gebruikerscomité welke elementen (processen, verantwoordelijkheden, …) vastgelegd moeten worden, en zorg dat deze duidelijk en volledig worden opgenomen.

3 Hoe maak ik een authentieke bron beschikbaar?

Deze sectie geeft een beter begrip omtrent het ontsluiten van een authentieke bron. Hiervoor dienen 2 stappen te gebeuren namelijk:

1. De bron erkennen als authentiek: De vorige secties gaven al toelichting over wat een authentieke bron is en hoe je deze moet opzetten. In deze sectie wordt er verder ingegaan hoe een authentieke bron echter ook kan erkend worden.
2. Tenslotte hoort een bron ontsloten te worden, zodat de gegevens opgevraagd kunnen worden door gebruikers, die hiervoor gemachtigd zijn.

3.1 Hoe kan ik mijn bron laten opnemen op de gepubliceerde lijst van authentieke bronnen van de federale dienstenintegrator

Het proces voor het publiceren van een authentieke bron kan op twee manieren gebeuren.

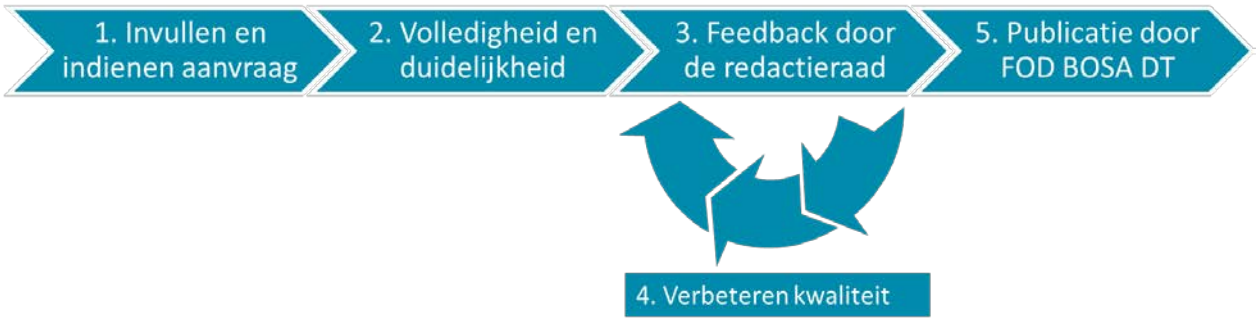
3.1.1 Publicatie als authentieke bron via Koninklijk Besluit

Een gegevensbron kan als authentiek bron verklaard worden, indien hiervoor een Koninklijk Besluit of Wet wordt goedgekeurd. Na publicatie in het Belgisch staatsblad, kunnen de gegevens van uw authentieke bron door FOD BOSA worden opnemen in de lijst van authentieke bronnen.

3.1.2 Publicatie als authentieke bron door de redactieraad

Opmerking: Deze procedure is nog niet finaal. Alle informatie in deze sectie is onderhevig aan wijzigingen. Bij wijziging publiceert FOD BOSA DT een nieuwe versie van dit document.

Het coördinatiecomité van de Federale dienstenintegrator, waarin alle participerende overheden vertegenwoordigd zijn, heeft een “Redactieraad Authentieke Bronnen” aangesteld. Deze redactieraad is gemandateerd om te evalueren dat potentiele gegevensbronnen voldoen aan de vereisten van een authentieke bron, en deze op te nemen in de lijst van authentieke bronnen.



1. Indien men een publicatie wenst door de federale dienstenintegrator van de authentieke bron, vult u de template voor de publicatie in (zie Sectie 4: “Aanvraagformulier publicatie”). De aanvraag wordt ingediend bij FOD BOSA DT, via *https://dtservices.bosa.be/nl/Contact/contactformulier*
2. De federale dienstenintegrator stemt overeen met de aanvrager om de volledigheid en duidelijkheid van de aanvraag te verzekeren.

