

Algemene inleiding - Logboek dataverwerkingen

Logius Praktijkrichtlijn
Werkversie 09 december 2024



Deze versie:

https://logius-standaarden.github.io/logboek-dataverwerkingen_Inleiding/

Laatst gepubliceerde versie:

https://gitdocumentatie.logius.nl/publicatie/api/logboek_algemeen/

Laatste werkversie:

https://logius-standaarden.github.io/logboek-dataverwerkingen_Inleiding/

Redacteurs:

Vedran Bilanovic (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Eelco Hotting (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Auteurs:

Nil Barua (Logius)

Martin van der Plas (Logius)

Jeroen Mulder (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Doe mee:

[GitHub Logius-standaarden/logboek-dataverwerkingen](https://github.com/logius-standaarden/logboek-dataverwerkingen)

[Dien een melding in](#)

[Revisiehistorie](#)

[Pull requests](#)

Dit document is ook beschikbaar in dit niet-normatieve formaat: [pdf](#)



Dit document valt onder de volgende licentie:
[Creative Commons Attribution 4.0 International Public License](#)

Samenvatting

De overheid wil voor burgers en bedrijven zo transparant mogelijk zijn in de omgang met hun gegevens. Daarom is het bij de informatieverwerking in datasets belangrijk om voor elke mutatie of raadpleging vast te leggen wie deze actie wanneer uitvoert, en waarom. Deze herleidbaarheid speelt zowel een rol in het kader van de wetgeving op het gebied van privacy als ook het streven naar openheid en transparantie bij de overheid. Voor een optimale samenwerking over organisaties en bronnen heen is voor deze logging een algemene standaard nodig.

Het project Logboek Dataverwerkingen (voorheen: Verwerkingenlogging) maakt deel uit van het [actieplan Data bij de Bron](#) en onderzoekt met Digilab in samenwerking met diverse overheidspartijen (ministeries, uitvoeringsorganisaties en gemeentes) of we op basis van de tot nu toe opgedane inzichten een overheidsbrede standaard kunnen vaststellen. Na het succesvol beproeven van de standaard wordt deze voorgesteld voor opname in de [‘Pas toe of leg uit’-lijst van het Forum voor Standaardisatie](#).

bron: <https://digilab.overheid.nl/projecten/logboek-dataverwerkingen/>

§ Verwijzingen

De Logboek Dataverwerkingen (LDV) standaard bestaat uit de volgende drie documenten:

Beschrijving van het document	Gepubliceerde versie	Werk versie	Repository
1. De LDV Normatieve Standaard	-	Logboek dataverwerkingen (werkversie)	logboek-dataverwerkingen
2. De Algemene Inleiding	-	De Algemene Inleiding (werkversie)	logboek-dataverwerkingen_Inleiding

Beschrijving van het document	Gepubliceerde versie	Werk versie	Repository
3. het Juridische Beleidskader	-	Juridisch Beleidskader (werkversie)	logboek-dataverwerkingen_Juridisch-beleidskader
4. LDV Extensie voor objecten	-	Onderzoek logboek dataverwerkingen voor (geo) objecten	logboek-dataverwerkingen-voor-objecten

Status van dit document

Dit is een werkversie die op elk moment kan worden gewijzigd, verwijderd of vervangen door andere documenten. Het is geen door het TO goedgekeurde consultatieversie.

Inhoudsopgave

Samenvatting

Verwijzingen

Status van dit document

1. Inleiding

1.1 Aanleiding en context van Logboek dataverwerkingen

1.1.1 Standaard Logboek dataverwerkingen

1.2 Scope van de Standaard Logboek dataverwerkingen

1.2.1 In scope van deze standaard

1.2.2 Buiten scope van deze standaard

1.3 Totstandkoming van de standaard

1.3.1 aanleiding en achtergrond

1.3.2 Interdisciplinaire aanpak

1.3.3 Beheer en doorontwikkeling

2. FAQ

2.1 Vragen

2.1.1 Wat is het doel van de standaard Logboek Dataverwerking?

2.1.2 Wie kan de standaard Logboek Dataverwerking gebruiken?

2.1.3 Is de standaard Logboek Dataverwerking alleen bedoeld voor de verwerking van persoonsgegevens?

2.1.4 Is in de standaard Logboek Dataverwerking opgenomen hoe logging plaatsvinden ten aanzien van beveiligingsincidenten (denk ook aan technische systeemactiviteiten en toegangsbeheer)?

2.1.5 Wie is eigenaar en beheerder van de standaard Logboek Dataverwerking?

2.1.6 Is mijn organisatie verplicht de standaard Logboek Dataverwerking te implementeren?

2.1.7 Wat is de relatie van Audit Log met de standaard Logboek Dataverwerking?

2.1.8 Zijn er dingen die je moet aanpassen aan je Audit Log als je de standaard Logboek Dataverwerking implementeert?

2.1.9 Kan je de standaard Logboek Dataverwerking implementeren als je een cloud (SaaS) applicatie gebruikt?

2.1.10 Is de performance van de standaard Logboek Dataverwerking getest? / Zal de standaard Logboek Dataverwerking de performance van mijn applicaties beperken?

2.1.11 Hoe werken het Register van verwerkingsactiviteiten (RvVA) en het Logboek Dataverwerkingen samen?

2.1.12 Moet ik mijn RvVA aanpassen als ik deze standaard Logboek Dataverwerking implementeer?

2.1.13 Mijn organisatie heeft geen RvVA API. (Hoe) Kan ik dan nog steeds de standaard Logboek Dataverwerking implementeren?

2.1.14 Hoe gedetailleerd moet mijn RvVA zijn om de standaard Logboek Dataverwerking te implementeren? / Heeft de detailniveau van mijn RvVA invloed op de werking van deze standaard?

2.1.15 Wat gebeurt er als ik mijn RvVA wil wijzigen na de implementatie van de Logboek Dataverwerkingenstandaard?

3. Architectuur

3.1 Inleiding Architectuur

3.2 De relatie tussen logboekelementen, waarom eigenlijk?

3.2.1 Welke relatiegegevens moeten er dan worden opgeslagen per Logregel?

3.2.2 Het logboek en het Register van Verwerkingsactiviteiten

3.2.3 TraceId als grootste gemene deler

3.2.4	Relatie tussen (sub)Operations
3.2.5	Voorbeeld van een traceringsconstructie
3.2.6	Situatieschets
3.2.7	Procesgang
3.2.8	traceId
3.2.9	OperationId
3.2.10	Totaalbeeld
3.3	Canoniek Gegevensmodel
3.3.1	attribute
3.3.2	dplCoreDataSubjectId
3.3.3	dataSubjectCategories
3.3.4	dplCoreProcessingActivityId
3.3.5	endTime
3.3.6	envisagedTimeLimit
3.3.7	foreignOperation.entity
3.3.8	foreignOperation.operationId
3.3.9	LegalBasis
3.3.10	LegalBasisComment
3.3.11	operationId
3.3.12	operationName
3.3.13	parentDplCoreProcessingActivityId
3.3.14	parentOperationId
3.3.15	personalDataCategories
3.3.16	purpose
3.3.17	recipientsCategories
3.3.18	resource.attribute
3.3.19	resource.name
3.3.20	resource.version
3.3.21	startTime
3.3.22	statusCode
3.3.23	traceId

4. Besluitenlijst

4.1	Logregels bevatten alleen wat nodig is voor verantwoording door verantwoordelijke
4.1.1	Context en probleemstelling
4.1.2	Besluit
4.1.3	Gevolgen
4.2	Logregels bevatten geen gegevens die al vastliggen in een Register
4.2.1	Context en probleemstelling
4.2.2	Besluit
4.2.3	Gevolgen
4.2.3.1	Loggen van een verwerking
4.2.3.2	Tonen van een verwerking
4.3	Bewaartermijnen worden in het Profiel vastgelegd
4.3.1	Context en probleemstelling
4.3.2	Besluit
4.3.3	Gevolgen
4.4	Geen gegevens over gebruikers in logregels
4.4.1	Context en probleemstelling
4.4.2	Besluit
4.4.3	Gevolgen
4.5	Standaard beschrijft geen interface voor verwijderen van logs
4.5.1	Context en probleemstelling
4.5.2	Besluit
4.5.3	Gevolgen
4.6	Vertrouwelijkheid wordt vastgelegd per Verwerkingsactiviteit
4.6.1	Context en probleemstelling
4.6.2	Besluit
4.6.3	Gevolgen
4.7	Verwijzingen naar Registers zijn zo los mogelijk
4.7.1	Context en probleemstelling

4.7.2	Besluit
4.7.3	Gevolgen
4.8	Log Sampling is niet toegestaan
4.8.1	Context en probleemstelling
4.8.2	Besluit
4.8.3	Gevolgen
5.	Voorbeelden
5.1	Parkeervergunning - inzien
5.1.1	Situatieschets (Parkeervergunning - inzien)
5.1.2	Uitgangspunten (Parkeervergunning - inzien)
5.1.3	Globaal proces (Parkeervergunning - inzien)
5.1.4	Logging van gegevens (Parkeervergunning - inzien)
5.1.5	Relatie tussen gegevens (Parkeervergunning - inzien)
5.1.6	Relatie met de standaard Logboek dataverwerkingen (Parkeervergunning - inzien)
5.2	Parkeervergunning - wijzigen
5.2.1	Situatieschets (Parkeervergunning - wijzigen)
5.2.2	Uitgangspunten (Parkeervergunning - wijzigen)
5.2.3	Globaal proces (Parkeervergunning - wijzigen)
5.2.4	Logging van gegevens (Parkeervergunning - wijzigen)
5.2.5	Relatie tussen gegevens (Parkeervergunning - wijzigen)
5.2.6	Relatie met de standaard Logboek Dataverwerkingen (Parkeervergunning - wijzigen)
5.2.6.1	Standaard Logverwerkingen: paragraaf 3.3.1 Gedrag
5.3	Registratie Verhuizing - Eenvoudig, traditioneel systeem
5.3.1	Situatieschets (Registratie Verhuizing - Eenvoudig)
5.3.2	Uitgangspunten (Registratie Verhuizing - Eenvoudig)
5.3.3	Globaal proces (Registratie Verhuizing - Eenvoudig)
5.3.4	Logging van gegevens (Registratie Verhuizing - Eenvoudig)
5.3.5	Relatie tussen gegevens (Registratie Verhuizing - Eenvoudig)
5.3.6	Relatie met de standaard Logboek dataverwerkingen (Registratie Verhuizing - Eenvoudig)
5.4	Registratie verhuizing – Opvragen meerdere BSN's
5.4.1	Situatieschets (Registratie verhuizing)
5.4.2	Uitgangspunten (Registratie verhuizing)
5.4.3	Globaal proces (Registratie verhuizing)
5.4.4	Logging van gegevens (Registratie verhuizing)
5.4.5	Relatie tussen gegevens (Registratie verhuizing)
5.4.6	Relatie met de standaard Logboek dataverwerkingen (Registratie verhuizing)
5.5	Voorbeeldapplicaties
5.5.1	Register van de verwerkingsactiviteiten (RvvA)
6.	Conformiteit
A.	Index
A.1	Begrippen gedefinieerd door deze specificatie
A.2	Begrippen gedefinieerd door verwijzing
B.	Referenties
B.1	Normatieve referenties
B.2	Informatieve referenties

§ 1. Inleiding

Het idee is dat het Logboek Dataverwerkingen een basis biedt om te zorgen dat de overheid precies de data logt die zij nodig heeft om verantwoording af te leggen over haar taken. Niet meer, maar ook niet minder. En om te zorgen dat organisaties data zodanig loggen dat zij zich niet alleen over een eigen handelen kunnen verantwoorden, maar ook over hun gezamenlijk handelen als “de overheid”.

§ 1.1 Aanleiding en context van Logboek dataverwerkingen

Informatiehuishouding van de overheid moet op orde worden gebracht. De overheid werkt ten dienste van burgers en bedrijven. De overheid verwerkt daarvoor informatie van deze burgers en bedrijven. Het is belangrijk dat de informatiehuishouding van de overheid op orde is, zodat de overheid transparant en aanspreekbaar is, en zich daarover goed kan verantwoorden.

Dat werkt als een soort vliegwiel, omdat daardoor ook de kwaliteit van de informatie beter wordt. De overheid kan daarmee betere dienstverlening bieden en ook zorgen dat de burger minder met fouten wordt geconfronteerd, of dat overheden fouten beter en sneller kunnen herstellen als deze zich onverhoopt voordoen.

Eenduidige en integrale verantwoording over dataverwerkingen door de overheid. Belangrijk is dat overheidsorganisaties op een eenduidige manier met informatie omgaan en op een eenduidige manier informatie met elkaar uitwisselen.

Voorafgaand aan informatie-uitwisseling is het belangrijk dat transparant is waarom dat gebeurt en, achteraf moet de overheid verantwoording kunnen afleggen over de data en de wijze waarop de data is verwerkt. Zo kunnen eventuele fouten of onregelmatigheden worden hersteld en kunnen burgers hun rechten op grond van de AVG geldend maken (oa. inzage en correctie). Het gaat daarbij niet alleen om overheidsorganisaties afzonderlijk, maar het gaat er ook – juist – om dat “dé overheid” zich als geheel ten opzichte van de burger kan verantwoorden.

Een belangrijk instrument om verbetering van de informatiehuishouding te bereiken is standaardisatie. Op diverse aspecten is daarom standaardisatie nodig en worden deze ontwikkeld. Een van deze aspecten is de wijze waarop overheden zich verantwoorden. Standaardisatie daarvan vormt daarmee een puzzelstukje in het bredere geheel. Hiermee kunnen overheden hun dataverwerkingen op dezelfde wijze verantwoorden en deze verantwoording onderling relateren, zodat de keten van dataverwerkingen tussen organisaties compleet inzichtelijk kan worden gemaakt.

§ 1.1.1 Standaard Logboek dataverwerkingen

Om eenduidige verantwoording over dataverwerkingen te regelen en te zorgen dat deze verantwoording over overheidsorganisaties heen relateerbaar is, is de standaard Logboek Dataverwerkingen in ontwikkeling. De standaard heeft tot doel geautomatiseerd eenduidige verslaglegging van dataverwerkingen binnen organisaties te bevorderen, en dataverwerkingen tussen organisaties aan elkaar te relateren.

§ 1.2 Scope van de Standaard Logboek dataverwerkingen

Dit beschrijft een overzicht van de scope van de standaard, inclusief de zaken die wel en niet binnen de scope van de standaard vallen.

§ 1.2.1 In scope van deze standaard

Logging over dataverwerkingen in overheidssystemen. Het uitgangspunt van deze standaard is de verantwoordingsplicht van de overheid over de uitvoering van haar taken en de wetten en kaders die daarbij horen.

§ 1.2.2 Buiten scope van deze standaard

De volgende zaken worden **niet** behandeld in deze standaard:

- **Toegangsbeheer:** Logging rondom toegang tot systemen en data, waarbij zowel succesvolle als mislukte pogingen om toegang te krijgen worden vastgelegd. Deze logs zijn bedoeld voor het controleren van wie toegang heeft tot gevoelige informatie en voor het detecteren van ongeautoriseerde toegang.
- **Toegangsverlening Logboek:** De standaard specificeert geen functionaliteit rondom het aanmaken en beheren van toegangs- en onderhoudsprofielen ten behoeve van het logboek. Voor meer informatie zie [Federatieve Toegangsverlening](#).

- **Gebruikersactiviteiten:** Logging van namen van gebruikers die data gebruiken of verwerken.
- **Beveiligingsincidenten:** Specifieke logs voor incidenten die de beveiliging kunnen beïnvloeden, zoals malware-detectie, aanvallen of misbruik. Dit soort logging is van groot belang voor het identificeren van bedreigingen en het kunnen reageren op incidenten.
- **Technische en Systeemlogs:** Logging van systeemfouten, configuratiewijzigingen en technische problemen. Deze logs helpen bij het waarborgen van de stabiliteit en betrouwbaarheid van IT-systemen en ondersteunen het oplossen van technische problemen.
- **Logging ten behoeve van motivatie totstandkoming besluitvorming:** anders dan uitgevoerde dataverwerkingen (niet: beslisregels, algoritmes, etcetera).
- **Correcties op- en verwijdering van verwerkte data:** dit wordt gezien als verwerking en volgt de gewone route van datalogging. Voor meer informatie zie [besluit 4.5](#).
- **Beperkingen op informatieplichten (bijvoorbeeld indien er een strafrechtelijk onderzoek plaatsvindt):** het is aan de organisatie zelf om procedures te implementeren om beperking van inzage uit te voeren. Voor meer informatie zie [besluit 4.6](#).

§ 1.3 Totstandkoming van de standaard

§ 1.3.1 aanleiding en achtergrond

Het Logboek Dataverwerkingen is een doorontwikkeling van de conceptstandaard GEMMA Verwerkingenlogging, die door VNG Realisatie is gemaakt met als doel de naleving van AVG-verplichtingen rondom de verwerking van persoonsgegevens te verbeteren.

In 2023 heeft het Ministerie van Binnenlandse Zaken, in samenwerking met verschillende overheidspartijen, een project gestart om de GEMMA Verwerkingenlogging-standaard verder te ontwikkelen. Het uitgangspunt was het vergroten van de transparantie van de overheid en het verbeteren van de informatiepositie van de burger. Vanaf 2024 werd breder gekeken dan alleen de AVG; wettelijke kaders, zoals verantwoordingsverplichtingen, werden als uitgangspunt genomen voor het vormgeven van de standaard. Om aan deze eisen te voldoen, is de standaard aangepast en hernoemd tot Logboek Dataverwerkingen.

§ 1.3.2 Interdisciplinaire aanpak

Voor de ontwikkeling van de standaard Logboek Dataverwerkingen was het essentieel dat de verschillende aspecten (juridische beleidskaders, techniek, inhoud en beheer) goed op elkaar werden afgestemd. Daartoe werkte het project met een interdisciplinair team: juristen, beleidsmakers en adviseurs van BZK werkten nauw samen met technische experts van Digilab en medewerkers van Logius, de beoogde beheerder. Deze interdisciplinaire aanpak zorgde ervoor dat de standaard aansluit op juridische randvoorwaarden, eenvoudig te beheren en te implementeren is, én effectief functioneert in de praktijk. Dit laatste aspect werd getest in Digilab, waar de standaard in verschillende simulatieomgevingen (Fieldlabs) werd ingebouwd en beproefd op praktische toepasbaarheid.

§ 1.3.3 Beheer en doorontwikkeling

Om de overgang tussen ontwikkeling en beheer soepel te laten verlopen, was Logius vanaf een vroeg stadium betrokken bij het project. De inzet van Logius is in de loop van de tijd uitgebreid, zodat in 2025 het beheer van de standaard volledig kan worden overgedragen. Dit beheer wordt ingericht volgens de BOMOS-methodologie (Beheer- en OntwikkelModel voor Open Standaarden). Het opzetten van een goede governance-structuur is een integraal onderdeel van het beheer. Hierbij zullen, naast de gebruikers van de standaard, belangrijke rollen zijn weggelegd voor MIDO (Meerjarenprogramma Infrastructuur Digitale Overheid) en het Forum Standaardisatie. Deze gremia zullen naar verwachting respectievelijk de standaard vaststellen en deze opnemen op de Pas-Toe-Of-Leg-Uit-lijst. Het Ministerie van Binnenlandse Zaken blijft opdrachtgever voor het beheer van de standaard.

§ 2. FAQ

Dit hoofdstuk bevat veelgestelde vragen over de standaard Logboek Dataverwerking en in dit hoofdstuk worden deze veelgestelde vragen beantwoord en toegelicht.

§ 2.1 Vragen

§ 2.1.1 Wat is het doel van de standaard Logboek Dataverwerking?

De overheid moet zich verantwoorden over haar handelen. Daar valt ook onder het verantwoorden van het gebruik van data. Met het gebruik van de standaard Logboek Dataverwerking is een organisatie in staat de logging van de verwerking van data gestandaardiseerd uit te voeren. Dit geldt zowel voor verwerkingen binnen de eigen organisatie als voor verwerkingen die tussen organisaties plaatsvinden.

§ 2.1.2 Wie kan de standaard Logboek Dataverwerking gebruiken?

Elke organisatie die gegevens verwerkt kan de standaard Logboek Dataverwerking inzetten bij processen waar logging en monitoring, bijvoorbeeld vanuit de wetgeving wenselijk is.

§ 2.1.3 Is de standaard Logboek Dataverwerking alleen bedoeld voor de verwerking van persoonsgegevens?

Nee, de standaard kan ook worden gebruikt voor verwerking van andere typen gegevens, zoals bijvoorbeeld de registratie van (geografische) objecten.

§ 2.1.4 Is in de standaard Logboek Dataverwerking opgenomen hoe logging plaatsvinden ten aanzien van beveiligingsincidenten (denk ook aan technische systeemactiviteiten en toegangsbeheer)?

Nee, deze materie is buiten scope van de standaard Logboek Dataverwerkingen.

§ 2.1.5 Wie is eigenaar en beheerder van de standaard Logboek Dataverwerking?

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor deze standaard en de doorontwikkeling ervan. Het beheer wordt door Logius uitgevoerd.

§ 2.1.6 Is mijn organisatie verplicht de standaard Logboek Dataverwerking te implementeren?

Er zijn momenteel geen verplichtingen voor gebruik van de standaard. Indien de standaard ooit verplicht wordt zal dit worden gepubliceerd bij het Forum Standaardisatie op de Pas-toe-of-leg-uit-lijst. Hiervoor dient eerst de gehele procedure te worden doorlopen.

§ 2.1.7 Wat is de relatie van Audit Log met de standaard Logboek Dataverwerking?

In de standaard Logboek Dataverwerking wordt geen identificerende data opgeslagen over gebruiker van het systeem (bijv. de ambtenaar die het systeem gebruikt). We gaan ervan uit dat daar in de organisatie een Audit log voor is ingericht,

aangezien dat verplicht is vanuit BIO. Vanuit Audit Log kan wel een relatie gelegd worden met een verwerking in de standaard Logboek Dataverwerking door te verwijzen naar de Operation ID die de verwerking identificeert.

Voor redenering hierachter, zie [besluit 4.4](#)

Daarnaast is het van belang om te beseffen dat het vastleggen van data over een gebruiker in de Audit Log, ook een dataverwerking is. Immers, de data van de gebruiker (bijv. de ambtenaar die het systeem heeft gebruikt) worden daarbij opgeslagen (verwerkt). Dat is dus een eigen, aparte, dataverwerking die gelogd dient te worden in de Logboek Dataverwerkingen van de verwerker.

§ 2.1.8 Zijn er dingen die je moet aanpassen aan je Audit Log als je de standaard Logboek Dataverwerking implementeert?

In de logging worden geen identificerende gegevens opgeslagen over gebruiker van het systeem (bijv. de ambtenaar die het systeem gebruikt). Om de link tussen een gebruiker en de standaard Logboek Dataverwerking te maken, kan de Audit Log worden aangepast door te verwijzen naar de Operation ID die de dataverwerking identificeert die door de gebruiker is uitgevoerd.

§ 2.1.9 Kan je de standaard Logboek Dataverwerking implementeren als je een cloud (SaaS) applicatie gebruikt?

Ja dat kan. Het is wel van belang een duidelijk onderscheid te maken tussen verantwoordelijke en een verwerker van de gegevens. Dit bepaalt bijvoorbeeld de Register van verwerkingsactiviteiten waarnaar u dient te verwijzen bij implementatie van de standaard Logboek Dataverwerking.

Voor meer informatie over de rol van een verantwoordelijke en een verwerker kunt u de website van [Autoriteit Persoonsgegevens](#) raadplegen.

§ 2.1.10 Is de performance van de standaard Logboek Dataverwerking getest? / Zal de standaard Logboek Dataverwerking de performance van mijn applicaties beperken?

Ja, de performance is getest met een aantal demo-applicaties. De testen toonden aan dat er weinig tot geen performanceverlies was op geraakte applicaties.

§ 2.1.11 Hoe werken het Register van verwerkingsactiviteiten (RvvA) en het Logboek Dataverwerkingen samen?

In het Register van verwerkingsactiviteiten (art 30 AVG) zijn de binnen de organisatie uit te voeren taken en processen waarin verwerkingen worden uitgevoerd benoemd. In de **Logboek Dataverwerkingen standaard** wordt de relatie gelegd tussen de beschreven processen in het register en de daadwerkelijk uitgevoerde activiteit waarbij **data** zijn verwerkt. **Door deze relatie ontstaat** inzicht in de taak en activiteit waarvoor de **data** verwerkt zijn.

§ 2.1.12 Moet ik mijn RvvA aanpassen als ik deze standaard Logboek Dataverwerking implementeer?

Voor de implementatie van deze standaard is het noodzakelijk dat iedere verwerkingsactiviteit in uw RvvA uniek te identificeren is. Mocht dat nog niet het geval zijn, voeg dan een unieke identifier toe aan alle dataverwerkingen.

Het is aanbevolen – maar niet verplicht – om de RvvA benaderbaar te maken met een API. Dat voorkomt dat de identificatoren van de verwerkingsactiviteiten “hardcoded” moeten worden toegevoegd aan de logging en dat bij inzage, handmatig data uit de RvvA moeten worden toegevoegd in de logging.

Het is van belang dat, als de RvvA wordt aangepast, de wijzigingen toegevoegd worden als nieuwe verwerkingsactiviteiten met een eigen unieke identifier. Bestaande verwerkingsactiviteiten mogen niet wijzigen of verwijderd worden. Hierdoor blijven de oude verwijzingen uit de Logboek Dataverwerking intact.

2.1.13 Mijn organisatie heeft geen RvvA API. (Hoe) Kan ik dan nog steeds de standaard Logboek Dataverwerking implementeren?

Ja, dat kan nog steeds. Het is niet verplicht een RvvA API te implementeren, de RvvA is uiteraard wel verplicht in het geval van persoonsgegevensverwerking. Voor de implementatie van de Logboek Dataverwerkingen is het van belang dat iedere verwerkingsactiviteit te identificeren is met een unieke identificator.

Stel de RvvA is uitgewerkt in een MS-Exceldocument en het systeem heeft daar geen API-toegang toe. Daarnaast zijn de dataverwerkingen in de RvvA niet uniek te identificeren met een identificator.

In dat geval zal er een kolom moeten worden toegevoegd aan het MS-Exceldocument waar iedere dataverwerking een unieke identificator krijgt. Deze identificatoren van de dataverwerkingen in uw RvvA zullen dan 'hardcoded' moeten worden toegevoegd in de logging. Bij inzage zullen de data uit de RvvA, die horen bij een dataverwerking, handmatig moeten worden opgezocht.

§ 2.1.14 Hoe gedetailleerd moet mijn RvvA zijn om de standaard Logboek Dataverwerking te implementeren? / Heeft de detailniveau van mijn RvvA invloed op de werking van deze standaard?

De standaard Logboek Dataverwerking gaat er alleen vanuit dat er een RvvA is. Hoe gedetailleerd de RvvA is, is een beslissing van de organisatie zelf. Uiteraard is het wel zo dat hoe gedetailleerder de RvvA is opgezet, hoe transparanter er kan worden gerapporteerd naar burger en (overige) overheid.

§ 2.1.15 Wat gebeurt er als ik mijn RvvA wil wijzigen na de implementatie van de Logboek Dataverwerkingenstandaard?

Het is van belang dat als de RvvA aangepast moet worden, de wijzigingen toegevoegd worden als nieuwe verwerkingsactiviteit met een eigen unieke identificator. Bestaande verwerkingsactiviteiten mogen niet worden aangepast of verwijderd.

Hierdoor blijven de oude verwijzingen uit de Logboek Dataverwerking intact.

§ 3. Architectuur

§ 3.1 Inleiding Architectuur

- @@@@ todo architectuur uitwerken
- @@@@ plaatjes opnemen en beschrijven

§ 3.2 De relatie tussen logboekelementen, waarom eigenlijk?

Logging van gegevensverwerkingen kunnen vaak en veelvuldig plaatsvinden. Het geheel kan groot en complex worden want sommige Logregels zijn aan elkaar gerelateerd. Deze relaties kunnen gelegd worden met Logregels met andere applicaties binnen dezelfde organisatie of met logregels van applicaties van andere organisaties. Maar ook zijn er relaties nodig met activiteiten in het Register van Verwerkingsactiviteiten. Wat nu als alle Logregels zonder relaties worden opgeslagen? Bij een rapportage (bijvoorbeeld een verzoek tot inzage van een burger) moet nu handmatig worden uitgezocht welke gegevensverwerkingen bij elkaar horen en er moet, in het ernstigste geval, ook contact worden gezocht met andere organisaties om te onderzoeken of daar ook de nodige gegevensverwerkingen zijn uitgevoerd. Als er bij elke Logregel de nodige relatiegegevens worden bijgevoegd, kan de rapportage snel en accuraat worden gegenereerd.

§ 3.2.1 Welke relatiegegevens moeten er dan worden opgeslagen per Logregel?

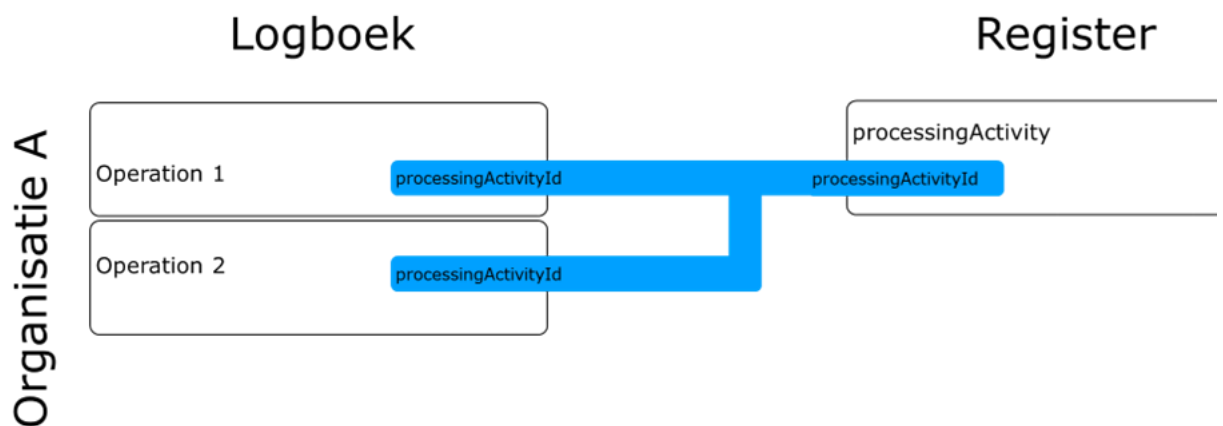
Om er zeker van te zijn dat de relatie tussen Logregels gelegd kan worden, moeten de volgende gegevens worden geregistreerd per Logregel:

- **processingActivityId:** elke gegevensverwerking die een organisatie doet, moet bekend zijn in het Register van Verwerkingsactiviteiten. Het processingActivity legt de relatie tussen de gegevensverwerking door een applicatie, en de activiteit gedefinieerd in het Register.
- **traceId:** alle logregels die voor een specifieke gegevensverwerking bij elkaar horen, krijgen een traceId. De traceId-waarde voor alle Logregels die bij elkaar horen is hetzelfde.
- **operationId:** elke individuele Logregel (Operation) krijgt een eigen, unieke operationId (net zoals elk databaserecord dat ook krijgt).

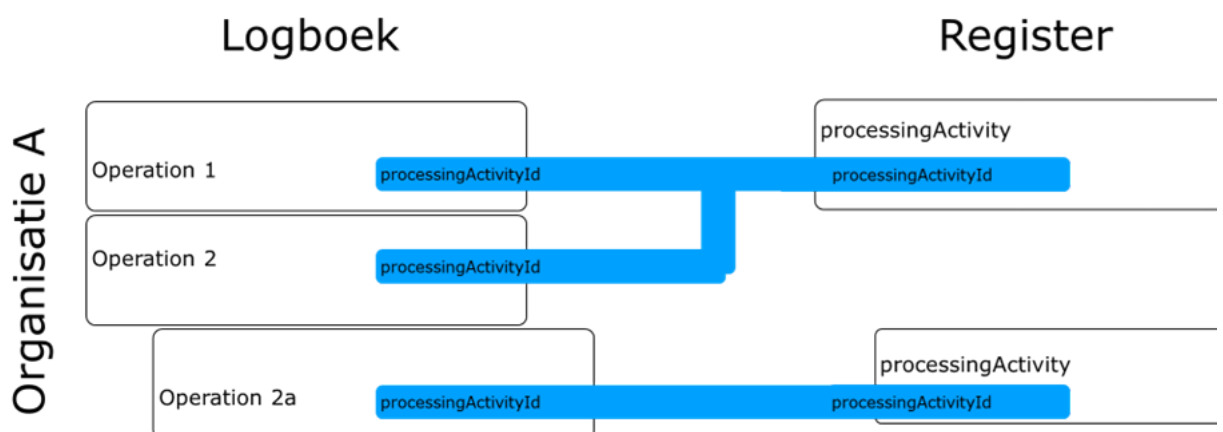
In werkelijkheid worden alle relaties door de Applicatie in een fractie van een seconde (in parallel) gelegd. Om het grote geheel beter te begrijpen, worden alle relaties hieronder stap voor stap uitgelegd.

§ 3.2.2 Het logboek en het Register van Verwerkingsactiviteiten

Als er een Dataverwerking plaatsvindt, moet dit altijd een relatie hebben met het Register van Verwerkingsactiviteiten. In dit Register staat informatie over de gegevens die een organisatie verwerkt. Het Register is verplicht, een geautomatiseerde koppeling met het Logboek niet. Bij elke Dataverwerking wordt door het Logboek een relatie gelegd met het Register door middel van het processingActivityId. Als er meerdere dezelfde Dataverwerkingen ('Operations') zijn, krijgen deze dus allemaal dezelfde processingActivityId.

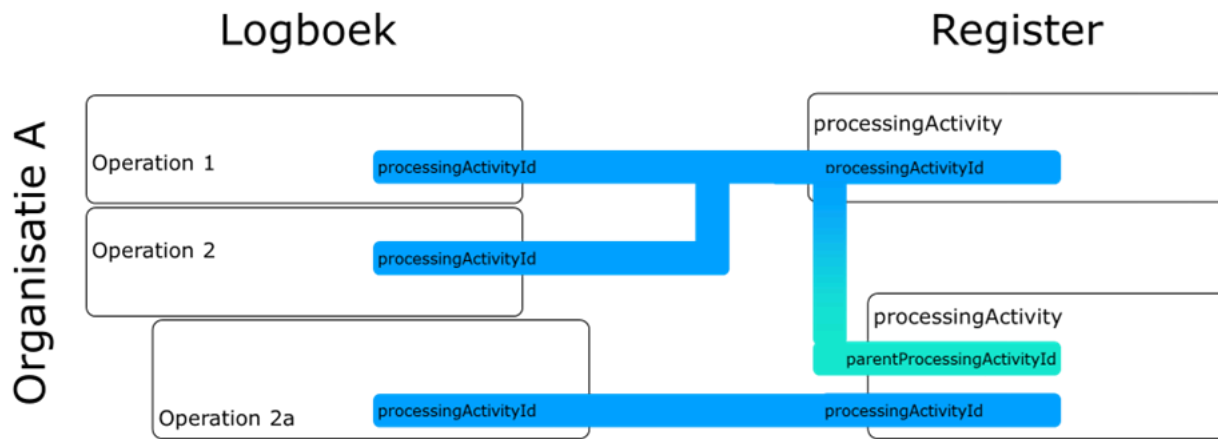


In het geval er een Dataverwerking plaatsvindt ter ondersteuning van een andere Dataverwerking (suboperation), dan kan deze ondersteunende Dataverwerking een eigen processingActivityId krijgen. Deze kan anders zijn dan het processingActivityId van de 'hoofdprocessingActivity'.

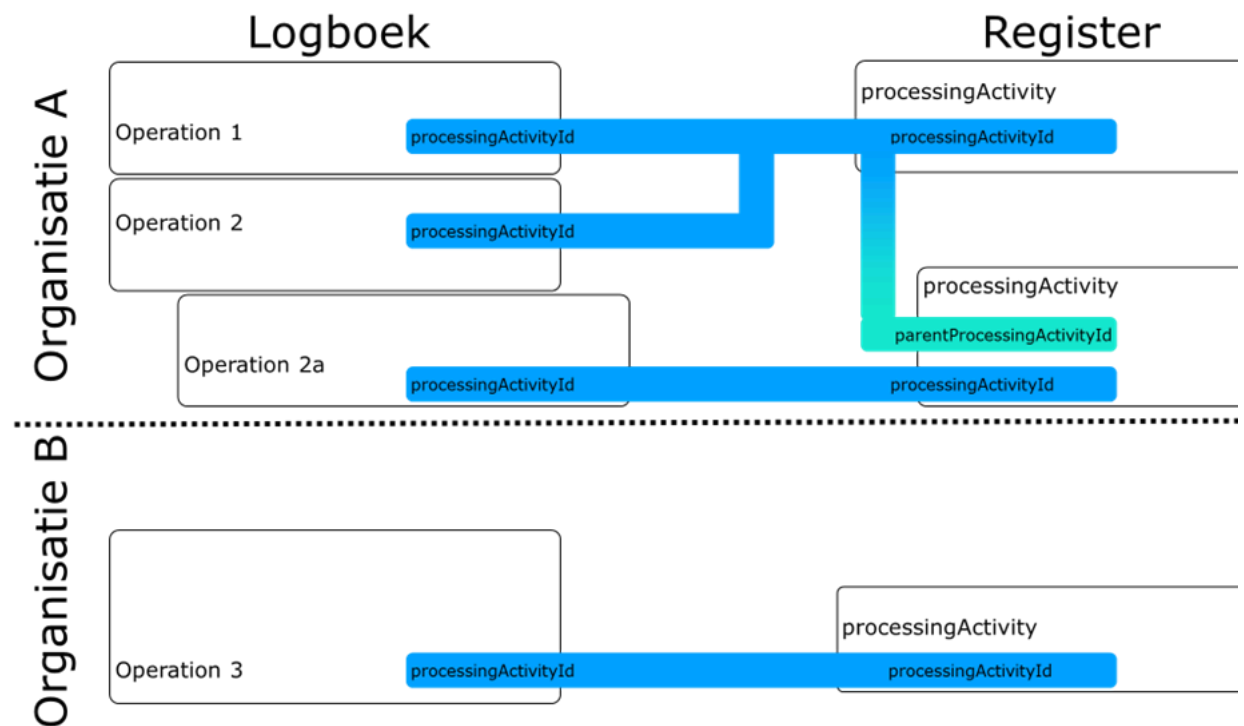


De subOperation heeft nu een eigen processingActivityId gekregen, maar het is nog niet duidelijk aan welke hoofdprocessingActivityId deze gekoppeld is. Om dit op te lossen, wordt ook een 'parentProcessingActivityId' geregistreerd. Bij de subOperation wordt in dit geval naast de processingActivityId ook een parentProcessingActivityId

geregistreerd. De waarde van deze parentProcessingActivityId is gelijk aan de waarde van het hoofdProcessingActivityId.



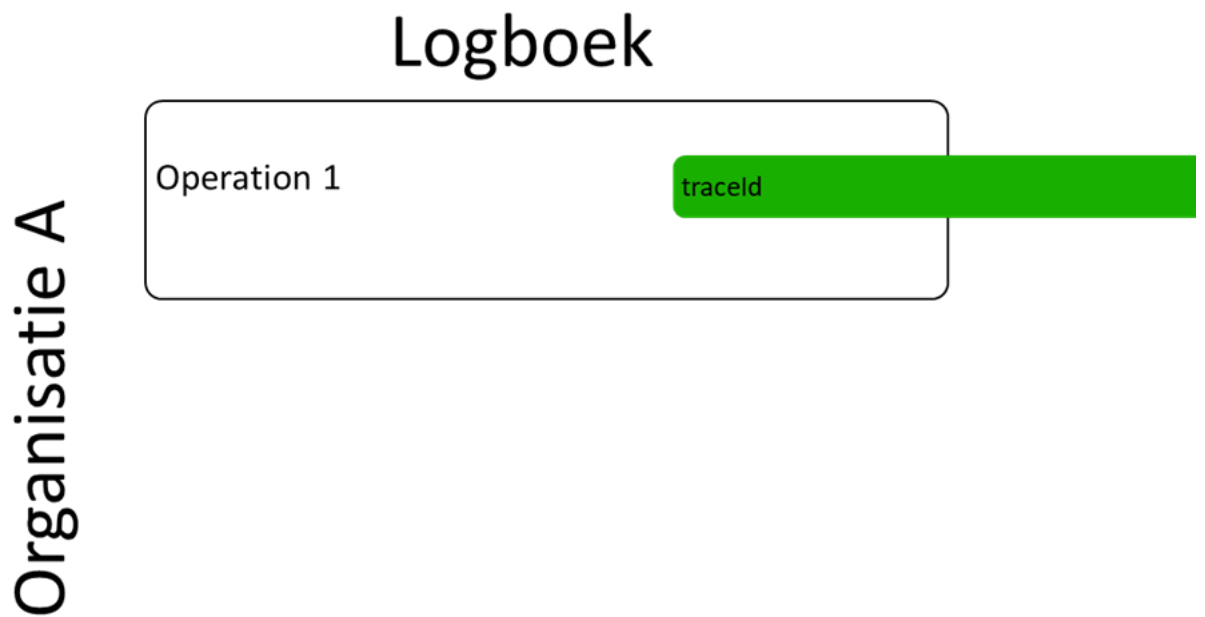
Bij een Dataverwerking kan het zijn dat gegevens moeten worden opgevraagd bij een andere organisatie. Deze organisatie heeft zelf ook een Register van Verwerkingsactiviteiten. In dit Register staat beschreven dat een specifieke organisatie specifieke gegevens mag opvragen als aparte operation. Bij het verstrekken van deze gegevens aan de aanvragende organisatie, wordt het processingActivityId van de gegevensverstrekende organisatie geregistreerd. Er is dus GEEN rechtstreekse koppeling tussen het Register van de aanvragende en het Register van de verstrekende organisatie.