3. Federale Dienstenintegrator verdeelt aanvraag aan leden van redactieraad. De leden van de redactieraad hebben 3 weken (te bevestigen) om feedback te geven. Indien geen feedback wordt ontvangen, wordt de aanvraag goedgekeurd
4. De Federale Dienstenintegrator ondersteunt de aanvrager om de kwaliteit van de authentiek bron te verhogen.
5. Bij aanvaarding van de aanvraag wordt de eigenaar ingelicht en neemt de federale dienstenintegrator de bron op in de lijst van authentieke bronnen, en voorziet links naar de informatie van de eigenaar over de authentieke bron, die deze dient te publiceren:

    1. De *kenmerken* van het gegeven zoals, de inhoud, de wijze van registratie, de periodiciteit van de aanpassingen en de technische specificaties;
    2. De procedures voor de *registratie*;
    3. Het *beheer* van het gegeven en de *verdeling van de taken* tijdens elke fase van de registratie;
    4. De procedure voor de *toegankelijkheid* van het gegeven;
    5. De procedure om de *juistheid*, de *volledigheid*, de *veiligheid* en de *beschikbaarheid* van het gegeven blijvend te verzekeren;
    6. *Transparante afspraken* met de overheidsdienst die het gegeven wenst af te nemen;
    7. De procedure voor *terugmelding* van fouten in het gegeven en voor *correctie* van het gegeven;
    8. Overleg met het oog op de verbetering van de *kwaliteit*, de *beschikbaarheid* en het *gebruik* van het gegeven;
    9. De omschrijving van de manieren waarop de *betrokkene* zijn *rechten* ten opzichte van de persoonsgegevens die over hem/haar verwerkt worden, kan *uitoefenen.*

3.2 Hoe kan ik mijn bron ontsluiten?

De eigenaar en technische beheerder van de authentieke bron bepalen op welke manier de authentieke bron ontsloten zal worden. Deze keuze is afhankelijk van het type gegevens dat aangeboden wordt en de manier waarop de gebruiker deze gegevens hanteert.

Via de federale dienstenintegrator kan de ontsluiting efficiënt verlopen en wordt verzekerd dat de toegang tot de authentieke bronnen en de snelle uitwisseling van gegevens op een veilige en homogene manier gebeurt.

Enkele mogelijkheden voor het ontsluiten van een authentieke bron worden hieronder opgesomd:

1. Webservice: via de technologie van REST of SOAP
2. File Transfer Protocol (FTP)
3. HTML
4. Excel
5. Website publicatie
6. …

Verder dienen zij een keuze te maken omtrent frequentie (real time versus batch processing) van de verwerking van de gegevens en de beschikbaarheid van zijn bron (continu versus periodiek). Bij deze beslissingen kan de eigenaar adviezen van het coördinatiecomité, de veiligheidsadviseur en de technisch beheerder in rekening nemen. De technisch beheerder dient nadien de nodige technologische ondersteuning te bieden voor de beslissingen omtrent de ontsluiting van de authentieke bron.

Typisch worden volgende activiteiten opgenomen in de ontsluiting van de authentieke bron:

- Opmaken van functionele beschrijving van de bron
- Definiëren van test-cases
- Opzetten van een testomgeving, eventueel met geanonimiseerde gegevens
- Documentatie van de functionele en technische error-codes.

Voor meer informatie over deze activiteiten kan u contact opnemen met FOD BOSA DT.

4 Aanvraagformulier publicatie

Via dit aanvraagformulier kan u alle gegevens van uw mogelijke authentieke bron invullen. Deze checklist dient u ook te gebruiken bij het indienen van uw publicatieaanvraag in te dienen (zie sectie 3.1.2: “Publicatie als authentieke bron door de redactieraad”)

1. Business Case

Geef een korte beschrijving van de doelstelling van uw authentieke bron, en de mogelijke gebruikers die deze data kunnen bevragen.

2. Wettelijke opdracht

Gelieve aan te duiden welke wettelijke basis, ordonnantie of andere informatie van toepassing is op uw organisatie, waaruit u concludeert dat u de wettelijk opdracht hebt om deze gegevens te verzamelen en op te slaan in een authentieke bron:

3. Beschrijving van de authentieke bron:

Beschrijf welke gegevens u zal opslaan in de authentieke bron

4. Garantie van juistheid en volledigheid:

Beschrijf hoe u verzekert dat uw gegevens volledig en juist zijn, en hoe u kan verzekeren dat deze in de toekomst ook volledig en juist blijven.