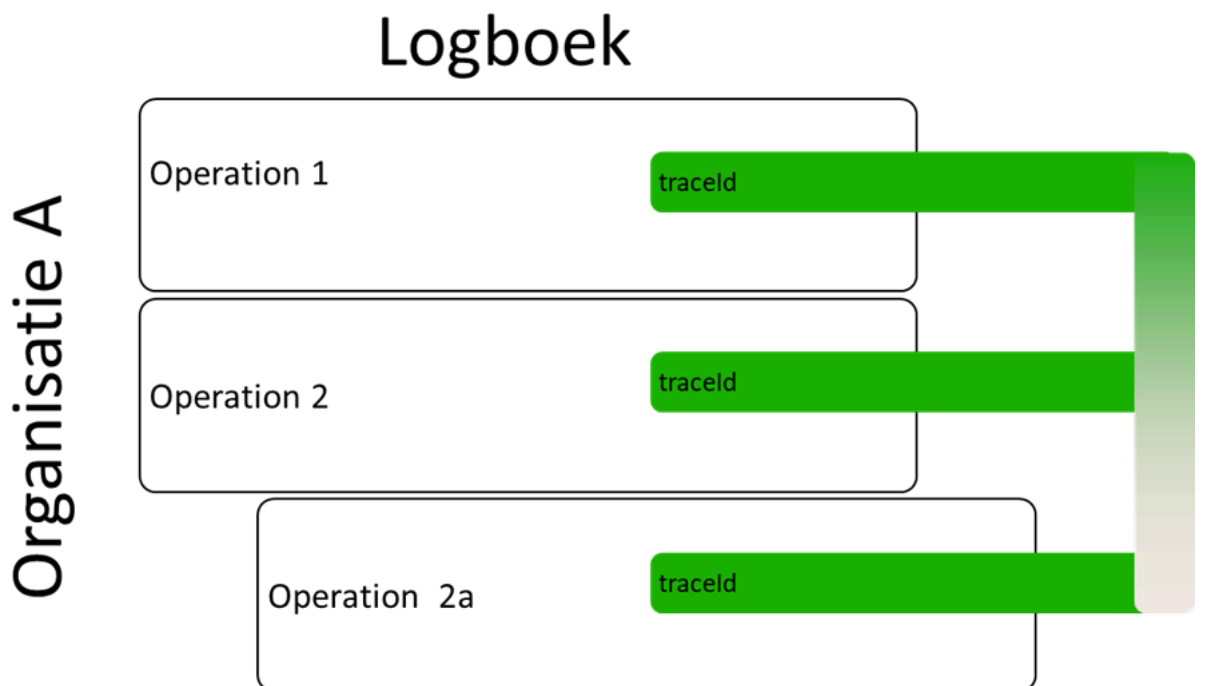
§ 3.2.3 TraceId als grootste gemene deler

Operations kunnen bestaan uit meerdere (sub)Operations binnen de eigen organisatie maar ook over organisaties heen. Het geheel kan een grote en ingewikkelde constructie worden. Om toch het overzicht te kunnen behouden, is het noodzakelijk een 'traceId' te introduceren per (sub)Operation. Het traceId is als het ware de 'lijm' tussen alle (sub)Operations. Als er nog

geen traceId bekend is, wordt deze automatisch gegenereerd voor de eerste Operation.

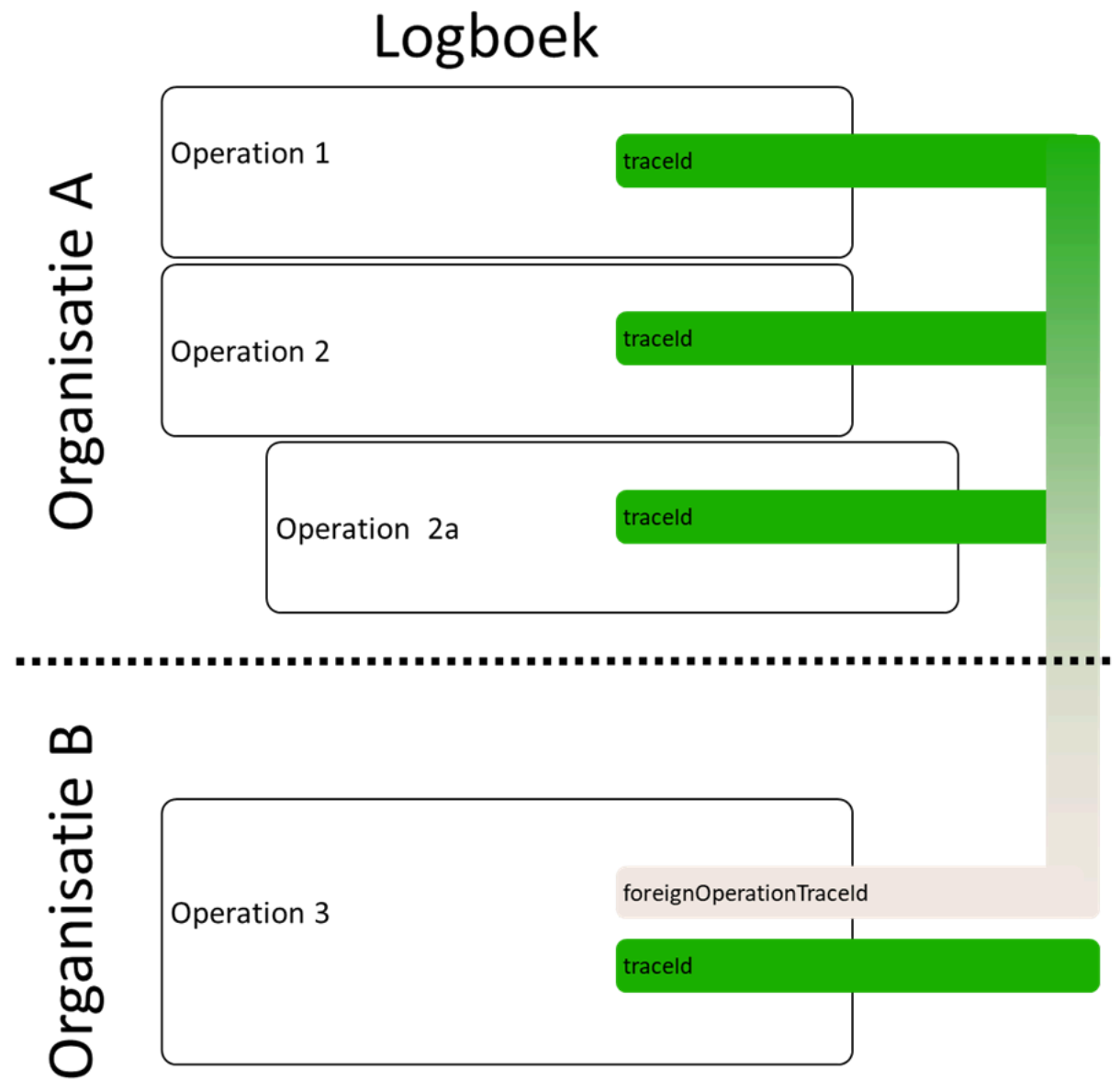


Alle bij elkaar horende (sub)Operations, krijgen vervolgens dezelfde traceId-waarde.



In het geval er gegevens worden opgevraagd aan een andere organisatie, krijgt elke operation bij verstreckende organisatie een traceId. Om de relatie te leggen tussen de vragende en de verstreckende organisatie, wordt bij elke Operation van de verstreckende organisatie een 'foreignOperationTraceId' geregistreerd. De waarde van de foreignOperationTraceId van de

verstreckende organisatie is gelijk aan de waarde van traceId van de vragende organisatie.

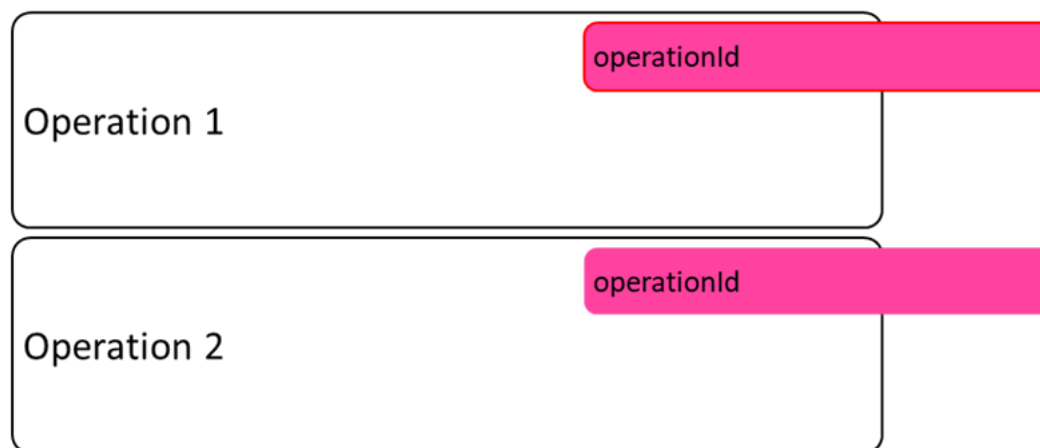


§ 3.2.4 Relatie tussen (sub)Operations

Elke (sub)Operation krijgt een eigen, unieke operationId. Hiermee zijn alle loggings altijd uniek traceerbaar. Ook subOperations krijgen een eigen, unieke OperationId.

Organisatie A

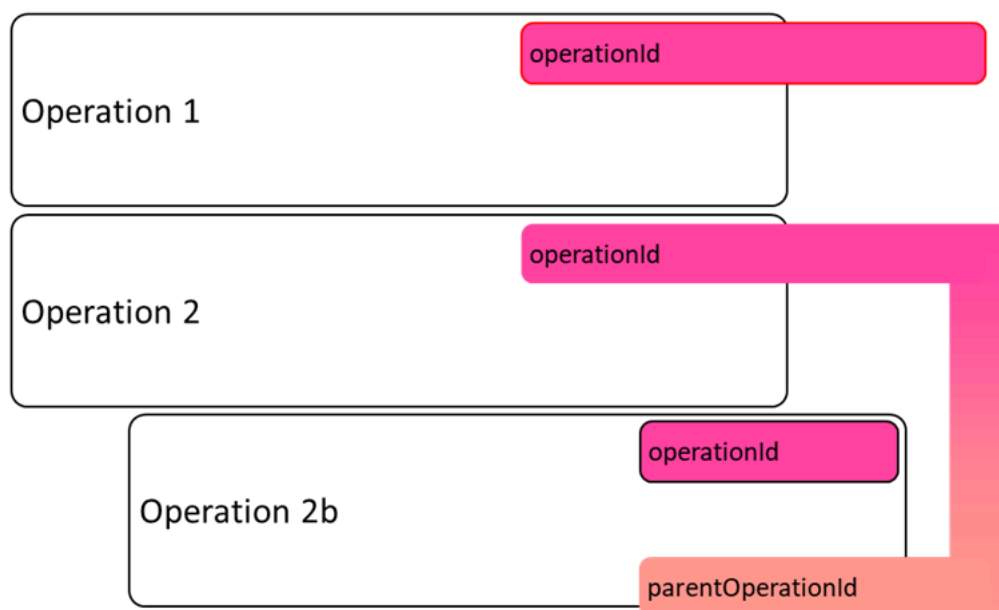
Logboek



Als er ook subOperations plaatsvinden, moet er ook een 'parentOperationId' worden geregistreerd om de koppeling met de hoofdOperation te realiseren.

Organisatie A

Logboek



In het geval er gegevens nodig zijn van een andere organisatie, krijgt de Operation van de verstreckende organisatie ook een eigen, unieke operationId. Daarnaast wordt bij deze Operation ook het operationId geregistreerd die het verzoek voor informatie geïnitieerd heeft (vanuit de vragende organisatie). Deze specifieke operationId wordt het 'foreignOperationId'

genoemd en krijgt de waarde gelijk aan het operationId van de initiërende Operation van de vragende organisatie.



§ 3.2.5 Voorbeeld van een traceringsconstructie

Het nu volgende voorbeeld is volledig fictief en is puur bedoeld om een beeld te schetsen ten behoeve van een traceringsconstructie in een logboek.

§ 3.2.6 Situatieschets

Een persoon heeft een parkeervergunning in een gemeente. Er is een nieuwe auto aangeschaft, het kenteken moet worden aangepast ten behoeve van de vergunning. De persoon kan het kenteken online wijzigen in de 'mijnGemeente' applicatie. Om het voorbeeld eenvoudig te houden, worden foutsituaties buiten beschouwing gelaten.

§ 3.2.7 Procesgang

1. Persoon logt in gemeenteapplicatie.

2. Gemeente toont huidige parkeervergunning.
3. Persoon wijzigt kenteken in de gemeenteapplicatie.
4. Gemeenteapplicatie vraagt het RDW om gegevens op basis van de tenaamstelling.
5. RDW geeft de gevraagde gegevens terug aan de gemeenteapplicatie.
6. Gemeenteapplicatie accepteert de wijziging van de persoon.

De traceringsgegevens worden als volgt vastgelegd:

processingActivityId

In de gemeenteapplicatie worden de volgende Operations uitgevoerd die een relatie hebben met het Register van Verwerkingsactiviteiten van de gemeente:

- **Toon alle vergunningen:** na het inloggen, worden de parkeervergunningen van de persoon getoond. Deze Operation is gerelateerd aan de processingActivity **Parkeervergunningadministratie voeren**.
- **Wijzig kenteken:** het wijzigen van het kenteken valt ook onder de processingActivity **Parkeervergunningadministratie voeren**. Hierdoor is het processingActivityId hetzelfde als die van de Operation **Toon alle vergunningen**.
- **Controleer tenaamstelling:** deze Operation zorgt voor de aanvraag van gegevens richting het RDW en controle van de terugontvangen gegevens. Deze Operation is een subOperation van **Wijzig kenteken** en krijgt een processingActivity wat hoort bij de processingActivity in het Register genaamd **Tenaamstelling controleren**. De processingActivity is op zijn beurt weer een subprocessingActivity van **Parkeeradministratie voeren**. Om deze relatie te leggen, moet ook een parentProcessingActivityId worden geregistreerd. De waarde hiervan is gelijk aan de waarde van het processingActivityId van **Parkeervergunningadministratie voeren**.

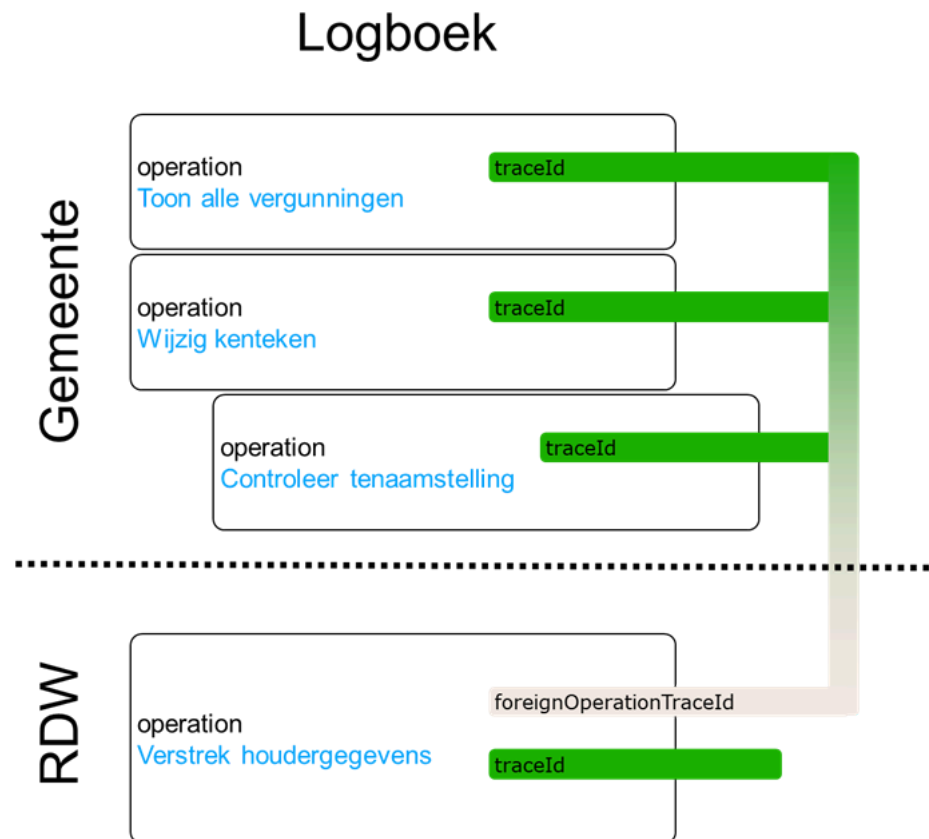
In de RDW-applicatie wordt het verstrekken van gegevens aan de gemeenteapplicatie ook geregistreerd. De Operation **Verstrek houdergegevens** is gerelateerd aan de processingActivity **Kentekenhoudergegevens verstrekken**. Merk op dat er hier dus GEEN directe relatie is tussen het Register van Verwerkingsactiviteiten van de gemeente en die van het RDW.



§ 3.2.8 traceId

- De gemeenteOperations **Toon alle vergunningen**, **Wijzig kenteken** en **Controleer tenaamstelling** behoren tot dezelfde handeling (met als eindresultaat het wijzigingen van het kenteken op de vergunning). Deze Operations krijgen allemaal dezelfde traceId.
- De RDW-Operation **Verstrek houdergegevens** krijgt een eigen traceId.
- Om het geheel te koppelen over de organisaties heen, wordt bij het RDW ook een foreignOperationTraceId opgeslagen, de waarde hier van is gelijk aan de

waarde van de traceId van de Operation **Controleer tenaamstelling**.

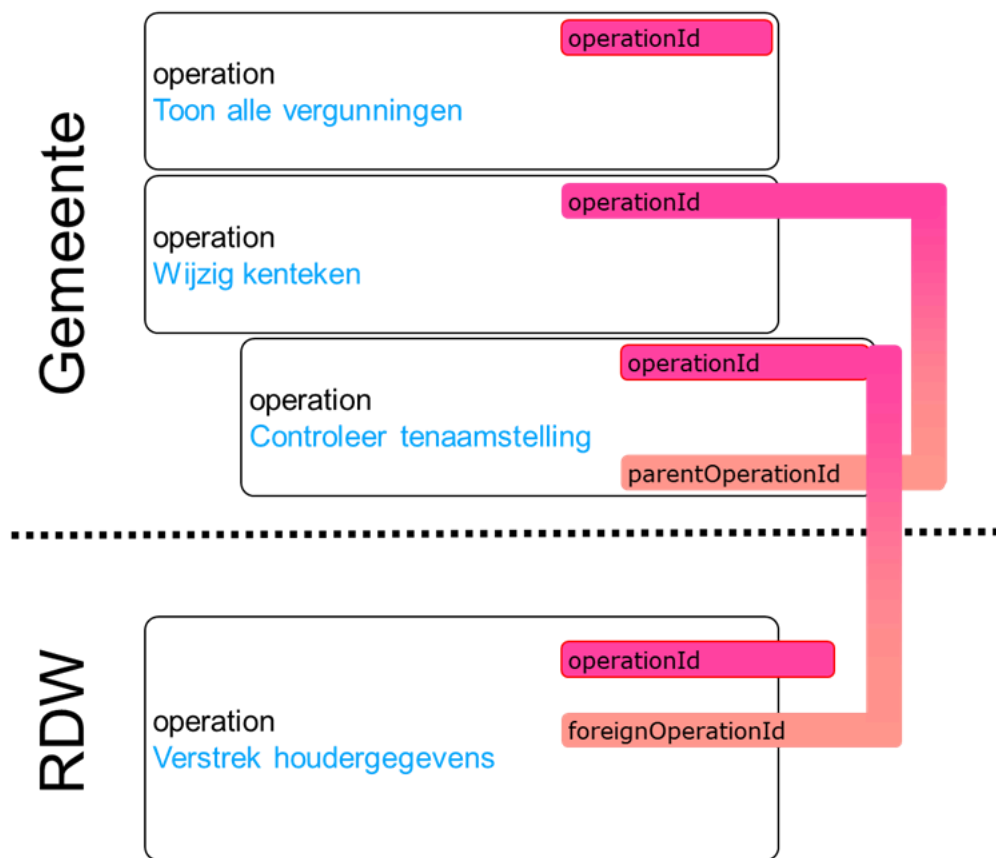


§ 3.2.9 OperationId

In de gemeente-applicatie krijgt elke (sub)Operation een eigen, unieke OperationId. • De (sub)Operation **Controleer tenaamstelling** krijgt daarnaast ook nog een parentOperationId met de waarde van OperationId van de **Operation Wijzig kenteken** om een relatie te leggen. • Ook de RDW-Operation **Verstrek houdergegevens** krijgt een eigen unieke OperationId. • Om de relatie over de organisaties heen te leggen, wordt er bij de RDW-Operation **Verstrek houdergegevens** ook een foreignOperationId moeten worden vastgelegd. De waarde van deze foreignOperationId is gelijk aan de waarde van

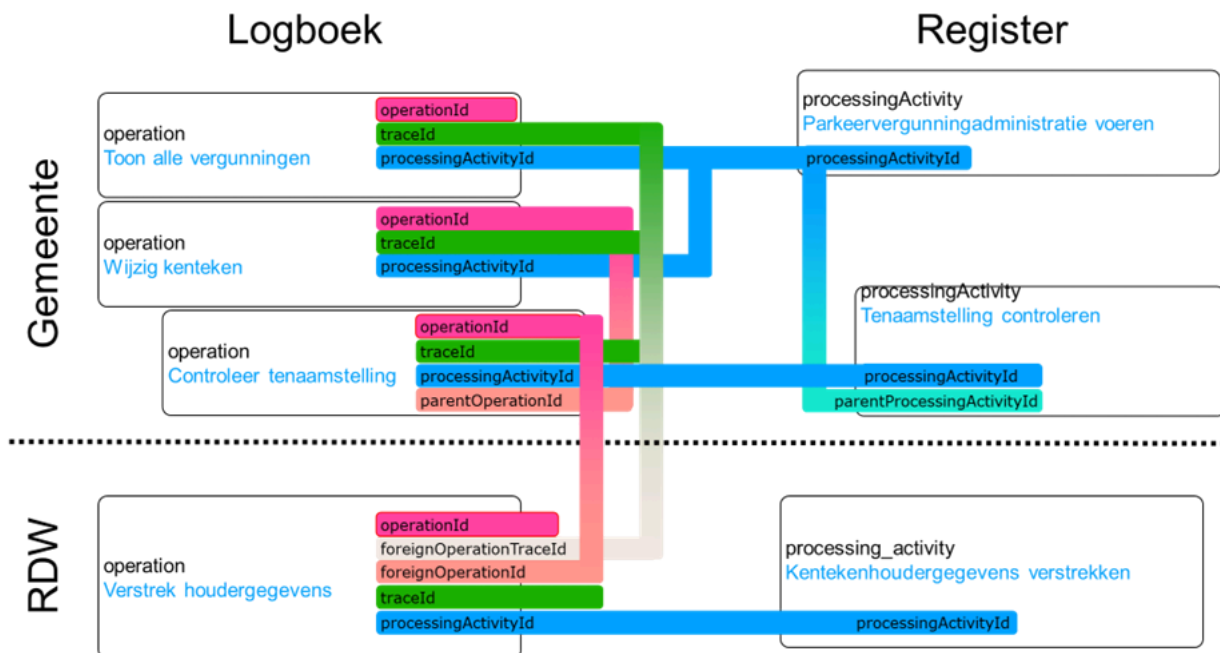
de OperationId van de gemeente-Operation **Controleer tenaamstelling**.

Logboek



§ 3.2.10 Totaalbeeld

Als alle relaties gelegd zijn, ziet de traceringsconstructie er als volgt uit:



Meer gedetailleerde voorbeelden staan beschreven in de [inleiding](#) van de standaard logboek dataverwerkingen.

§ 3.3 Canoniek Gegevensmodel

Ter verduidelijking van de standaard is een Canoniek gegevensmodel uitgewerkt, dit gestandaardiseerd model voor datarepresentatie is ontworpen om de attributen eenduidig en consistent te maken. Het biedt een uniforme structuur en terminologie voor alle relevante gegevens in de standaard. Zie voor de definitie van de gebruikte terminologie ook [Paragraaf 1.2 van de standaard](#).

§ 3.3.1 attribute

Attribuut	Beschrijving
Attribuutnaam	attribute
Definitie Engels	Attributes in the form of key value pairs.
Attribuutnaam Nederlands	attribuut
Definitie Nederlands	Attributen in de vorm van key value pairs.
Toelichting	Organisaties hebben de vrijheid om zelf key value pairs te bepalen als dit bijdraagt aan de inzichtelijkheid van een gegevensverwerkingsactie.
Noodzakelijkheid	Vanuit de standaard is het onmogelijk om alle attribuutsoorten te definiëren die belangrijk zijn voor de inzichtelijkheid van een gegevensverwerkingsactie. Daarom is er in de standaard rekening gehouden met een mogelijkheid om per organisatie of per systeem eigen attribuutsoorten te bepalen.
Datatype	-
Voorbeeld	-
Verplicht	Nee
Gebruikt in	Logboek
Enumeratiewaarden	-

§ 3.3.2 dplCoreDataSubjectId

Attribuut	Beschrijving
Attribuutnaam	dplCoreDataSubjectId
Definitie Engels	Refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.
Attribuutnaam Nederlands	dplCorebetrokkeneId
Definitie Nederlands	De geïdentificeerde of identificeerbare natuurlijk persoon op wie de verwerkte en/of de te verwerken persoonsgegevens betrekking hebben.
Toelichting	Bij het gebruik van dataSubject (betrokkene) moet rekening gehouden met artikel 32-1a: <i>Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: a) de pseudonimisering en versleuteling van persoonsgegevens.</i>
Noodzakelijkheid	Gegevensverwerkingsacties moeten per betrokkene worden opgeslagen. Indien er gevraagd wordt om de gegevensverwerkingsacties van een betrokkene kan er niet gerapporteerd worden zonder dit attribuutsoort.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.3 dataSubjectCategories

Attribuut	Beschrijving
Attribuutnaam	dataSubjectCategories
Definitie Engels	A classification of data subjects relevant to an organization. Can be used to categorize business-specific and regulation-specific categories. Examples: Employees Customers Suppliers
Attribuutnaam Nederlands	categorieënBetrokkenen
Definitie Nederlands	Een beschrijving van de categorieën van personen van wie gegevens verwerkt worden.
Toelichting	-
Noodzakelijkheid	In AVG artikel 30-1c wordt de volgende maatregel benoemd: <i>Elke verantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens: een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens.</i>
Datatype	Enumwaarde
Voorbeeld	Burger
Verplicht	Ja
Gebruikt in	Register
Enumeratiewaarden	Afhankelijk van het type systeem en betrokken actoren. Er kunnen meerdere categorieën van toepassing zijn.

§ 3.3.4 dplCoreProcessingActivityId

Attribuut	Beschrijving
Attribuutnaam	dplCoreProcessingActivityId
Definitie Engels	Reference to Register with more information about the processing activity.
Attribuutnaam Nederlands	dplCoreVerwerkingsactiviteitId
Definitie Nederlands	Verwijzing naar Register met meer informatie over de verwerkingsactiviteit.
Toelichting	-
Noodzakelijkheid	Elke gegevensverwerking in het logboek moet in lijn zijn met de vooraf gedefinieerde verwerkingsactiviteiten in het register (zie AVG artikel 30). Om te voorkomen dat alle attribuutsoorten van het register gedupliceerd worden in het logboek, wordt in het logboek alleen verwezen naar het VerwerkingsactiviteitId van het register.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Ja
Gebruikt in	Register en Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.5 endTime

Attribuut	Beschrijving
Attribuutnaam	endTime
Definitie Engels	Timestamp representing the end of a data processing logging action.
Attribuutnaam Nederlands	eindTijd
Definitie Nederlands	Tijdstempel die het einde van een logboekactie voor gegevensverwerking vertegenwoordigt.

Attribuut	Beschrijving
Toelichting	Een logboekregel wordt pas weggeschreven in het logboek als de volledige transactie (succesvol of niet succesvol) is afgerond.
Noodzakelijkheid	Bij een inzageverzoek van de Betrokkene ten aanzien van gegevensverwerkingsacties, wordt ook een tijdsspanne gevraagd. Alleen de details van een gegevenswerkingsactie binnen opgegeven tijdsspanne worden gerapporteerd. Zonder begin- en eindtijd van een gegevensverwerkingsactie is het onmogelijk de juiste details op te leveren.
Datatype	DateTime
Voorbeeld	2025-02-23T00:00:00
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing.

§ 3.3.6 envisagedTimeLimit

Attribuut	Beschrijving
Attribuutnaam	envisagedTimeLimit
Definitie Engels	The maximum period for which the personal data is necessary to achieve the purpose of the processing or no longer than the period anchored in sector-specific legislation.
Attribuutnaam Nederlands	bewaarTermijn
Definitie Nederlands	De maximale periode waarin de persoonsgegevens noodzakelijk worden bewaard om het doel van de verwerking te bereiken of niet langer dan de termijn die verankerd is in sectorspecifieke wetgeving.
Toelichting	Als het bewaartermijn van een bewaard gegeven verstreken is, dan moet het gegeven worden verwijderd uit het logboek.
Noodzakelijkheid	In AVG artikel 30-1f wordt de volgende maatregel benoemd: <i>Elke verantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens: indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist.</i> De concrete datum waarop een gegevensverwerking moet worden gewist uit het logboek, kan bepaald worden door middel van het bewaartermijn in het register en de eindtijd waarop een gegevensverwerking is gelogd in het logboek. Daardoor is het onnodig om de concrete verwijderdatum van een gegevensverwerking te registreren in het logboek.
Datatype	DateTime
Voorbeeld	2025-02-23T00:00:00
Verplicht	Ja
Gebruikt in	Register
Enumeratiewaarden	Niet van toepassing

§ 3.3.7 foreignOperation.entity

Attribuut	Beschrijving
Attribuutnaam	foreignOperation.entity
Definitie Engels	Reference to external entity.
Attribuutnaam Nederlands	entiteit
Definitie Nederlands	Verwijzing naar externe entiteit.
Toelichting	Indien er voor een verwerking ook een logging heeft plaatsgevonden door een externe informatiebron, dan wordt er een verwijzing aangemaakt om de gegevens van deze logging in te kunnen zien.

Attribuut	Beschrijving
Noodzakelijkheid	Indien het noodzakelijk is ook gegevensverwerkingsacties van een externe gegevensbron te gebruiken, dan wordt een unieke referentie naar deze externe gegevensverwerkingsactie geregistreerd in het logboek. Door alleen te verwijzen naar de externe gegevensverwerkingsactie, kan voorkomen worden dat gegevens gedupliceerd worden opgeslagen in het logboek.
Datatype	URI
Voorbeeld	foo://techtargat.com:8042/over/there?name=parrot#beak
Verplicht	Nee
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.8 foreignOperation.operationId

Attribuut	Beschrijving
Attribuutnaam	foreignOperation.operationId
Definitie Engels	Unique name given to a foreign processing operation.
Attribuutnaam Nederlands	externeActie.actieId
Definitie Nederlands	Identificator die de externe verwerkingsactie uniek identificeert.
Toelichting	Externe verwerkingsacties kunnen een onderdeel zijn van de totale verwerkingsactie. OperationId is in dit geval een attribuutsoort van het objecttype foreignOperation.
Noodzakelijkheid	Indien het noodzakelijk is ook gegevensverwerkingsacties van een externe gegevensbron te gebruiken, dan wordt een unieke referentie naar deze externe gegevensverwerkingsactie geregistreerd in het logboek. Het foreignOperation.operationId refereert naar één specifieke gegevensverwerkingsactie door de externe gegevensbron. Door alleen te verwijzen naar de externe gegevensverwerkingsactie, kan voorkomen worden dat gegevens gedupliceerd worden opgeslagen in het logboek.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Nee
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.9 LegalBasis

Attribuut	Beschrijving
Attribuutnaam	LegalBasis
Definitie Engels	The general conditions governing the lawfulness of processing by the controller.
Attribuutnaam Nederlands	grondslag
Definitie Nederlands	Algemene voorwaarden inzake de rechtmatigheid van verwerking door de verantwoordelijke.
Toelichting	De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de voorwaarden is voldaan.
Noodzakelijkheid	In AVG artikel 6-1 worden de volgende maatregelen benoemd: <i>De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de voorwaarden is voldaan.</i> <i>a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;</i> <i>b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;</i>

Attribuut	Beschrijving
	<i>c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verantwoordelijke rust;</i>
	<i>d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;</i>
	<i>e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verantwoordelijke is opgedragen;</i>
	<i>f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.</i>
	Er moet worden aangetoond dat de verwerking rechtmatig is op basis van één of meer grondslagen.
Datatype	Enumwaarden
Voorbeeld	Legal obligation
Verplicht	Ja
Gebruikt in	Register
Enumeratiewaarden EN	- Consent data subject (6-1a)
	- Necessary contract data subject (6-1b)
	- Legal obligation (6-1c)
	- Protect vital interests (6-1d)
	- Performance task (6-1e)
	- Legitimate interests (6-1f)
Enumeratiewaarden NL	- Toestemming betrokkene (6-1a)
	- Uitvoering overeenkomst betrokkene (6-1b)
	- Wettelijke verplichting (6-1c)
	- Vitaal belang (6-1d)
	- Algemeen belang (6-1e)
	- Gerechtvaardigd belang (6-1f)

§ 3.3.10 LegalBasisComment

Attribuut	Beschrijving
Attribuutnaam	LegalBasisComment
Definitie Engels	More detailed explanation of the general conditions governing the lawfulness of processing by the controller.
Attribuutnaam Nederlands	grondslagUitleg
Definitie Nederlands	Uitleg bij de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verantwoordelijke.
Toelichting	-
Noodzakelijkheid	Organisaties mogen persoonsgegevens alleen verzamelen met een gerechtvaardigd doel. Dat doel moet specifiek zijn en vooraf uitdrukkelijk zijn omschreven. Artikel 5-1 van de AVG benoemt (onder andere) de volgende maatregelen: <i>Persoonsgegevens moeten:</i>
	<i>a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is ("rechtmatigheid, behoorlijkheid en transparantie");</i>
	<i>b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang,</i>

Attribuut	Beschrijving
	<i>wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding");</i>
	<i>c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking").</i>
Datatype	CharacterString
Voorbeeld	Paspoortenregeling Nederland
Verplicht	Nee
Gebruikt in	Register
Enumeratiewaarden	Niet van toepassing

§ 3.3.11 operationId

Attribuut	Beschrijving
Attribuutnaam	operationId
Definitie Engels	Unique name given to a processing operation.
Attribuutnaam Nederlands	actieId
Definitie Nederlands	Identificator die de gegevensverwerkingsactie uniek identificeert.
Toelichting	Het iD is betekenisloos, kent geen volgorde en is uniek over alle systemen in de wereld.
Noodzakelijkheid	Elke gegevensverwerkingsactie wordt uniek opgeslagen in het logboek. Indien een rapportage moet worden gemaakt voor de betrokkene, moet de unieke gegevensverwerkingsactie opgehaald kunnen worden uit het logboek. Het ophalen van de gegevens gaat op basis van het operationId, dus zonder dit gegeven is het aanmaken van een rapportage niet mogelijk.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.12 operationName

Attribuut	Beschrijving
Attribuutnaam	operationName
Definitie Engels	Specific operation addressed or referred to.
Attribuutnaam Nederlands	actieNaam
Definitie Nederlands	Naam van een specifieke gegevensverwerkingsactie.
Toelichting	Aanbevolen wordt om alle gegevensverwerkingsacties te beschrijven als een werkwoord (in de infinitief) gevolgd door een zelfstandig naamwoord.
Noodzakelijkheid	Om duidelijk te maken aan de betrokkene (bij een verzoek om gegevensinzage) wat er concreet is gebeurd bij een gegevensverwerkingsactie, wordt een operationName gedefinieerd. Zie ook artikel 4 van de AVG, waarin de definitie van 'verwerking' wordt genoemd: <i>een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.</i>
Datatype	CharacterString
Voorbeeld	Opslaan persoonsgegevens
Verplicht	Ja

Attribuut	Beschrijving
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.13 parentDplCoreProcessingActivityId

Attribuut	Beschrijving
Attribuutnaam	parentDplCoreProcessingActivityId
Definitie Engels	A parent is one class, and a child is another class that inherits all of the attributes and functions assigned to the parent class. The parentId refers to the parent class.
Attribuutnaam Nederlands	parentDplCoreVerwerkingsactiviteitId
Definitie Nederlands	Een parent is één klasse, en een child is een andere klasse die alle attributen en functies overerft die aan de bovenliggende klasse zijn toegewezen. De parentId verwijst naar de bovenliggende klasse.
Toelichting	Een verwerkingsactiviteit kan onderdeel zijn een andere verwerkingsactiviteit. Op deze manier ontstaat er een hiërarchie van verwerkingsactiviteiten.
Noodzakelijkheid	Een bepaalde verwerkingsactiviteit kan een onderdeel zijn van een andere verwerkingsactiviteit. Door gebruik te maken van een 'parent/child'-structuur, hoeven er geen nieuwe attributen gedefinieerd te worden om een hiërarchie van verwerkingsactiviteiten te creëren.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Ja
Gebruikt in	Register en Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.14 parentOperationId

Attribuut	Beschrijving
Attribuutnaam	parentOperationId
Definitie Engels	A parent is one class, and a child is another class that inherits all of the attributes and functions assigned to the parent class. The parentId refers to the parent class.
Attribuutnaam Nederlands	parentActieId
Definitie Nederlands	Een parent is één klasse, en een child is een andere klasse die alle attributen en functies overerft die aan de bovenliggende klasse zijn toegewezen. De parentId verwijst naar de bovenliggende klasse.
Toelichting	Een gegevensverwerkingsactie kan onderdeel zijn een andere verwerkingsactie. Op deze manier ontstaat er een hiërarchie van gegevensverwerkingsacties.
Noodzakelijkheid	Een bepaalde verwerkingsactie kan een onderdeel zijn van een andere verwerkingsactie. Door gebruik te maken van een 'parent/child'-structuur, hoeven er geen nieuwe attributen gedefinieerd te worden om een hiërarchie van gegevensverwerkingsacties te creëren.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.15 personalDataCategories

Attribuut	Beschrijving
Attribuutnaam	personalDataCategories
Definitie Engels	Category of information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Attribuutnaam Nederlands	categorieënPersoonsgegevens
Definitie Nederlands	Categorieën van Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare levende natuurlijke persoon. Losse gegevens die samengevoegd kunnen leiden tot de identificatie van een bepaalde persoon vormen ook persoonsgegevens.
Toelichting	Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.
Noodzakelijkheid	In AVG artikel 30-1c wordt de volgende maatregel benoemd: <i>Elke verantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens: een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens.</i>
Datatype	Enumwaarde
Voorbeeld	Nummer van identiteitskaart
Verplicht	Ja
Gebruikt in	Register
Enumeratiewaarden	Afhankelijk van het type systeem en betrokken actoren. Er kunnen meerdere categorieën van toepassing zijn.

§ 3.3.16 purpose

Attribuut	Beschrijving
Attribuutnaam	purpose
Definitie Engels	Personal data may only be processed for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with those purposes.
Attribuutnaam Nederlands	doelEinde
Definitie Nederlands	Persoonsgegevens mogen slechts worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.
Toelichting	Persoonsgegevens mogen alleen verwerken als je vóóraf de specifieke doeleinden voor de verwerking bepaald zijn.
Noodzakelijkheid	In AVG artikel 5-1b wordt de volgende maatregel benoemd: <i>Persoonsgegevens moeten: voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding”).</i>
Datatype	CharacterString
Voorbeeld	Het aanvragen, afgeven en innemen van reisdocumenten en het verwerken van kennisgevingen van het in het buitenland afgegeven reisdocumenten.

Attribuut	Beschrijving
Verplicht	Ja
Gebruikt in	Register
Enumeratiewaarden	Niet van toepassing

§ 3.3.17 recipientsCategories

Attribuut	Beschrijving
Attribuutnaam	recipientsCategories
Definitie Engels	Categories of natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
Attribuutnaam Nederlands	categorieënOntvangers
Definitie Nederlands	Categorieën van natuurlijke of rechtspersonen, overheidsinstanties, agentschap of andere instanties waaraan de persoonsgegevens worden bekendgemaakt, al dan niet een derde partij.
Toelichting	-
Noodzakelijkheid	In AVG artikel 30-1d wordt de volgende maatregel benoemd: <i>Elke verantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens: de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties.</i>
Datatype	Enumwaarde
Voorbeeld	Aanvragers, rechthebbenden
Verplicht	Ja
Gebruikt in	Register
Enumeratiewaarden	Afhankelijk van het type systeem en betrokken actoren. Er kunnen meerdere categorieën van toepassing zijn.

§ 3.3.18 resource.attribute

Attribuut	Beschrijving
Attribuutnaam	resource.attribute
Definitie Engels	Attributes in the form of key value pairs.
Attribuutnaam Nederlands	informatiebron.attribuut
Definitie Nederlands	Attribuutsoorten in de vorm van key value pairs.
Toelichting	Organisaties hebben de vrijheid om zelf key value pairs te bepalen als dit bijdraagt aan de inzichtelijkheid voor de logging van een gegevensverwerkingsactie. Naast naam en versie van de informatiebron, kan de organisatie andere attribuutsoorten definiëren ten aanzien van de informatiebron.
Noodzakelijkheid	In AVG grond 61 wordt de volgende maatregel benoemd: <i>De informatie over de verwerking van persoonsgegevens betreffende de betrokkene dient hem te worden meegedeeld bij het verzamelen bij de betrokkene van de gegevens of, indien de gegevens uit een andere bron zijn verkregen, binnen een redelijke termijn, die afhangt van de omstandigheden van het geval. Wanneer de persoonsgegevens rechtmatig aan een andere ontvanger kunnen worden verstrekt, dient de betrokkene te worden meegedeeld wanneer de persoonsgegevens voor het eerst aan de ontvanger worden verstrekt. Wanneer de verantwoordelijke voornemens is de persoonsgegevens te verwerken met een ander doel dan dat waarvoor zij zijn verzameld, moet de verantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en andere noodzakelijke informatie verstrekken. Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt. De organisatie kan meerdere attribuutsoorten definiëren indien dit preciezere informatie oplevert ten aanzien van de gegevensbron.</i>

Attribuut	Beschrijving
Datatype	-
Voorbeeld	-
Verplicht	Nee
Gebruikt in	Logboek
Enumeratiewaarden	-

§ 3.3.19 resource.name

Attribuut	Beschrijving
Attribuutnaam	resource.name
Definitie Engels	Name of any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, a data processing organisation.
Attribuutnaam Nederlands	informatiebron.naam
Definitie Nederlands	Naam van een materieel of immaterieel bezit dat gegevens in elektronische vorm kan genereren, verzenden, ontvangen, verwerken of vertegenwoordigen, waarbij het actief eigendom is van, in licentie is gegeven, wordt geëxploiteerd, beheerd of beschikbaar wordt gesteld door, of anderszins wordt gebruikt door, een gegevensverwerkingsorganisatie.
Toelichting	Naam (name) is een attribuutsoort van het objecttype Informatiebron (Resource).
Noodzakelijkheid	In AVG grond 61 wordt de volgende maatregel benoemd: <i>De informatie over de verwerking van persoonsgegevens betreffende de betrokkene dient hem te worden meegedeeld bij het verzamelen bij de betrokkene van de gegevens of, indien de gegevens uit een andere bron zijn verkregen, binnen een redelijke termijn, die afhangt van de omstandigheden van het geval. Wanneer de persoonsgegevens rechtmatig aan een andere ontvanger kunnen worden verstrekt, dient de betrokkene te worden meegedeeld wanneer de persoonsgegevens voor het eerst aan de ontvanger worden verstrekt. Wanneer de verantwoordelijke voornemens is de persoonsgegevens te verwerken met een ander doel dan dat waarvoor zij zijn verzameld, moet de verantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en andere noodzakelijke informatie verstrekken. Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt.</i>
Datatype	CharacterString
Voorbeeld	Vergunningenadministratie
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.20 resource.version

Attribuut	Beschrijving
Attribuutnaam	resource.version
Definitie Engels	Version of any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, a data processing organisation.
Attribuutnaam Nederlands	informatiebron.versie
Definitie Nederlands	Naam van een materieel of immaterieel bezit dat gegevens in elektronische vorm kan genereren, verzenden, ontvangen, verwerken of vertegenwoordigen, waarbij het actief eigendom is van, in licentie is gegeven, wordt geëxploiteerd, beheerd of beschikbaar wordt gesteld door, of anderszins wordt gebruikt door, een gegevensverwerkingsorganisatie.
Toelichting	Versie (version) is een attribuutsoort van het objecttype Informatiebron (Resource).