Is er een terugkoppelprocedure (bv meldpunt) om fouten te corrigeren?

5. Rollen

Geef aan wie de onderstaande rollen zal opnemen:

Gegevensinitiator(en)	*Wie zal de gegevens invoeren en aanpassen indien nodig?*
Eigenaar	*Wie wordt eigenaar van uw authentieke bron*
Technisch beheerder	*Wie zal het technisch beleid doen van uw authentieke bron?*
Gebruiker(s)	*Wie zijn de potentiële gebruikers van uw authentieke bron?*
Gebruikerscomité	*Hoe wordt het gebruikerscomité samengesteld?*
Data Protection Officer	*Welke persoon zal als DPO optreden voor uw authentieke bron?*
Veiligheidsadviseur	*Welke persoon zal als veiligheidsadviseur optreden voor uw authentieke bron ?*

6. Privacy audit log & trail

Gelieve aan te geven dat u voldoet aan volgende aspecten van de privacy audit logs.:

Ieder systeem betrokken in mijn authentieke bron heeft een privacy audit log	*Ja/Nee*
De privacy audit logs van alle systemen worden 10 jaar bijgehouden	*Ja/Nee*
De gegevens uit de privacy audit logs kunnen binnen 24u aangeleverd worden op verzoek	*Ja/Nee*

7. Datamodel

Lijst kort de verwachtingen van uw stakeholders op: welke informatie over uw gegevens hebben zij nodig?

Vertaal bovenstaande lijst in concrete en unieke dataelementen.

8. Service level agreement

Is er een service level agreement voorzien tussen alle betrokken partijen? Indien niet, motiveer kort waarom.

Is het gebruikerscomité geraadpleegd voor advies omtrent wat moet opgenomen worden in de service level agreement(s)?

Wat moet er beschreven staan in de service level agreement(s) omtrent de aard van de gegevens?

Welke technische vereisten dienen er opgenomen te worden in de service level agreement(s) voor de uitwisseling van de gegevens?

5 Definities

Authentieke bron	*"Een authentieke bron is een gegevensbank waarin authentieke gegevens gehouden worden" (Wet houdende oprichting en organisatie van een federale dienstenintegrator, 15 augustus 2012, Art. 2).* Deze gegevens worden erkend als de originele gegevens en vormen bijgevolg de meest betrouwbare bron. Authentieke bronnen zorgen ervoor dat gegevens over een persoon of een bedrijf slechts éénmalig worden ingezameld *Gedetailleerde informatie over de authentieke bronnen en gegevens vindt u in hoofdstuk 1*.
Authentiek gegeven	*"Dit is een gegeven dat door een instantie ingezameld en beheerd wordt in een gegevensbank en geldt als uniek en oorspronkelijk gegeven over de desbetreffende persoon of rechtsfeit, zodanig dat andere instantie ditzelfde gegeven niet meer hoeven in te zamelen" (Wet houdende oprichting en organisatie van een federale dienstenintegrator, 15 augustus 2012, Art. 2) .* *Gedetailleerde informatie over de authentieke bronnen en gegevens vindt u in hoofdstuk 1*
Coördinatiecomité (van de federale dienstenintegrator)	*"Het coördinatiecomité brengt aan de federale dienstenintegrator advies uit over:* 1. *de mogelijke ontsluiting via de federale dienstenintegrator van gegevensbanken of authentieke bronnen;* 2. *de mogelijke aanpassing van de geselecteerde authentieke bronnen zodat, voor zover mogelijk, enkel authentieke gegevens worden ontsloten;* 3. *het gebruik van verwijzingen naar het authentiek gegeven in de authentieke bron wat gegevens betreft die geheel of gedeeltelijk overlappen met een authentiek gegeven in een authentieke bron;* 4. *het vastleggen van een regelbank voor één of meerdere gegevensbanken;* 5. *de verdeling van aansprakelijkheid tussen de federale dienstenintegrator, de participerende overheidsdiensten en de andere dienstenintegratoren rekening houdend met de bevoegdheden die hen door deze wet zijn toegewezen."* *(Wet houdende oprichting en organisatie van een federale dienstenintegrator, 15 augustus 2012, Art. 27. §1) .*