Attribuut	Beschrijving
Noodzakelijkheid	In AVG grond 61 wordt de volgende maatregel benoemd: <i>De informatie over de verwerking van persoonsgegevens betreffende de betrokkene dient hem te worden meegedeeld bij het verzamelen bij de betrokkene van de gegevens of, indien de gegevens uit een andere bron zijn verkregen, binnen een redelijke termijn, die afhangt van de omstandigheden van het geval. Wanneer de persoonsgegevens rechtmatig aan een andere ontvanger kunnen worden verstrekt, dient de betrokkene te worden meegedeeld wanneer de persoonsgegevens voor het eerst aan de ontvanger worden verstrekt. Wanneer de verantwoordelijke voornemens is de persoonsgegevens te verwerken met een ander doel dan dat waarvoor zij zijn verzameld, moet de verantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en andere noodzakelijke informatie verstrekken. Wanneer de oorsprong van de persoonsgegevens niet aan de betrokkene kan worden meegedeeld omdat verschillende bronnen zijn gebruikt, moet algemene informatie worden verstrekt.</i> Van sommige informatiebronnen zijn meerdere versies aanwezig. In dit geval is de vermelding van de versie van deze informatiebron een preciezere definitie.
Datatype	CharacterString
Voorbeeld	1.0.1.e
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.21 startTime

Attribuut	Beschrijving
Attribuutnaam	startTime
Definitie Engels	Timestamp representing the start of a data processing logging action.
Attribuutnaam Nederlands	startTijd
Definitie Nederlands	Tijdstempel die het begin van een logboekactie voor gegevensverwerking vertegenwoordigt.
Toelichting	Een logboekregel wordt pas weggeschreven in het logboek als de volledige transactie (succesvol of niet succesvol) is afgerond.
Noodzakelijkheid	Bij een inzageverzoek van de Betrokkene ten aanzien van gegevensverwerkingsactie, wordt ook een tijdsspanne gevraagd. Alleen de details van gegevenswerkingactie binnen opgegeven tijdsspanne worden gerapporteerd. Zonder begin- en eindtijd van een gegevensverwerkingactie is het onmogelijk de juiste details op te leveren.
Datatype	DateTime
Voorbeeld	2025-02-23T00:00:00
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 3.3.22 statusCode

Attribuut	Beschrijving
Attribuutnaam	statusCode
Definitie Engels	Indicates whether a request has been processed successfully or not by the server.
Attribuutnaam Nederlands	statusCode
Definitie Nederlands	Geeft aan of een verzoek al dan niet met succes door de server is verwerkt.
Toelichting	Als een geautomatiseerd verzoek correct wordt afgehandeld, dan zal de status 'OK' zijn. Bij een foutmelding (ongeacht het type foutmelding) zal de statusCode 'NOK' zijn.

Attribuut	Beschrijving
Noodzakelijkheid	Indien een gegevensverwerkingactie heeft plaatsgevonden, is het van belang te weten of deze verwerkingsactie gelukt is of niet. Zonder de statuscode kan er niet worden gerapporteerd aan een betrokkene of een wijziging daadwerkelijk heeft plaatsgevonden.
Datatype	Enumwaarde
Voorbeeld	OK
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	0: Unknown 1: OK 2: NOK

§ 3.3.23 traceId

Attribuut	Beschrijving
Attribuutnaam	traceId
Definitie Engels	Unique identifier of the request in the system, which adds the possibility of tracing the history of the request in detail.
Attribuutnaam Nederlands	traceerId
Definitie Nederlands	Unieke identificatie van een bericht in het systeem, waarmee de mogelijkheid ontstaat om de geschiedenis van het bericht in detail te volgen.
Toelichting	Een trace is het proces waarbij informatie wordt vastgelegd over de stroom van transacties of verzoeken van een applicatie of systeem. Logboekregistratie is doorgaans breder van opzet en legt een breder scala aan gebeurtenissen vast, terwijl tracering meer specifieke informatie biedt over het uitvoeringspad van individuele verzoeken.
Noodzakelijkheid	De traceId is de unieke factor die alle (sub)gegevenswerkingsacties die betrekking hebben op een (hoofd)gegevensverwerkingactie aan elkaar verbindt. Zonder de traceId kan een totaal aan elkaar gelieerde gegevensverwerkingsacties niet worden gerapporteerd.
Datatype	URI
Voorbeeld	6e8bc430-9c3a-11d9-9669-0800200c9a66
Verplicht	Ja
Gebruikt in	Logboek
Enumeratiewaarden	Niet van toepassing

§ 4. Besluitenlijst

Deze sectie is *tijdelijk* en *niet normatief*, bedoeld om informatie te geven over achterliggende afwegingen bij de standaard.

In de definitieve standaard wordt deze lijst niet opgenomen, omdat veel afwegingen specifiek zijn voor de context van de Nederlandse overheid waarin deze standaard is ontstaan. De standaard is breder inzetbaar, en voor de implementatie is het niet relevant om de afwegingen bij alle aspecten van de standaard in de context van de Nederlandse overheid te kennen.

§ 4.1 Logregels bevatten alleen wat nodig is voor verantwoording door verantwoordelijke

Dit onderdeel is niet normatief.

- Status: draft
- Datum: 2024-06-24

§ 4.1.1 Context en probleemstelling

Vanuit de wens om zoveel mogelijk context vast te leggen om zo een compleet beeld te schetsen van wat er is gebeurd rond een [Dataverwerking](#) kan de neiging ontstaan om informatie uit andere organisaties vast te leggen in de logregels.

Hierdoor kom je al snel in lastig vaarwater, juridisch gezien. Er worden dan zaken vastgelegd die niet noodzakelijk zijn voor het verantwoorden van het handelen. Bovendien is het mogelijk om een compleet beeld te krijgen door de informatie te laten in de organisatie waar een dataverwerking is uitgevoerd. Dit is dan ook beter om te doen, vanuit het oogpunt van dataminimalisatie.

Voor de uitoefening van het Inzagerecht is de consequentie dat de Betrokkene informatie uit alle organisaties moet ophalen en deze volgens een paar relatief eenvoudige businessrules aan elkaar moet relateren voor het verkrijgen van een compleet beeld. Dit kan door alle organisaties te bevragen, of door gericht bij één organisatie te beginnen en vervolgens de URI's te volgen naar logrecords in andere organisaties.

Het kan zijn dat organisatie A de logs wel op orde heeft, en organisatie B (nog) niet. Dan is het resultaat dat geen compleet beeld kan worden gegeven. Daarmee komt de prikkel tot verbetering op de juiste plek, namelijk bij de organisatie die het Logboek nog niet op orde heeft.

§ 4.1.2 Besluit

Logregels bevatten alleen wat nodig is voor verantwoording door de Verantwoordelijke.

§ 4.1.3 Gevolgen

- In logregels wordt alleen een identifier vastgelegd van gerelateerde Dataverwerkingen in een andere context (bijv. een andere organisatie), geen inhoudelijke informatie
- Voor een analyse, bijvoorbeeld in het kader van een audit of uitoefening inzagerecht, is het nodig om op dat moment de URI's naar logs in andere organisaties te volgen

§ 4.2 Logregels bevatten geen gegevens die al vastliggen in een [Register](#)

Dit onderdeel is niet normatief.

- Status: proposed
- Datum: 2024-02-01

§ 4.2.1 Context en probleemstelling

Om logs zo begrijpelijk mogelijk te maken is het aantrekkelijk om de benodigde informatie redundant weg te schrijven in elk logrecord, zodat er geen afhankelijkheid bestaat van andere bronnen.

Dit heeft nadelen, zoals:

- Wanneer de statische gegevens (zoals bewaartermijn, verantwoordelijke, etc.) wijzigen, zou dit moeten worden aangepast in alle logrecords. Dat verhoudt zich slecht tot het 'immutable' (onveranderbaar) zijn van deze logrecords.
- De grote vrijheid in alle clients om invulling te geven aan deze gegevens leidt er vrijwel zeker toe dat verdere divergentie optreedt. Dit heeft o.a. tot gevolg dat het lastig wordt om te rapporteren uit de logs
- De API voor het wegschrijven van logs wordt ingewikkeld en relatief traag voor het wegschrijven van records
- We niet voldoen aan alle uitgangspunten die horen bij dataminimalisatie

In de gewenste situatie:

- staan alle statische gegevens in het Register van de Verwerkingsactiviteiten (RvVA), en bevatten logrecords verwijzen naar dat Register. Specifiek gaat dit om de resources '[verwerkingsactiviteiten](#)' en 'organisaties'.
- kan bij het configureren van clients in de RvVA-API worden opgezocht welke organisaties en verwerkingsactiviteiten van toepassing zijn
- kunnen wijzigingen in verwerkingsactiviteiten worden doorgevoerd zonder dat logrecords gewijzigd behoeven te worden

Met name het wegschrijven van logs kan op deze manier met hogere performance worden uitgevoerd. Dit kan nog verder worden geoptimaliseerd door niet te vereisen dat dit middels REST API calls gebeurt, maar een interface te definiëren die kan worden geïmplementeerd met bijvoorbeeld gRPC of andere streaming protocollen.

Wanneer het aan de gebruiker is om in de software die de Logboek API aanroept de namen van acties, de vertrouwelijkheid en de bewaartermijn te bepalen, zal de invulling daarvan op allerlei manieren uiteen gaan lopen. Door dit in het RvVA te bepalen zal eerder uniformering plaatsvinden. De vulling van RvVA's kan waarschijnlijk zelfs in hoge mate gestandaardiseerd worden.

Met meer gestandaardiseerde namen en bewaartermijnen en een eenduidige omgang met vertrouwelijkheid is het ook eenvoudiger om eenduidig te communiceren naar de [Betrokkene](#). Bijvoorbeeld: een portaal dat aan de Betrokkene toont hoe de persoonsgegevens zijn verwerkt, is lastig vorm te geven wanneer in de praktijk blijkt dat software-leveranciers verschillende interpretaties hebben van het niveau waarbij sprake is van een verwerking, handeling of actie. Eenduidige interpretatie is cruciaal, en dit kan waarschijnlijk alleen in het RvVA.

Overigens werkt het conceptueel wél wanneer men geen API op het RvVA aanbiedt, deze link kan ook handmatig worden gelegd iedere keer als deze informatie nodig is, en het RvVA bijvoorbeeld alleen bestaat als Excel document.

§ 4.2.2 Besluit

Logregels bevatten geen informatie over Verwerkingsactiviteiten en Verantwoordelijkheden die al vastliggen in een Register

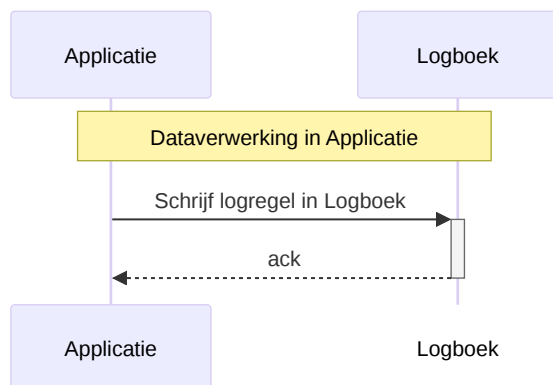
§ 4.2.3 Gevolgen

- In de standaard Logboek Dataverwerkingen is het nodig om ook de benodigde interface op de RvVA te standaardiseren. Dit is nodig om de logs geautomatiseerd en realtime te kunnen interpreteren: zonder gestandaardiseerde manier om informatie over verwerkingsactiviteiten op te vragen kan men aan logregels niet zien of het verwerkingen, handelingen of acties betreft.

Met de volgende sequentie diagrammen wordt in beeld gebracht wat de gevolgen zijn voor de diverse flows in het gebruik van de standaard.

§ 4.2.3.1 Loggen van een verwerking

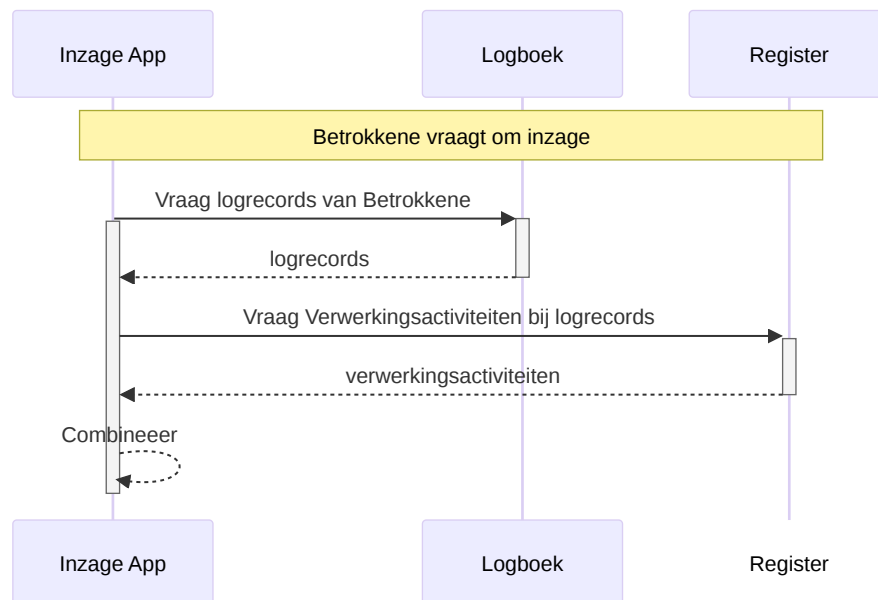
Het wegschrijven van een verwerking in de log-API is uiterst simpel:



Deze transactie is geoptimaliseerd op eenvoud en snelheid, want deze heeft rechtstreeks invloed op de snelheid van verwerkingen. Deze transactie moet schaalbaar zijn naar bijv. tienduizenden transacties per seconde.

§ 4.2.3.2 Tonen van een verwerking

Voor het op betekenisvolle manier tonen van verwerkingen aan bijvoorbeeld een Betrokkene is het dan nodig om gegevens op te vragen uit zowel de logs als het RvVA. Deze flow mag wat complexer zijn, omdat deze niet voor alle vastgelegde data wordt uitgevoerd en het belang van de bevraging rechtvaardigt dat een bevraging wat langer kan duren.



§ 4.3 Bewaartermijnen worden in het Profiel vastgelegd

Dit onderdeel is niet normatief.

- Status: draft
- Datum: 2024-05-23

§ 4.3.1 Context en probleemstelling

Logrecords moeten op enig moment worden verwijderd. Wanneer?

Voor vrijwel alle vastgelegde gegevens geldt dat deze op enig moment moeten worden vernietigd of overgebracht naar een archief. Dit geldt ook voor logrecords.

Anders dan bij gegevens over rechtsfeiten zullen logrecords typisch allemaal dezelfde bewaartermijn hebben. Het kan zijn dat de Dataverwerking waar het logrecord betrekking op heeft leidt tot gegevens waarvoor complexe bewaartermijnen gelden (bijvoorbeeld een dynamische termijn die duurt totdat Betrokkene is overleden gevolgd door een statische termijn van enkele tientallen jaren). De logrecords die de Dataverwerking beschrijven kennen deze complexe bewaartermijn niet, deze kunnen statisch zijn en generiek worden vastgesteld per organisatie of eventueel per verwerkingsactiviteit. Het is aan de organisatie zelf om daarin keuzes te maken.

Voor samenwerkende organisaties die zich ten doel stellen om gezamenlijk op eenduidige manier te verantwoorden over dataverwerkingen kan het nuttig zijn afspraken over bewaartermijnen vast te leggen in een Profiel.

§ 4.3.2 Besluit

Bewaartermijnen worden in het Profiel vastgelegd.

§ 4.3.3 Gevolgen

- In de Logregel liggen geen gegevens vast over bewaartermijnen.
- Vanuit een beheercomponent (een applicatie die functionaliteit biedt voor beheren van logboek. Is een kwestie van implementatie en valt buiten scope van deze standaard) kunnen Logregels worden verwijderd door te kijken naar de datum van de Logregel in relatie tot de bewaartermijn die de organisatie hanteert voor Logregels. Deze bewaartermijn kan gezamenlijk zijn afgesproken en ligt dan vast in het Profiel.

§ 4.4 Geen gegevens over gebruikers in logregels

Dit onderdeel is niet normatief.

- Status: draft
- Datum: 2024-05-23

§ 4.4.1 Context en probleemstelling

Om te verantwoorden dat een dataverwerking correct is uitgevoerd is het nodig te weten wie de dataverwerking heeft geïnitieerd, zodat kan worden nagegaan dat dit met de juiste autorisatie is gedaan.

De wens zou kunnen bestaan om in elke logregel vast te leggen welke gebruiker een rol heeft gehad bij de betreffende Dataverwerking.

Echter, de vastlegging van een handeling van een gebruiker als medewerker van een organisatie betreft ook een Dataverwerking die onder de AVG valt, waardoor rechten ontstaan voor de betreffende gebruiker om Inzage te verkrijgen. De vastlegging van de betrokkenheid van de gebruiker is een Dataverwerking op zich. Door een dergelijke vastlegging in de logregels te doen ontstaat een ongewenste recursiviteit.

Ook is de relatie van de gebruiker tot de Dataverwerking niet eenvoudig eenduidig te modelleren, o.a. omdat bij een enkele Dataverwerking meerdere gebruikers in meerdere rollen betrokken kunnen zijn.

Daarnaast kan het goed zijn dat de Dataverwerking in het Audit Log (Een log file die activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen vastgelegd. Dit is o.a. vanuit BIO verplicht) onder een andere Verantwoordelijke valt dan de Dataverwerking die op dat moment door de gebruiker wordt uitgevoerd. Bijvoorbeeld:

- Een Dataverwerking wordt door een gebruiker bij een [Verwerker](#) uitgevoerd
- De Dataverwerking valt onder verantwoordelijkheid van de [Verantwoordelijke](#), namelijk de organisatie die de Verwerker heeft ingehuurd
- De Audit Log is een aparte Dataverwerking die valt onder verantwoordelijkheid van de Verwerker, in de rol van Verantwoordelijke over de eigen bedrijfsvoering.

Het is daarom zuiverder om een andere oplossing te kiezen, namelijk:

- Betrokkenheid van gebruiker wordt vastgelegd in een Audit Log (buiten scope van deze standaard)
- In het Audit Log kan eventueel een relatie worden gelegd met het Processing ID dat ook in het Logboek Dataverwerkingen wordt gebruikt
- Iedere keer dat in het Audit Log gegevens over een gebruiker worden vastgelegd, moet tevens een Dataverwerking worden gelogd in het Logboek Dataverwerkingen.

Let wel, deze Dataverwerking is een *andere Dataverwerking* dan de Dataverwerking die op dat moment wordt uitgevoerd door de Gebruiker, heeft een eigen Trace Context, en wordt gerelateerd aan een andere Verwerkingsactiviteit.

§ 4.4.2 Besluit

In logregels worden geen identificerende gegevens over gebruikers van de Applicaties vastgelegd.

§ 4.4.3 Gevolgen

- In gevallen dat het nodig is te achterhalen welke gebruiker een specifieke Dataverwerking heeft uitgevoerd, moet dit worden achterhaald door de Dataverwerking te koppelen aan het Audit Log (buiten scope van de standaard)
- Het koppelen van Dataverwerking aan Audit Log is mogelijk door in Audit Logs hetzelfde Processing ID op te nemen als in de logregel die in het Logboek Dataverwerkingen wordt opgenomen.

§ 4.5 Standaard beschrijft geen interface voor verwijderen van logs

Dit onderdeel is niet normatief.

- Status: draft
- Datum: 2024-05-24

§ 4.5.1 Context en probleemstelling

Logrecords moeten op enig moment worden vernietigd. Moet er een interface in de standaard worden gedefinieerd voor het verwijderen van vastgelegde logrecords?

De wijze waarop logrecords worden weggeschreven is sterk afhankelijk van de keuzes die een organisatie maakt bij de implementatie van de standaard.

Interoperabiliteit is daarbij niet relevant, omdat het wijzigen of verwijderen van logrecords niet gebeurt vanuit de applicatie die oorspronkelijk de dataverwerking uitvoerde en het wegschrijven van het logrecord veroorzaakte. Wijzigen en verwijderen gebeurt vanuit een beheercomponent. Deze zijn vaak hard gekoppeld aan de voor logging gekozen oplossing, waardoor het voorschrijven van een interface tot onnodige complexiteit leidt.

§ 4.5.2 Besluit

- De standaard beschrijft geen interface voor het wijzigen of verwijderen van logrecords

§ 4.5.3 Gevolgen

- Iedere organisatie kan een bij de eigen implementatie passende oplossing kiezen voor het verwijderen van logrecords
- Het wijzigen van logrecords is in principe ongewenst maar kan op soortgelijke manier opgelost worden

§ 4.6 Vertrouwelijkheid wordt vastgelegd per Verwerkingsactiviteit

Dit onderdeel is niet normatief.

- Status: draft
- Datum: 2024-05-23

§ 4.6.1 Context en probleemstelling

Alle verwerkingen worden gelogd. Een deel van deze verwerkingen mag bekend worden bij Betrokkenen, een deel niet. Hoe moet dit onderscheid geïmplementeerd worden?

Voorbeeld:

- Opsporingsinstantie A be vraagt bij Overheidsorgaan B gegevens op over Betrokkene X in het kader van opsporingsactiviteiten rond een misdrijf
- Betrokkene krijgt geen inzage in / wordt niet geïnformeerd over de verwerking van Opsporingsinstantie A, dit zou het onderzoek hinderen
- Als Betrokkene wel inzage krijgt / wordt geïnformeerd over de verwerking van Overheidsorgaan B, zou Betrokkene alsnog zien dat Opsporingsinstantie A deze gegevens heeft opgevraagd, met hetzelfde ongewenste effect.

Er zijn meerdere oplossingsrichtingen denkbaar. Wat is de gewenste oplossingsrichting, hoe wordt deze gespecificeerd?

Mogelijke oplossingsrichtingen:

1. Ken aan iedere Dataverwerking een status toe waarmee de vertrouwelijkheid wordt aangeduid, en geef deze status mee in de verwerking zodat alle betrokken organisaties dit in de logs kunnen verwerken
2. Leg vertrouwelijkheid meer categorisch vast op het niveau van Verwerkingsactiviteiten (in het Register)

Overwegingen:

Vertrouwelijke verwerkingen moeten meer strikt gescheiden moeten worden van niet-vertrouwelijke verwerkingen. Wanneer een bevraging zowel vertrouwelijk als niet-vertrouwelijk kan zijn (voorbeeld: het opvragen van eigenaargegevens van een voertuig) moeten twee gescheiden processen bestaan, waarbij de vertrouwelijke variant niet alleen apart wordt gelogd, maar in het geheel aan meer strikte regels wordt onderworpen, zoals eisen aan betrokken beheerders, classificatie van gegevens, etc.

Pogingen om het geschetste probleem op te lossen door op logrecord-niveau vast te leggen of een verwerking vertrouwelijk is leiden tot veel complexiteit en uitzonderingsgevallen in de implementatie van de standaard. Een aantal voorbeelden van ongewenste complexiteit:

- Vertrouwelijkheid vastleggen per logrecord betekent dat deze vertrouwelijkheid ook moet kunnen worden opgeheven
- Logrecords zijn dan niet langer 'immutable' tenzij ingewikkelde constructies worden gekozen waarbij een logrecord logisch wordt vervangen door een nieuw record toe te voegen
- Er zou een interface gedefinieerd moeten worden voor het wijzigen van de status 'vertrouwelijkheid'
- Vertrouwelijkheid van een handeling aan het einde van een proces zou gevolgen kunnen hebben voor reeds vastgelegde logrecords

Bovendien geldt dat Overheidsorganisatie B op impliciete wijze zou leren dat Betrokkene X onderwerp is van een opsporingsonderzoek, terwijl dit beter op expliciete wijze geregeld kan worden. Door het expliciet te regelen kan Overheidsorganisatie B alle benodigde maatregelen nemen om te zorgen dat de vertrouwelijkheid ook in die organisatie geborgd is.

§ 4.6.2 Besluit

Vertrouwelijkheid wordt vastgelegd per Verwerkingsactiviteit

§ 4.6.3 Gevolgen

- Vertrouwelijkheid wordt niet vastgelegd in logrecords
- Vertrouwelijkheid wordt per logrecord afgeleid uit wat over vertrouwelijkheid is vastgelegd bij de bijbehorende Verwerkingsactiviteit
- Vertrouwelijkheid wordt NIET uitgewisseld tussen organisaties
- Wanneer een verwerking niet langer vertrouwelijk is, bijvoorbeeld na verjaring, dan volgt dit uit gegevens die vastliggen in het Register (bijvoorbeeld status vertrouwelijkheid, duur vertrouwelijkheid) en wat vastligt in een logrecord (verwerkingsactiviteit_id en datum)
- Organisaties moeten vooraf borgen dat vertrouwelijke Dataverwerkingen worden uitgevoerd op een manier die verantwoord kan worden, door dit te regelen op het niveau van Verwerkingsactiviteit. Dit kan tot gevolg hebben dat twee aparte processen nodig zijn voor het vertrouwelijk en niet-vertrouwelijk opvragen van gegevens.

§ 4.7 Verwijzingen naar Registers zijn zo los mogelijk

Dit onderdeel is niet normatief.

- Status: proposed
- Datum: 2024-05-24

§ 4.7.1 Context en probleemstelling

In de logrecords staat zo min mogelijk inhoudelijke informatie [API Design Rules \(Nederlandse API Strategie IIa\)](#). Informatie over verwerkingsactiviteiten ligt vast in specifieke registers.

- Er kunnen meerdere van deze Registers zijn
- Deze kunnen ook van andere organisaties zijn
- Naar welk Register wordt verwezen is afhankelijk van het type dataverwerking. Verwerkingen in het kader van de Algemene Verordening Gegevensbescherming (AVG) verwijzen naar een Register van Verwerkingsactiviteiten zoals beschreven in AVG art. 30.
- Het Register van Verwerkingsactiviteiten (RvVA) is voor veel organisaties verplicht vanuit AVG art. 30, echter niet voor alle organisaties
- Als een Register bestaat, betekent dit niet dat het ook ontsloten wordt met een API. In de huidige praktijk bestaat het vaak alleen in een statisch document.

De standaard voor logging moet functioneren gegeven bovenstaande feiten.

§ 4.7.2 Besluit

De link naar de uitwerking van een verwerkingsactiviteit bestaat uit een *identifier* en daarnaast een URI, URL of URN, in de vorm van *key value pairs*. Eventuele nadere invulling voor het verwijzen naar specifieke Registers (zoals het RvVA) wordt uitgewerkt in extensies.

§ 4.7.3 Gevolgen

{ Wat zijn de gevolgen na het nemen van dit besluit }

§ 4.8 Log Sampling is niet toegestaan

Dit onderdeel is niet normatief.

- Status: proposed
- Datum: 2024-06-20

§ 4.8.1 Context en probleemstelling

Een bij logging veelgebruikte techniek is het zogenaamde 'Log Samplen', waarbij bijvoorbeeld slechts 1 op de 10 of 1 op de 100 acties die een log zouden veroorzaken daadwerkelijk worden weggeschreven. Dit wordt gedaan uit overwegingen van performance, opslagruimte en/of kosten. Voor veel toepassingen is het voldoende om uit deze logs trends te destilleren om zo fouten op te sporen of voorstellen voor verbetering te kunnen doen.

Wanneer dit zou worden toegepast bij onderhanden standaard, zou kunnen worden betoogd dat verantwoording nog altijd slaagt, omdat data voor een relevante, gerandomiseerde steekproef beschikbaar is. Echter, gelet op het belang van de

verantwoording, en de wettelijke verplichtingen waaraan met de standaard invulling wordt gegeven, is dit onwenselijk voor het Logboek Dataverwerkingen. De Logregels vormen o.a. de basis voor de Informatieplicht en het Inzagerecht uit de AVG. Daarvoor is het nodig om over iedere Dataverwerking metagegevens vast te leggen.

§ 4.8.2 Besluit

Log Sampling is niet toegestaan.

§ 4.8.3 Gevolgen

- Iedere logregel wordt weggeschreven in het LogBoek Dataverwerkingen
- Wanneer een techniek voor loggen wordt toegepast waarbij Log Sampling is ingericht, moet ervoor worden gewaakt dat dit niet geldt voor de logregels die beschreven worden in deze standaard.

§ 5. Voorbeelden

In dit hoofdstuk worden er voorbeelden beschreven van hoe de standaard gebruikt kan worden in verschillende scenario's om de lezer een beter beeld te geven van de standaard in zijn echte werking. Hierbij zijn er vier voorbeelden met elk een schets van de situatie, de uitgangspunten, het globale proces, de relatie tussen gegevens, de relatie met het Logboek Dataverwerkingen en het gedrag van de applicatie.

§ 5.1 Parkeervergunning - inzien

§ 5.1.1 Situatieschets (Parkeervergunning - inzien)

Een persoon heeft bij een gemeente een parkeervergunning in gebruik en wil de gegevens van deze vergunning bekijken.

§ 5.1.2 Uitgangspunten (Parkeervergunning - inzien)

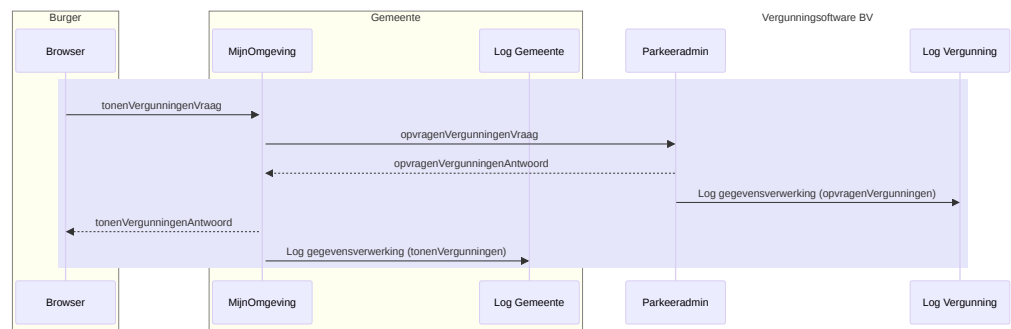
- Het beschreven proces is een voorbeeld, het werkelijke proces kan anders verlopen.
- Het proces is een 'happy flow' dit betekent dat validaties en eventuele foutsituaties in dit voorbeeld niet in ogenschouw worden genomen.
- Autorisatieprocessen zijn in dit voorbeeld niet meegenomen.
- Een Loggingsregel wordt toegevoegd aan het logboek per **geheel** afgeronde transactie. Er wordt dus **geen** aparte logregel aangemaakt per ontvangen of verstuurd bericht.
- Een aantal gegevens staan nog ter discussie (vanuit juridisch oogpunt). Voor de volledigheid worden een aantal gegevens in dit voorbeeld meegenomen. Het betreft de gegevens:
 - resource/name/version
 - receiver
 - dataSubject

§ 5.1.3 Globaal proces (Parkeervergunning - inzien)

1. Een persoon vraagt in zijn 'MijnOmgeving' van de gemeente om de bestaande parkeervergunninggegevens.
2. De 'MijnOmgeving' van de gemeente verzoekt de parkeervergunningapplicatie om de actuele parkeervergunninggegevens van de persoon.

3. Het parkeervergunningensysteem voert dit verzoek uit. Daarna verzendt de parkeervergunningapplicatie de gevraagde gegevens naar de gemeente. Het parkeervergunningensysteem logt dat er gegevens verzonden zijn naar de gemeente.
4. De gemeente toont de gegevens aan de persoon en logt dat deze gegevens zijn getoond aan de persoon.

Schematisch ziet dit proces er als volgt uit:



§ 5.1.4 Logging van gegevens (Parkeervergunning - inzien)

De volgende gegevens worden gelogd in de diverse logmomenten:

Log opvragenVergunningen (log vergunningenapplicatie):

Attribuut	Waarde
operationId	8451dcd9ede037cb
operationName	opvragenVergunningen
parentOperationId	<leeg>
traceId	ccf5064a324163ed939bfa09c2bcb210
startTime	2024-05-30 08:40:37.000
endTime	2024-05-30 08:40:37.000
statusCode	OK
resource.name	Parkeeradmin
resource.version	2.1.6
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	rva:12f2ec2a-0cc4-3541-9ae6-219a178fcfe4
attributeKey	<leeg>
attributeValue	<leeg>
foreignOperation.traceId	c7a26dcd0bee0c8900e2174c43c3393c
foreignOperation.operationId	9f8971bfd093637d

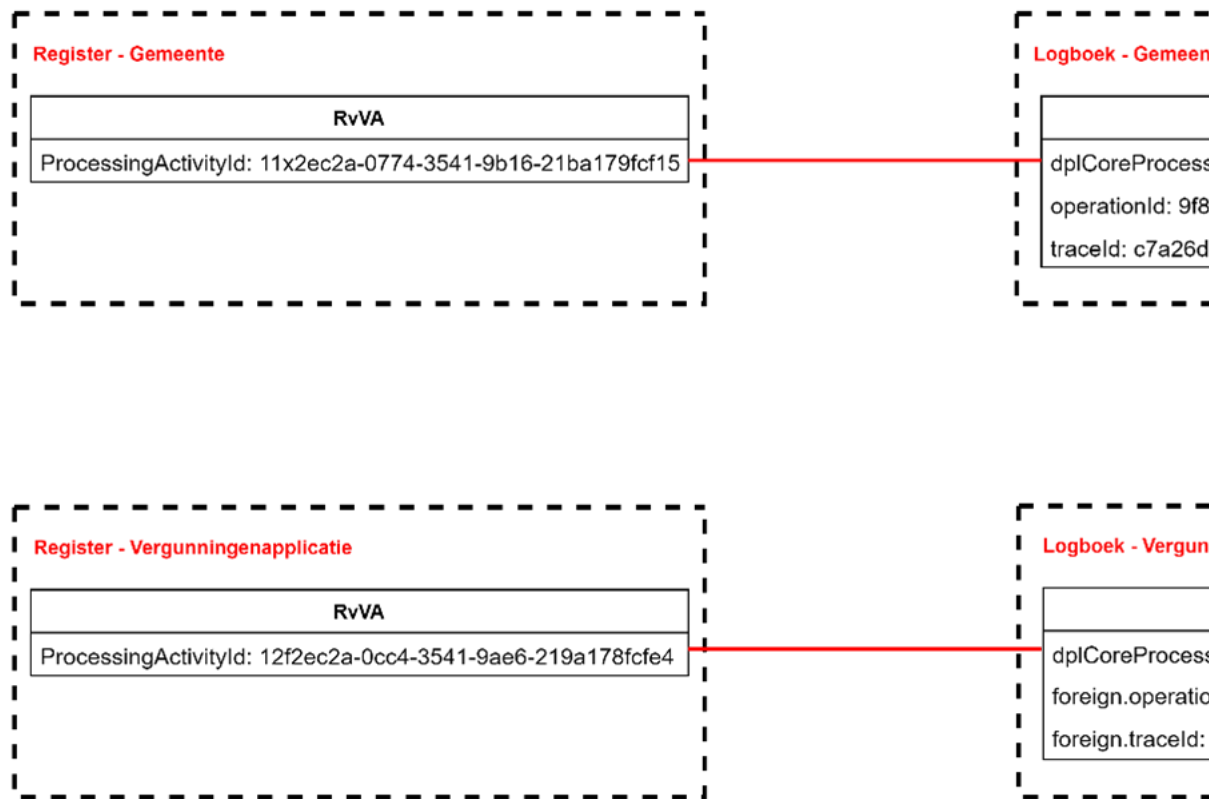
Log opvragenVergunningen (log gemeente)

Attribuut	Waarde
operationId	9f8971bfd093637d
operationName	tonenVergunningen
parentOperationId	<leeg>
traceId	c7a26dcd0bee0c8900e2174c43c3393c
startTime	2024-05-30 10:40:37.821
endTime	2024-05-30 10:40:37.845
statusCode	OK
resource.name	MijnOmgeving
resource.version	1.0.5
receiver	27fdey98605etc48

Attribuut	Waarde
attributeKey	dplCoreProcessingActivityId
attributeValue	rva:11x2ec2a-0774-3541-9b16-21ba179cf15
attributeKey	dplCoreDataSubjectId
attributeValue	rva:13j2ec27-0cc4-3541-9av6-219a178fcfe5

§ 5.1.5 Relatie tussen gegevens (Parkeervergunning - inzien)

Om uiteindelijk alle gegevens te kunnen rapporteren, is het van belang dat gegevens op een bepaalde manier aan elkaar gekoppeld zijn. In dit voorbeeld zijn de gegevens op de volgende manier gekoppeld:



§ 5.1.6 Relatie met de standaard Logboek dataverwerkingen (Parkeervergunning - inzien)

De relatie met de doelstellingen die gesteld zijn in de standaard Logboek dataverwerkingen worden, op basis van dit voorbeeld, als volgt concreet gerealiseerd:

- **het wegschrijven van logs van dataverwerkingen:** In dit voorbeeld is het de betrokkene zelf die via een portaal zijn eigen gegevens kan bekijken. Deze actie is een gegevensverwerking en wordt gelogd bij zowel de gemeenteapplicatie (gegevens worden getoond aan de betrokkene) als bij de vergunningenapplicatie (verstrekking specifieke informatie aan de gemeenteapplicatie).
- **het aan elkaar relateren van logs van dataverwerkingen:** Er zijn in dit voorbeeld twee applicaties nodig om het totaal aan gevraagde informatie te kunnen tonen aan de betrokkene. Beide applicaties hebben een logboek voor verwerkte gegevens. Om een totaalbeeld van de gelogde gegevens te kunnen construeren, is een relatie tussen de logs nodig. In dit voorbeeld wordt de koppeling gelegd door het operationId en traceId (gemeentelogboek) te linken aan het foreignOperationId en foreignTraceId (vergunningenlogboek).
- **het aan elkaar relateren van dataverwerkingen over de grenzen van systemen:** Naast het koppelen van logs van diverse applicaties, wordt ook een koppeling gelegd met het Register van verwerkingsactiviteiten. Dit gebeurt per applicatie op basis van het ProcessingActivityId (register) te koppelen aan dplCoreProcessingActivityId (logboek). De diverse registers hebben **geen** directe koppeling met elkaar.

Standaard Logverwerkingen: **paragraaf 3.3.1 Gedrag**

1. De applicatie MOET een Trace starten voor iedere Dataverwerking waarvan nog geen Trace bekend is. Bij elke start van een verwerking wordt een traceId aangemaakt. Bijvoorbeeld: in het voorbeeld komt er een bericht binnen bij de 'MijnOmgeving' van de gemeente (opvragenVergunningenVraag). Er wordt direct een traceId aangemaakt.
2. De applicatie MOET voor iedere Dataverwerking een logregel wegschrijven in een Logboek. Log Sampling is niet toegestaan. Een dataverwerking wordt opgeslagen als deze volledig is afgerond. In het voorbeeld is te zien dat een logregel wordt geschreven op het moment dat de vraag- en het antwoordbericht zijn afgerond.
3. De applicatie MOET bijhouden of een Dataverwerking geslaagd of mislukt is en dit per Dataverwerking als status meegeven aan het Logboek. Bij elke logregel in het voorbeeld staat de statusCode vermeld ('OK').
4. Als een Dataverwerking meerdere Betrokkenen heeft dan MOET de applicatie voor iedere betrokkene een aparte logregel wegschrijven. Een logregel kan naar 0 of 1 betrokkenen verwijzen. In het voorbeeld gaat het om één betrokkene (dplCoreDataSubjectId), er wordt steeds één logregel aangemaakt.
5. Als een applicatie aangeroepen kan worden vanuit een andere applicatie MOET de applicatie Trace Context metadata accepteren bij een dergelijke aanroepen deze metadata kunnen omzetten naar een foreign_operation bericht. Bij een externe verwerking (bijvoorbeeld opvragenVergunningen) geeft de 'MijnOmgeving' de traceId en OperationId mee aan de Vergunningenapplicatie. De vergunningenapplicatie registreert de traceId en operationId beide als 'foreignOperation'.

§ 5.2 Parkeervergunning - wijzigen

§ 5.2.1 Situatieschets (Parkeervergunning - wijzigen)

Een persoon heeft bij een gemeente een parkeervergunning in gebruik en wil de gegevens van het kenteken van deze vergunning wijzigen.

§ 5.2.2 Uitgangspunten (Parkeervergunning - wijzigen)

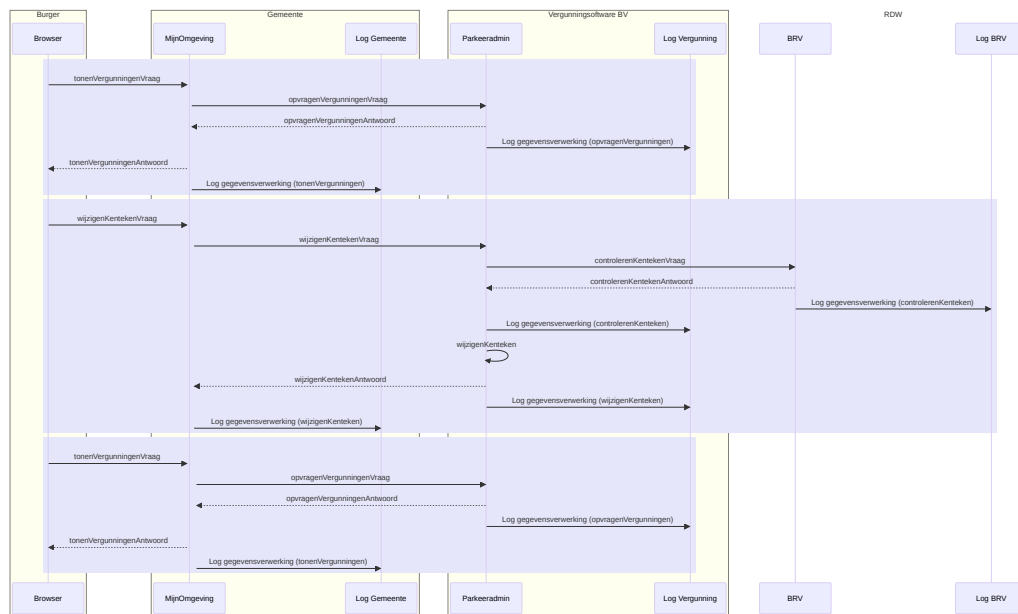
- Het beschreven proces is een voorbeeld, het werkelijke proces kan anders verlopen.
- Het proces is een 'happy flow' dit betekent dat validaties en eventuele foutsituaties in dit voorbeeld niet in ogenschouw worden genomen.
- Autorisatieprocessen zijn in dit voorbeeld niet meegenomen.
- Een Loggingsregel wordt toegevoegd aan het logboek per **geheel** afgeronde transactie. Er wordt dus **geen** aparte logregel aangemaakt per ontvangen of verstuurd bericht.
- Een aantal gegevens staan nog ter discussie (vanuit juridisch oogpunt). Voor de volledigheid worden een aantal gegevens in dit voorbeeld meegenomen. Het betreft de gegevens:
 - resource/name/version
 - receiver
 - dataSubject

§ 5.2.3 Globaal proces (Parkeervergunning - wijzigen)

1. Een persoon vraagt in zijn 'MijnOmgeving' van de gemeente om de bestaande parkeervergunninggegevens.
2. De 'MijnOmgeving' van de gemeente verzoekt de parkeervergunningapplicatie om de actuele parkeervergunninggegevens van de persoon.
3. De parkeervergunningapplicatie voert dit verzoek uit. Daarna verzendt de parkeervergunningapplicatie de gevraagde gegevens naar de gemeente. De parkeervergunningapplicatie logt dat er gegevens verzonden zijn naar de gemeente.
4. De gemeente toont de gegevens aan de persoon en logt dat deze gegevens zijn getoond aan de persoon.
5. De persoon wijzigt het kenteken in de 'MijnOmgeving' van de gemeente.
6. De 'MijnOmgeving' van de gemeente verzoekt de parkeervergunningapplicatie om de wijziging af te handelen.
7. De parkeervergunningapplicatie verzoekt het RDW te controleren of het kenteken ook daadwerkelijk bij de persoon hoort.