Datamodel	Het datamodel beschrijft hoe de gegevens in een gegevensbron opgeslagen worden, en hoe deze gegevens zich tegenover elkaar verhouden. Het datamodel wordt typisch opgesteld door een functionele analist of een IT architect, alvorens de gegevensbron ontwikkeld werd. *Gedetailleerde informatie over een datamodel vindt u in hoofdstuk 2.3.*
Data Protection Officer (DPO)	De GDPR wetgeving van 25 mei 2018 verplicht alle overheidsinstanties een Data Protection Officer rol in te voeren. De DPO wordt als deskundige aangesteld op het gebied van gegevensverwerking met oog op de privacy en veiligheid van persoonsgegevens in overeenstemming met de GDPR wetgeving van 25 mei 2018. *Gedetailleerde informatie over de DPO vindt u in hoofdstuk 2.2.2*
Dienstenintegrator	*"Een dienstenintegrator is een instantie die door of krachtens de wet belast is, binnen een bepaald overheidsniveau of in een bepaalde sector met dienstenintegratie"* (Wet houdende oprichting en organisatie van een federale dienstenintegrator, 15 augustus 2012, Art. 2). Dienstenintegratie is de organisatie van elektronische gegevensuitwisseling over instanties heen en de geïntegreerde ontsluiting van deze gegevens. Er zijn 3 federale dienstenintegratoren: - FOD BOSA DG Digitale Transformatie (voorheen Fedict); - e-Health; - Kruispuntbank Sociale zekerheid.
Eigenaar	De eigenaar is een van de noodzakelijke rollen voor het beheren van een authentieke bron. De eigenaar heeft de eindverantwoordelijkheid over de gegevens. Dit betekent dat eigenaar ook de eindverantwoordelijkheid draagt over de juistheid, volledigheid en beschikbaarheid van de gegevens, alsook de verwerking en de uitwisseling van de gegevens met andere instanties. *Gedetailleerde informatie over de rollen voor het beheer van een authentieke bron vindt u in hoofdstuk 2.2.*
Fedict-wet	"De wet van 15/08/2012 houdende de oprichting en organisatie van een federale dienstenintegrator" is algemeen bekend als de Fedict-wet.

	FOD BOSA DG DT (voorheen Fedict) werd hierin benoemd als dienstenintegrator die als taak heeft om de gegevensuitwisseling te vereenvoudigen en te optimaliseren tussen enerzijds de participerende overheidsdiensten (nl. alle federale overheidsdiensten- en instellingen exclusief deze die vallen onder de Sociale Zekerheid) onderling en tussen de participerende overheidsdiensten en de andere dienstenintegratoren anderzijds
Gebruiker	Iedere natuurlijke persoon of rechtspersoon, met inbegrip van ondernemingen, instellingen, verenigingen en alle onderdelen van de overheid zelf, die de machtiging bezitten om de authentiek gegevens te raadplegen en voor eigen doeleinden te gebruiken. Deze machtiging wordt toegewezen op basis van het advies van de gegevensbeschermingsautoriteit.
Gebruikerscomité	Iedere authentieke bron dient een gebruikerscomité te hebben. Het gebruikerscomité handelt als overkoepelend orgaan verantwoordelijk voor de goede werking van het proces van gegevenswerving en –uitwisseling. Het zorgt ervoor dat alle belangrijke stakeholders inspraak hebben in de werking en het beleid van de authentieke bron. (Advies 18/2012 van de Commissie voor de bescherming van de persoonlijke levenssfeer, 23 mei 2012). *Gedetailleerde informatie over de rollen voor het beheer van een authentieke bron vindt u in Sectie 2: "Hoe zet ik een authentieke bron op".*
Gegevensbeschermingsautoriteit	De Gegevensbeschermingsautoriteit is de Belgische overheidsinstelling die toeziet op de bescherming van de privacy bij de verwerking van persoonsgegevens. De Gegevensbeschermingsautoriteit is sedert het in voege treden van de GDPR wetgeving op 25 mei 2018 de opvolger van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), beter bekend onder de benaming van "Privacy commissie" (Wet tot oprichting van de Gegevensbeschermingsautoriteit, 3 december 2017, Art. 2 & Art. 4).
Gegevensinitiator	De gegevensinitiator is de organisatie verantwoordelijk voor het verzamelen, ingeven, valideren en corrigeren van gegevens. *Gedetailleerde informatie over de rollen voor het beheer van een authentieke bron vindt u in sectie 2.2.*