8. Het RDW stuurt een antwoord terug naar de parkeervergunningapplicatie en logt de gegevensverwerking.
9. De parkeervergunningapplicatie logt het controleverzoek aan het RDW.
10. De parkeervergunningapplicatie wijzigt het kenteken van de persoon en logt het wijzigingsverzoek van de persoon.
11. Nadat de wijziging is gedaan in de parkeervergunningapplicatie, wordt het wijzigingsverzoek gelogd in de 'MijnOmgeving' van de gemeente.
12. De persoon vraagt in zijn 'MijnOmgeving' van de gemeente om de bestaande parkeervergunninggegevens.
13. De 'MijnOmgeving' van de gemeente verzoekt de parkeervergunningapplicatie om de actuele parkeervergunninggegevens van de persoon.
14. De parkeervergunningapplicatie voert dit verzoek uit. Daarna verzendt de parkeervergunningapplicatie de gevraagde gegevens naar de gemeente. De parkeervergunningapplicatie logt dat er gegevens verzonden zijn naar de gemeente.
15. De gemeente toont de gegevens aan de persoon en logt dat deze gegevens zijn getoond aan de persoon.

Schematisch ziet dit proces er als volgt uit:



§ 5.2.4 Logging van gegevens (Parkeervergunning - wijzigen)

De volgende gegevens worden gelogd in de diverse logmomenten:

1. Log opvragenVergunningen (log vergunningenapplicatie):

Attribuut	Waarde
operationId	8ee7b01aca8d01d9
operationName	opvragenVergunningen
parentOperationId	<leeg>
traceId	c6adf4df949d03c662b53e95debd411
startTime	2024-07-29 08:16:49.000
endTime	2024-07-29 08:16:49.000
statusCode	OK
resource.name	Parkeeradmin
resource.version	2.1.6
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	12f2ec2a-0cc4-3541-9ae6-219a178fcfe4
attributeKey	<leeg>
attributeValue	<leeg>

Attribuut	Waarde
foreignOperation.traceId	bc9126aaae813fd491ee10bf870db292
foreignOperation.operationId	b2e339a595246e01

2. Log tonenVergunningen (log gemeente)

Attribuut	Waarde
operationId	b2e339a595246e01
operationName	tonenVergunningen
parentOperationId	<leeg>
traceId	bc9126aaae813fd491ee10bf870db292
startTime	2024-07-29 10:16:49.690
endTime	2024-07-29 10:16:49.723
statusCode	OK
resource.name	MijnOmgeving
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	11x2ec2a-0774-3541-9b16-21ba179fcf15
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5

3. Log controlerenKenteken (log RDW)

Attribuut	Waarde
operationId	433f276975204ccf
operationName	controlerenKenteken
parentOperationIdcontrolerenKenteken	<leeg>
traceId	8ccfd3c567c51d68937c263e00a352be
startTime	2024-07-29 08:17:02
endTime	2024-07-29 08:17:02
statusCode	OK
resource.name	BRV
resource.version	2.0
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	8c714e4a-a538-36f7-8b1f-37a6884cc68c
attributeKey	dplCoreDataSubjectId
attributeValue	<leeg>
foreignOperation.traceId	f176a58de7fe249ea37ed4f5979da02b
foreignOperation.operationId	414514cf1d40d6b2

4. Log controlerenKenteken (log vergunningenapplicatie)

Attribuut	Waarde
operationId	414514cf1d40d6b2
operationName	controlerenKenteken
parentOperationId	7a95b6989d2b28c7
traceId	f176a58de7fe249ea37ed4f5979da02b
startTime	2024-07-29 08:17:02.000
endTime	2024-07-29 08:17:02.000
statusCode	OK

Attribuut	Waarde
resource.name	Parkeeradmin
resource.version	2.1.6
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	19u2dd2a-0cb7-3541-9ae6-217a178fc9e6
attributeKey	dplCoreDataSubjectId
attributeValue	<leeg>
foreignOperation.traceId	8a1325a32aef8de4ffba7d7c931eeaec
foreignOperation.operationId	ba7cac7ca0489e42

5. Log wijzigenKenteken (log vergunningenapplicatie)

Attribuut	Waarde
operationId	7a95b6989d2b28c7
operationName	wijzigenKenteken
parentOperationId	<leeg>
traceId	f176a58de7fe249ea37ed4f5979da02b
startTime	2024-07-29 08:17:02.000
endTime	2024-07-29 08:17:02.000
statusCode	OK
resource.name	Parkeeradmin
resource.version	2.1.6
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	0b1ff20a-3ecb-34bf-8cf5-e4cbacb046ab
attributeKey	dplCoreDataSubjectId
attributeValue	<leeg>
foreignOperation.traceId	c0a7a38d56f3f16a2163ca0071d3779a
foreignOperation.operationId	df524ee2a3fd5ddf

6. Log wijzigenKenteken (log gemeente)

Attribuut	Waarde
operationId	df524ee2a3fd5ddf
operationName	wijzigenKenteken
parentOperationId	<leeg>
traceId	c0a7a38d56f3f16a2163ca0071d3779a
startTime	2024-07-29 10:17:02.010
endTime	2024-07-29 10:17:02.039
statusCode	OK
resource.name	MijnOmgeving
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	12c21c2a-0875-3543-9b16-21ja179fcf16
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5
foreignOperation.traceId	<leeg>
foreignOperation.operationId	<leeg>

7. Log opvragenVergunningen (log vergunningenapplicatie)

Attribuut	Waarde
operationId	6042d706f53fec76
operationName	opvragenVergunningen
parentOperationId	<leeg>
traceId	c6c2d53a5762d47779c57057d7983311
startTime	2024-07-29 08:17:02.000
endTime	2024-07-29 08:17:02.000
statusCode	OK
resource.name	Parkeeradmin
resource.version	2.1.6
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	12f2ec2a-0cc4-3541-9ae6-219a178fcfe4
attributeKey	<leeg>
attributeValue	<leeg>
foreignOperation.traceId	8a1325a32aef8de4ffba7d7c931eeaec
foreignOperation.operationId	ba7cac7ca0489e42

8. Log tonenVergunningen (log gemeente)

Attribuut	Waarde
operationId	ba7cac7ca0489e42
operationName	tonenVergunningen
parentOperationId	<leeg>
traceId	8a1325a32aef8de4ffba7d7c931eeaec
startTime	2024-07-29 10:17:02.274
endTime	2024-07-29 10:17:02.291
statusCode	OK
resource.name	MijnOmgeving
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	11x2ec2a-0774-3541-9b16-21ba179fcf15
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5

§ 5.2.5 Relatie tussen gegevens (Parkeervergunning - wijzigen)

Om uiteindelijk alle gegevens te kunnen rapporteren, is het van belang dat gegevens op een bepaalde manier aan elkaar gekoppeld zijn. In dit voorbeeld zijn de gegevens op de volgende manier gekoppeld:



§ 5.2.6 Relatie met de standaard Logboek Dataverwerkingen (Parkeervergunning - wijzigen)

De relatie met de doelstellingen die gesteld zijn in de standaard Logboek dataverwerkingen worden, op basis van dit voorbeeld, als volgt concreet gerealiseerd:

- **het wegschrijven van logs van dataverwerkingen:** In dit voorbeeld is het de betrokkene zelf die via een portaal zijn eigen gegevens kan bekijken en wijzigen. Deze acties zijn gegevensverwerkingen en worden gelogd bij zowel de gemeenteapplicatie (gegevens worden getoond aan de betrokkene) als bij de vergunningenapplicatie (verstrekking specifieke informatie aan de gemeenteapplicatie).
- **het aan elkaar relateren van logs van dataverwerkingen:** Er zijn in dit voorbeeld twee applicaties nodig om het totaal aan gevraagde informatie te kunnen tonen aan de betrokkene. Beide applicaties hebben een logboek voor verwerkte gegevens. Om een totaalbeeld van de gelogde gegevens te kunnen construeren, is een relatie tussen de logs nodig. In dit voorbeeld wordt de koppeling gelegd door het `operationId` en `traceId` (gemeentelogboek) te linken aan het `foreignOperationId` en `foreignTraceId` (vergunningenlogboek).
- **het aan elkaar relateren van dataverwerkingen over de grenzen van systemen:** Naast het koppelen van logs van diverse applicaties, wordt ook een koppeling gelegd met het Register van verwerkingsactiviteiten. Dit gebeurt per applicatie op basis van het `ProcessingActivityId` (register) te koppelen aan `dplCoreProcessingActivityId` (logboek). De diverse registers hebben **geen** directe koppeling met elkaar.

§ 5.2.6.1 Standaard Logverwerkingen: paragraaf 3.3.1 Gedrag

1. De applicatie MOET een Trace starten voor iedere Dataverwerking waarvan nog geen Trace bekend is. Bij elke start van een verwerking wordt een `traceId` aangemaakt. Bijvoorbeeld: in het voorbeeld komt er een bericht binnen bij de 'MijnOmgeving' van de gemeente (opvragenVergunningenVraag). Er wordt direct een `traceId` aangemaakt.
2. De applicatie MOET voor iedere Dataverwerking een logregel wegschrijven in een Logboek. Log Sampling is niet toegestaan. Een dataverwerking wordt opgeslagen als deze volledig is afgerond. In het voorbeeld is te zien dat een logregel wordt geschreven op het moment dat de vraag- en het antwoordbericht zijn afgerond.
3. De applicatie MOET bijhouden of een Dataverwerking geslaagd of mislukt is en dit per Dataverwerking als status meegeven aan het Logboek. Bij elke logregel in het voorbeeld staat de `statusCode` vermeld ('OK').
4. Als een Dataverwerking meerdere Betrokkenen heeft dan MOET de applicatie voor iedere betrokkene een aparte logregel wegschrijven. Een logregel kan naar 0 of 1 betrokkenen verwijzen. In het voorbeeld gaat het om één betrokkene (`dplCoreDataSubjectId`), er wordt steeds één logregel aangemaakt.
5. Als een applicatie aangeroepen kan worden vanuit een andere applicatie MOET de applicatie Trace Context metadata accepteren bij een dergelijke aanroepen deze metadata kunnen omzetten naar een `foreign_operation` bericht. Bij een externe verwerking (bijvoorbeeld opvragenVergunningen) geeft de 'MijnOmgeving' de `traceId` en `operationId` mee aan de Vergunningenapplicatie. De vergunningenapplicatie registreert de `traceId` en `operationId` beide als 'foreignOperation'.

§ 5.3 Registratie Verhuizing - Eenvoudig, traditioneel systeem

§ 5.3.1 Situatieschets (Registratie Verhuizing - Eenvoudig)

Deze case beschrijft de binnengemeentelijke verhuizing van een persoon. De beschrijving is functioneel zo eenvoudig mogelijk. De burger komt aan de balie en er is geen sprake van meeverhuizende gezinsleden.

§ 5.3.2 Uitgangspunten (Registratie Verhuizing - Eenvoudig)

- Het beschreven proces is een voorbeeld, het werkelijke proces kan anders verlopen.
- Het proces is een 'happy flow' dit betekent dat validaties en eventuele foutsituaties in dit voorbeeld niet in ogenschouw worden genomen.
- Autorisatieprocessen zijn in dit voorbeeld niet meegenomen.

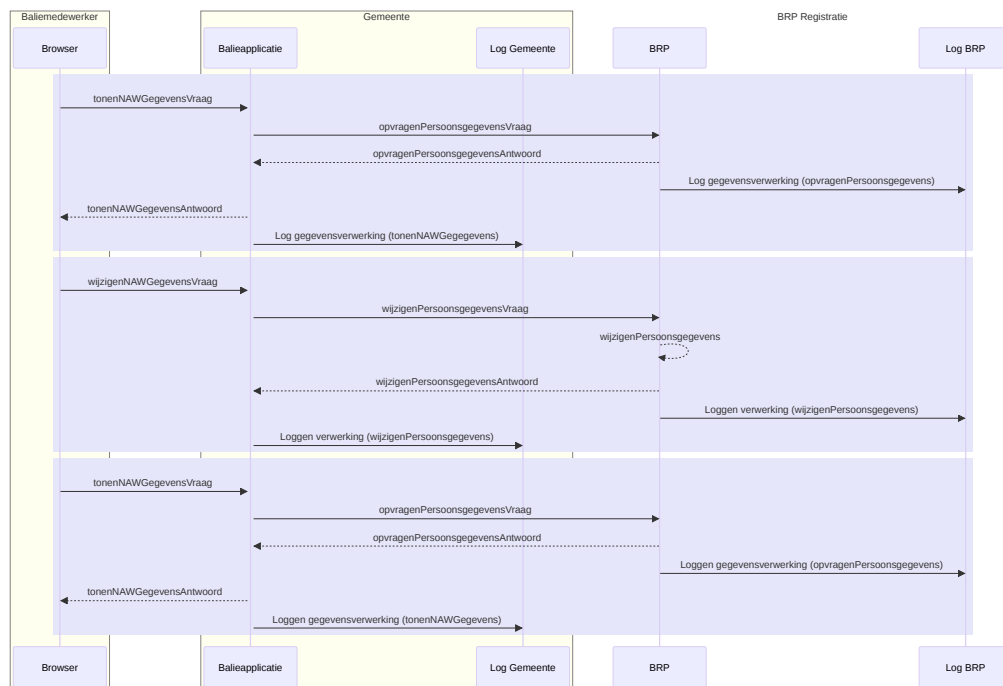
- Een Loggingsregel wordt toegevoegd aan het logboek per **geheel** afgeronde transactie. Er wordt dus **geen** aparte logregel aangemaakt per ontvangen of verstuurd bericht.
- Een aantal gegevens staan nog ter discussie (vanuit juridisch oogpunt). Voor de volledigheid worden een aantal gegevens in dit voorbeeld meegenomen. Het betreft de gegevens:
 - resource/name/version
 - receiver
 - dataSubject

§ 5.3.3 Globaal proces (Registratie Verhuizing - Eenvoudig)

Schematisch ziet dit proces er als volgt uit:

1. De Baliemedewerker voert BSN van de burger in.
2. De Browser vraagt om persoonsgegevens bij de gemeentelijke Balieapplicatie.
3. De gemeentelijke Balieapplicatie vraagt persoonsgegevens bij het BRP-systeem.
4. Het BRP systeem stuurt gevraagde gegevens naar de gemeentelijke Balieapplicatie en logt de aanvraag.
5. De gemeentelijke Balieapplicatie stuurt de gegevens naar de Browser en worden getoond aan de Baliemedewerker. De aanvraag wordt gelogd door de Balieapplicatie.
6. De Baliemedewerker voert de wijziging in en de Browser verstuurt de gegevens naar de gemeentelijke Balieapplicatie.
7. De gemeentelijke Balieapplicatie verstuurt de gegevens naar het BRP-systeem.
8. Het BRP-systeem verwerkt de wijziging, stuurt bevestiging terug naar de gemeentelijke Balieapplicatie en logt de verwerkingsactie.
9. De Browser vraagt de actuele persoonsgegevens op de gemeentelijke Balieapplicatie.
10. De gemeentelijke Balieapplicatie vraagt de persoonsgegevens op bij het BRP-systeem.
11. Het BRP-systeem stuurt de persoonsgegevens naar de gemeentelijke Balieapplicatie en logt de aanvraag.
12. De gemeentelijke Balieapplicatie stuurt de persoonsgegevens naar de Browser en logt de aanvraag.

Schematisch ziet dit proces er als volgt uit:



§ 5.3.4 Logging van gegevens (Registratie Verhuizing - Eenvoudig)

De volgende gegevens worden gelogd in de diverse logmomenten:

1. Log opvragenPersoonsgegevens (log BRP):

Attribuut	Waarde
operationId	7a22eb38-bca6-463f-9955-54ab040287cb
operationName	opvragenPersoonsgegevens
parentOperationId	<leeg>
traceId	c6adf4df949d03c662b53e95debd411
startTime	2024-07-29 08:16:49.000
endTime	2024-07-29 08:16:49.000
statusCode	OK
resource.name	BRP
resource.version	2.0
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	12f2ec2a-0cc4-3541-9ae6-219a178fcfe4
attributeKey	<leeg>
attributeValue	<leeg>
foreignOperation.traceId	bc9126aaae813fd491ee10bf870db292
foreignOperation.operationId	b2e339a595246e01

2. Log tonenNAWGegevens (log gemeente)

Attribuut	Waarde
operationId	b2e339a595246e01
operationName	tonenNAWGegevens
parentOperationId	<leeg>
traceId	bc9126aaae813fd491ee10bf870db292
startTime	2024-07-29 10:16:49.690
endTime	2024-07-29 10:16:49.723
statusCode	OK
resource.name	Balieapp
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	11x2ec2a-0774-3541-9b16-21ba179fcf15
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5

3. Log wijzigPersoonsgegevens (log BRP)

Attribuut	Waarde
operationId	433f276975204ccf
operationName	wijzigPersoonsgegevens
parentOperationId	<leeg>
traceId	8ccfd3c567c51d68937c263e00a352be
startTime	2024-07-29 08:17:02
endTime	2024-07-29 08:17:02
statusCode	OK
resource.name	BRP
resource.version	2.0
receiver	<leeg>

Attribuut	Waarde
attributeKey	dplCoreProcessingActivityId
attributeValue	8c714e4a-a538-36f7-8b1f-37a6884cc68c
attributeKey	<leeg>
attributeValue	<leeg>
foreignOperation.traceId	f176a58de7fe249ea37ed4f5979da02b
foreignOperation.operationId	414514cf1d40d6b2

4. Log wijzigenPersoonsgegevens (log gemeente)

Attribuut	Waarde
operationId	414514cf1d40d6b2
operationName	wijzigenPersoonsgegevens
parentOperationId	<leeg>
traceId	f176a58de7fe249ea37ed4f5979da02b
startTime	2024-07-29 08:17:02.000
endTime	2024-07-29 08:17:02.000
statusCode	OK
resource.name	Balieapp
resource.version	1.0.5
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	19u2dd2a-0cb7-3541-9ae6-217a178fc9e6
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5
foreignOperation.traceId	<leeg>
foreignOperation.operationId	<leeg>

5. Log opvragenPersoonsgegevens (log BRP)

Attribuut	Waarde
operationId	7a95b6989d2b28c7
operationName	opvragenPersoonsgegevens
parentOperationId	<leeg>
traceId	f176a58de7fe249ea37ed4f5979da02b
startTime	2024-07-29 08:17:02.000
endTime	2024-07-29 08:17:02.000
statusCode	OK
resource.name	BRP
resource.version	2.0
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	0b1ff20a-3ecb-34bf-8cf5-e4cbacb046ab
attributeKey	dplCoreDataSubjectId
attributeValue	<leeg>
foreignOperation.traceId	c0a7a38d56f3f16a2163ca0071d3779a
foreignOperation.operationId	df524ee2a3fd5ddf

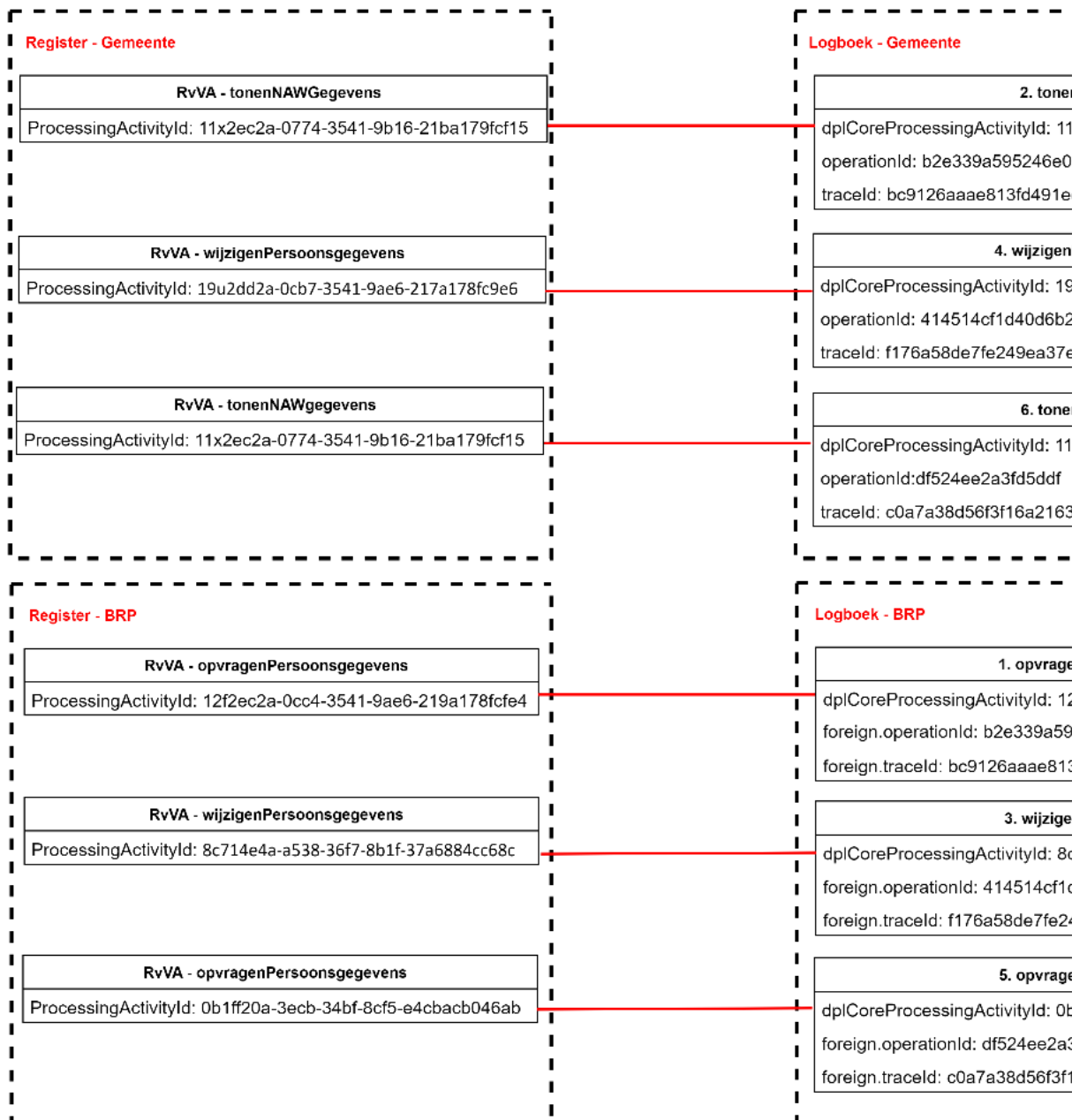
6. Log tonenNAWGegevens (log gemeente)

Attribuut	Waarde
operationId	df524ee2a3fd5ddf

Attribuut	Waarde
operationName	tonenNAWGegevens
parentOperationId	<leeg>
traceId	c0a7a38d56f3f16a2163ca0071d3779a
startTime	2024-07-29 10:17:02.010
endTime	2024-07-29 10:17:02.039
statusCode	OK
resource.name	Balieapp
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	12c21c2a-0875-3543-9b16-21ja179fcf16
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5
foreignOperation.traceId	<leeg>
foreignOperation.operationId	<leeg>

§ 5.3.5 Relatie tussen gegevens (Registratie Verhuizing - Eenvoudig)

Om uiteindelijk alle gegevens te kunnen rapporteren, is het van belang dat gegevens op een bepaalde manier aan elkaar gekoppeld zijn. In dit voorbeeld zijn de gegevens op de volgende manier gekoppeld:



§ 5.3.6 Relatie met de standaard Logboek dataverwerkingen (Registratie Verhuizing - Eenvoudig)

De relatie met de doelstellingen die gesteld zijn in de standaard Logboek dataverwerkingen worden, op basis van dit voorbeeld, als volgt concreet gerealiseerd:

- **het wegschrijven van logs van dataverwerkingen:** In dit voorbeeld is het de Baliemedewerker die via een Balieapplicatie de gegevens van een Betrokkene kan bekijken en wijzigen. Deze acties zijn gegevensverwerkingen en worden gelogd bij zowel de Balieapplicatie als bij het BRP-systeem.
- **het aan elkaar relateren van logs van dataverwerkingen:** Er zijn in dit voorbeeld twee applicaties nodig om het totaal aan gevraagde informatie te kunnen tonen aan de betrokkene. Beide applicaties hebben een logboek voor verwerkte gegevens. Om een totaalbeeld van de gelogde gegevens te kunnen construeren, is een relatie tussen de logs nodig. In dit voorbeeld wordt de koppeling gelegd door het operationId en traceId (gemeentelogboek) te linken aan het foreignOperationId en foreignTraceId (BRP-logboek).
- **het aan elkaar relateren van dataverwerkingen over de grenzen van systemen:** Naast het koppelen van logs van diverse applicaties, wordt ook een koppeling gelegd met het Register van verwerkingsactiviteiten. Dit gebeurt per applicatie op basis van het ProcessingActivityId (register) te koppelen aan dplCoreProcessingActivityId (logboek). De diverse registers hebben **geen** directe koppeling met elkaar.

Standaard Logverwerkingen: **paragraaf 3.3.1 Gedrag**

1. De applicatie MOET een Trace starten voor iedere Dataverwerking waarvan nog geen Trace bekend is. Bij elke start van een verwerking wordt een traceId aangemaakt. Bijvoorbeeld: in het voorbeeld komt er een bericht binnen bij de Balieapplicatie van de gemeente (tonenNAWGegevens). Er wordt direct een traceId aangemaakt.
2. De applicatie MOET voor iedere Dataverwerking een logregel wegschrijven in een Logboek. Log Sampling is niet toegestaan. Een dataverwerking wordt opgeslagen als deze volledig is afgerond. In het voorbeeld is te zien dat een logregel wordt geschreven op het moment dat de vraag- en het antwoordbericht zijn afgerond.
3. De applicatie MOET bijhouden of een Dataverwerking geslaagd of mislukt is en dit per Dataverwerking als status meegeven aan het Logboek. Bij elke logregel in het voorbeeld staat de statusCode vermeld ('OK').
4. Als een Dataverwerking meerdere Betrokkenen heeft dan MOET de applicatie voor iedere betrokkene een aparte logregel wegschrijven. Een logregel kan naar 0 of 1 betrokkenen verwijzen. In het voorbeeld gaat het om één betrokkene (dplCoreDataSubjectId), er wordt steeds één logregel aangemaakt.
5. Als een applicatie aangeroepen kan worden vanuit een andere applicatie MOET de applicatie Trace Context metadata accepteren bij een dergelijke aanroepen deze metadata kunnen omzetten naar een foreign_operation bericht. Bij een externe verwerking (bijvoorbeeld opvragenPersoonsgegevens) geeft de Balieapplicatie de traceId en OperationId mee aan het BRP-systeem. Het BRP-systeem registreert de traceId en operationId beide als 'foreignOperation'.

§ 5.4 Registratie verhuizing – Opvragen meerdere BSN's

§ 5.4.1 Situatieschets (Registratie verhuizing)

Deze case beschrijft de samenstelling van een huishouding op een bepaald adres. De beschrijving is functioneel zo eenvoudig mogelijk, een burger komt aan de balie en er is geen sprake van wijzigingen in de huishouding.

§ 5.4.2 Uitgangspunten (Registratie verhuizing)

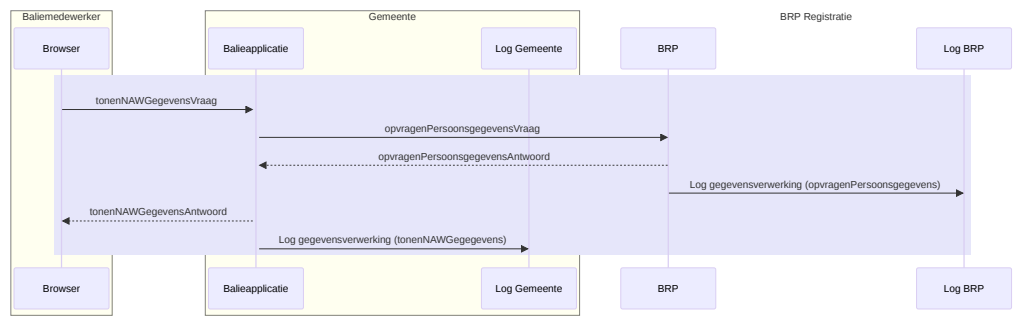
- Het beschreven proces is een voorbeeld, het werkelijke proces kan anders verlopen.
- Het proces is een 'happy flow' dit betekent dat validaties en eventuele foutsituaties in dit voorbeeld niet in ogenschouw worden genomen.
- Autorisatieprocessen zijn in dit voorbeeld niet meegenomen.
- Een Loggingsregel wordt toegevoegd aan het logboek per **geheel** afgeronde transactie. Er wordt dus **geen** aparte logregel aangemaakt per ontvangen of verstuurd bericht.
- Een aantal gegevens staan nog ter discussie (vanuit juridisch oogpunt). Voor de volledigheid worden een aantal gegevens in dit voorbeeld meegenomen. Het betreft de gegevens:
 - resource/name/version
 - receiver
 - dataSubject
- Het is optioneel om het BSN (dplCoreDataSubjectId) te versleutelen ten behoeve van extra gegevensbeveiliging. In dit voorbeeld wordt versleuteling van gegevens toegepast.

§ 5.4.3 Globaal proces (Registratie verhuizing)

Schematisch ziet dit proces er als volgt uit:

1. De Baliemedewerker voert adres van de burger in.
2. De Browser vraagt om persoonsgegevens bij de gemeentelijke Balieapplicatie.
3. De gemeentelijke Balieapplicatie vraagt persoonsgegevens bij het BRP-systeem.
4. Het BRP systeem stuurt gevraagde gegevens naar de gemeentelijke Balieapplicatie en logt de aanvraag.
5. De gemeentelijke Balieapplicatie stuurt de gegevens naar de Browser en worden getoond aan de Baliemedewerker. De aanvraag wordt gelogd door de Balieapplicatie.

Schematisch ziet dit proces er als volgt uit:



§ 5.4.4 Logging van gegevens (Registratie verhuizing)

De volgende gegevens worden gelogd in de diverse logmomenten:

1. Log opvragenPersoonsgegevens (log BRP) persoon 1:

Attribuut	Waarde
operationId	7a22eb38-bca6-463f-9955-54ab040287cb
operationName	opvragenPersoonsgegevens
parentOperationId	<leeg>
traceId	c6adf4df949d03c662b53e95debd411
startTime	2024-07-29 08:16:49.000
endTime	2024-07-29 08:16:49.000
statusCode	OK
resource.name	BRP
resource.version	2.0
receiver	<leeg>
attributeKey	dplCoreProcessingActivityId
attributeValue	12f2ec2a-0cc4-3541-9ae6-219a178fcfe4
foreignOperation.traceId	bc9126aaae813fd491ee10bf870db292
foreignOperation.operationId	b2e339a595246e01
<u>BSN 1</u>	<leeg>
attributeKey	dplCoreDataSubjectId
attributeValue	ddj2ey299-0cf4-3541-9ar6-21ia178fcfrr
operationId	r2e3229059BG246e01
parentOperationId	7a22eb38-bca6-463f-9955-54ab040287cb

2. Log opvragenPersoonsgegevens (log BRP) persoon 2:

Attribuut	Waarde
operationId	7a22eb38-bca6-463f-9955-54ab040287cb
operationName	opvragenPersoonsgegevens
parentOperationId	<leeg>
traceId	c6adf4df949d03c662b53e95debd411
startTime	2024-07-29 08:16:49.000
endTime	2024-07-29 08:16:49.000
statusCode	OK
resource.name	BRP
resource.version	2.0
receiver	<leeg>

Attribuut	Waarde
attributeKey	dplCoreProcessingActivityId
attributeValue	12f2ec2a-0cc4-3541-9ae6-219a178fcfe4
foreignOperation.traceId	bc9126aaae813fd491ee10bf870db292
foreignOperation.operationId	b2e339a595246e01
<u>BSN 2</u>	<leeg>
attributeKey	dplCoreDataSubjectId
attributeValue	f4j2ey299-3er4-3aa41-9ar6-21ia178fc3tyy
operationId	9as5y3t-3ca7-463f-wwt9a5-54ab0402rft
parentOperationId	7a22eb38-bca6-463f-9955-54ab040287cb

3. Log tonenNAWGegevens (log gemeente) persoon 1:

Attribuut	Waarde
operationId	b2e339a595246e01
operationName	tonenNAWGegevens
parentOperationId	<leeg>
traceId	bc9126aaae813fd491ee10bf870db292
startTime	2024-07-29 10:16:49.690
endTime	2024-07-29 10:16:49.723
statusCode	OK
resource.name	Balieapp
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	11x2ec2a-0774-3541-9b16-21ba179fcf15
<u>BSN 1</u>	<leeg>
attributeKey	dplCoreDataSubjectId
attributeValue	13j2ec27-0cc4-3541-9av6-219a178fcfe5
operationId	42f33gfa595246ert
parentOperationId	b2e339a595246e01

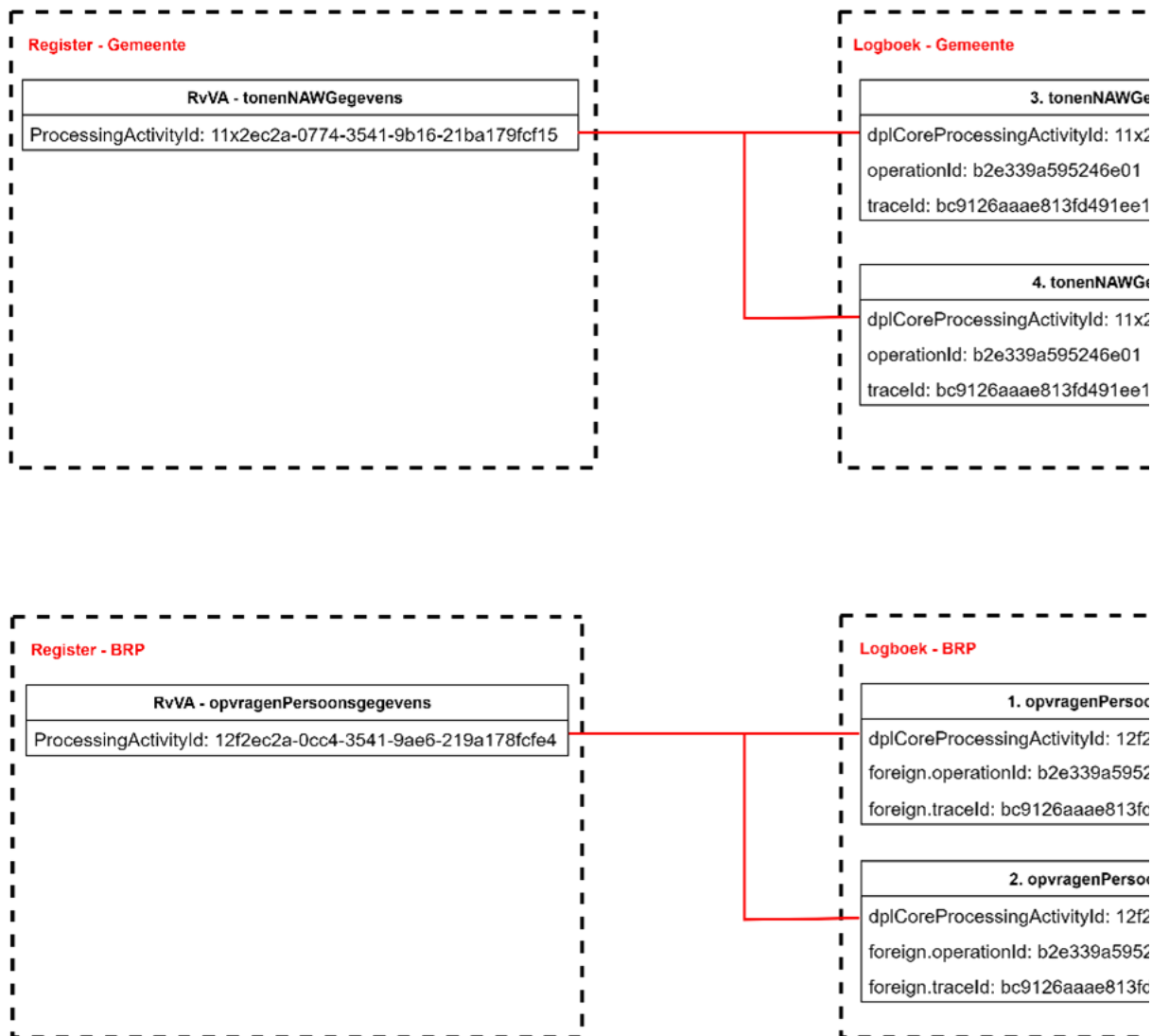
4. Log tonenNAWGegevens (log gemeente) persoon 2:

Attribuut	Waarde
operationId	b2e339a595246e01
operationName	tonenNAWGegevens
parentOperationId	<leeg>
traceId	bc9126aaae813fd491ee10bf870db292
startTime	2024-07-29 10:16:49.690
endTime	2024-07-29 10:16:49.723
statusCode	OK
resource.name	Balieapp
resource.version	1.0.5
receiver	27fdey98605etc48
attributeKey	dplCoreProcessingActivityId
attributeValue	11x2ec2a-0774-3541-9b16-21ba179fcf15
<u>BSN 2</u>	<leeg>
attributeKey	dplCoreDataSubjectId
attributeValue	342ec27-aa41-dav6-219a178f5ty6
operationId	aef53rfa59e240ert

Attribuut	Waarde
parentOperationId	b2e339a595246e01

§ 5.4.5 Relatie tussen gegevens (Registratie verhuizing)

Om uiteindelijk alle gegevens te kunnen rapporteren, is het van belang dat gegevens op een bepaalde manier aan elkaar gekoppeld zijn. In dit voorbeeld zijn de gegevens op de volgende manier gekoppeld:



§ 5.4.6 Relatie met de standaard Logboek dataverwerkingen (Registratie verhuizing)

De relatie met de doelstellingen die gesteld zijn in de standaard Logboek dataverwerkingen worden, op basis van dit voorbeeld, als volgt concreet gerealiseerd:

- **het wegschrijven van logs van dataverwerkingen:** In dit voorbeeld is het de Baliemedewerker die via een Balieapplicatie de gegevens van een Betrokkene kan bekijken. Deze acties zijn dataverwerkingen en worden gelogd bij zowel de Balieapplicatie als bij het BRP-systeem.
- **het aan elkaar relateren van logs van dataverwerkingen:** Er zijn in dit voorbeeld twee applicaties nodig om het totaal aan gevraagde informatie te kunnen tonen aan de betrokkene. Beide applicaties hebben een logboek voor verwerkte gegevens. Om een totaalbeeld van de gelogde gegevens te kunnen construeren, is een relatie tussen de logs nodig. In dit voorbeeld wordt de koppeling gelegd door het operationId en traceId (gemeentelogboek) te linken aan het foreignOperationId en foreignTraceId (BRP-logboek). De aanroep van de gemeente-applicatie naar het BRP betreft één opvraag op basis van één adres, één operationId en één traceId. Het resultaat is meervoudig en moeten naar dezelfde

operationId en traceId leiden van de gemeente-applicatie. Het onderscheid zit in de verschillende BSN's van de personen die via een parentOperationId gekoppeld zijn.

- **het aan elkaar relateren van dataverwerkingen over de grenzen van systemen:** Naast het koppelen van logs van diverse applicaties, wordt ook een koppeling gelegd met het Register van verwerkingsactiviteiten. Dit gebeurt per applicatie op basis van het ProcessingActivityId (register) te koppelen aan dplCoreProcessingActivityId (logboek). De diverse registers hebben **geen** directe koppeling met elkaar.

Standaard Logverwerkingen: paragraaf 3.3.1 Gedrag

1. *De applicatie MOET een Trace starten voor iedere Dataverwerking waarvan nog geen Trace bekend is.* Bij elke start van een verwerking wordt een traceId aangemaakt. Bijvoorbeeld: in het voorbeeld komt er een bericht binnen bij de Balieapplicatie van de gemeente (tonenNAWGgegevens). Er wordt direct een traceId aangemaakt.
2. *De applicatie MOET voor iedere Dataverwerking een logregel wegschrijven in een Logboek. Log Sampling is niet toegestaan.* Een dataverwerking wordt opgeslagen als deze volledig is afgerond. In het voorbeeld is te zien dat logregels worden geschreven op het moment dat de vraag- en het antwoordbericht zijn afgerond.
3. *De applicatie MOET bijhouden of een Dataverwerking geslaagd of mislukt is en dit per Dataverwerking als status meegeven aan het Logboek.* Bij elke logregel in het voorbeeld staat de statusCode vermeld ('OK').
4. *Als een Dataverwerking meerdere Betrokkenen heeft dan MOET de applicatie voor iedere betrokkene een aparte logregel wegschrijven. Een logregel kan naar 0 of 1 betrokkenen verwijzen.* In het voorbeeld gaat het om twee betrokkenen (dplCoreDataSubjectId), er wordt één logregel aangemaakt per BSN.
5. *Als een applicatie aangeroepen kan worden vanuit een andere applicatie MOET de applicatie Trace Context metadata accepteren bij een dergelijke aanroepen deze metadata kunnen omzetten naar een foreign_operation bericht.* Bij een externe verwerking (bijvoorbeeld opvragenPersoonsgegevens) geeft de Balieapplicatie de traceId en OperationId mee aan het BRP-systeem. Het BRP-systeem registreert de traceId en operationId beide als 'foreignOperation'.

§ 5.5 Voorbeeldapplicaties

§ 5.5.1 Register van de verwerkingsactiviteiten (RvVA)

Dit project biedt een overzicht van gegevensverwerkingen binnen de overheid, waaronder het Register van de verwerkingsactiviteiten (RvVA). Dit register documenteert hoe gegevens worden verwerkt, waarschijnlijk ter ondersteuning van transparantie en naleving van de Algemene Verordening Gegevensbescherming (AVG).

Je kunt de voorbeeldapplicatie van het logboek en de specifieke RvVA-sectie hier bekijken:

- gitlab.com/digilab.overheid.nl/ecosystem/logboek-dataverwerkingen/rva
- gitlab.com/digilab.overheid.nl/ecosystem/logboek-dataverwerkingen

§ 6. Conformiteit

Naast onderdelen die als niet normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet normatief. Verder is alles in dit document normatief.

Het trefwoord *MOET* in dit document moet worden geïnterpreteerd als in [BCP 14 \[RFC2119\]](#) [\[RFC8174\]](#) als, en alleen als deze in hoofdletters zijn weergegeven, zoals hier getoond.

§ A. Index

§ A.1 Begrippen gedefinieerd door deze specificatie

§ A.2 Begrippen gedefinieerd door verwijzing

§ B. Referenties

§ B.1 Normatieve referenties

[RFC2119]

Key words for use in RFCs to Indicate Requirement Levels, S. Bradner. IETF. March 1997. Best Current Practice. URL: <https://www.rfc-editor.org/rfc/rfc2119>

[RFC8174]

Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words, B. Leiba. IETF. May 2017. Best Current Practice. URL: <https://www.rfc-editor.org/rfc/rfc8174>

§ B.2 Informatieve referenties

[ADR]

API Design Rules (Nederlandse API Strategie IIa). Jasper Roes; Joost Farla. Logius. Juli 2020. URL: <https://gitdocumentatie.logius.nl/publicatie/api/adr/>