General Data Protection Regulation (GDPR)	De GDPR is een Europese verordening (in voege sinds 25 mei 2018) die geharmoniseerd is met de Europese privacywetgeving. De GDPR heeft als doel een betere bescherming te bieden voor persoonsgegevens van individuen. Deze wet heeft twee toepassingsgebieden. Enerzijds is ze van toepassing op de verwerking van persoonsgegevens door Europese bedrijven en organisaties, ongeacht de locatie waar deze verwerking plaatsvindt. Anderzijds is de wet van toepassing op de verwerking van de persoonsgegevens van EU-onderdanen door bedrijven die niet binnen de EU zijn gelokaliseerd, wanneer deze bedrijven goederen of diensten aanbieden aan deze onderdanen binnen de EU, of het gedrag van EU-onderdanen monitoren, voor zover dit gedrag binnen de Unie plaatsvindt (General Data Protection Regulations, 25 mei 2018)
Informatieveiligheidscomité (IVC)	Het informatieveiligheidscomité is een onafhankelijk orgaan dat bepaalt welke persoonsgegevens gedeeld mogen worden en onder welke veiligheidsvoorwaarden. Het IVC bestaat uit een kamer voor de sociale zekerheid en gezondheid en een kamer voor de federale overheid (Wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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, 5 september 2018)
Only-Once Wet	"*De wet van 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en de instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren*" is algemeen gekend als de Only-Once wet. Deze wet bepaalt dat instanties beschikbare gegevens uit de zogenaamde (authentieke) bronnen dienen te hergebruiken in plaats van ze opnieuw bij burgers of bedrijven op te vragen. Hierbij wordt het belang van een correcte gegevensuitwisseling tussen de verschillende instanties benadrukt.
Privacy audit log	Een privacy audit log bestaat uit informatie omtrent de raadpleging of de wijziging van gegevens - aanmaak, aanpassing & verwijdering - die automatisch gegeneerd wordt door het systeem. Deze informatie zorgt ervoor dat je per systeem steeds kan nagaan

	welke consultatie of manipulatie van gegevens zich heeft voorgedaan. *Gedetailleerde informatie over de privacy audit log & trail vindt u in sectie 2.4*.
Privacy audit trail	Een privacy audit trail wordt geconstrueerd door de audit logs van de verschillende ketenpartners samen te voegen. Dergelijke audit trail zorgt ervoor dat de transacties die via de dienstenintegrator worden uitgevoerd, kunnen worden gereconstrueerd ter naleving van de wettelijke verplichting *(Wet ter bescherming van de persoonlijke levenssfeer, 8 december 1992, Art. 16).* *Gedetailleerde informatie over de privacy audit log & trail vindt u in sectie 2.*4
Service Level Agreement	Een service Level Agreement (SLA) is een overeenkomst ter coördinatie van de informatie-uitwisseling tussen de 2 betrokken partijen. Een SLA omvat een aantal voorwaarden en componenten waaraan beide partijen zich houden. *Gedetailleerde informatie over SLA's vindt u in sectie 2.5.*
Technisch beheerder	De technisch beheerder van de (authentieke) gegevens is de instantie die onder verantwoordelijkheid van de eigenaar zorgt voor het technische beleid inzake het capteren, opslag en onderhoud van de gegevens en de ontsluiting naar zijn dienstenintegrator. De connectie met andere integratoren of instanties wordt gestuurd door de gekoppelde dienstenintegrator. *Gedetailleerde informatie over de rollen voor het beheer van een authentieke bron vindt u in sectie 2.*
Veiligheidsadviseur	Een veiligheidsadviseur adviseert en begeleidt betreffende alle aspecten van informatieveiligheid. Een veiligheidsadviseur wordt als deskundige aangesteld op het gebied van gegevensverwerking met oog op de veiligheid van gegevens.