Logius Praktijkrichtlijn - Werkversie

Juridisch Beleidskader - Logboek Dataverwerking

Logius Praktijkrichtlijn
Werkversie 09 december 2024

Deze versie:
https://logius-standaarden.github.io/logboek-dataverwerkingen/

Laatst gepubliceerde versie:
https://gitdocumentatie.logius.nl/publicatie/api/logboek_juridisch/

Laatste werkversie:
https://logius-standaarden.github.io/logboek-dataverwerkingen/

Redacteurs:
Vedran Bilanovic (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Eelco Hotting (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Jeroen Mulder (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Pieter Teekens (Ministerie van Binnelandse Zaken en Koninkrijksrelaties)
Nil Barua (Logius)
Martin van der Plas (Logius)

Auteurs:
Wouter Diephuis (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Mirian van Ansem (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Doe mee:
GitHub Logius-standaarden/logboek-dataverwerkingen
Dien een melding in
Revisiehistorie
Pull requests

Dit document is ook beschikbaar in dit niet-normatieve formaat: pdf

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.

> bron: Digitale overheid.nl

§ 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
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

1. Inleiding

Dit Juridisch beleidskader biedt het overzicht van de (juridische) verantwoording die de overheid over haar handelen moet afleggen en is opgesteld ten behoeve van de Logboek Dataverwerkingen standaard. Er wordt toegelicht hoe de standaard vanuit het denken over verantwoording is opgebouwd. Het doel daarvan is dat het Logboek Dataverwerkingen een basis biedt om te zorgen dat de overheid precies de gegevens 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 gegevens zodanig loggen dat zij zich niet alleen over een eigen handelen kunnen verantwoorden, maar ook over hun gezamenlijk handelen als “de overheid”.

1.1 Scope van dit verantwoordingsdocument

Dit document beschrijft de wijze waarop de overheid zich moet verantwoorden in brede zin en de informatie die daarvoor beschikbaar moet zijn. De standaard beoogt – initieel – niet alle aspecten te adresseren, maar biedt wel de basis om te zorgen dat **eenduidigheid en relateerbaarheid** van (log)informatie geborgd is. Deze aspecten bepalen de scope van dit document.

Dit document en - de standaard – staan daarin (bewust) neutraal ten opzichte de termijnen die gelden voor het bewaren van logging. Deze termijnen kunnen en zullen verschillen afhankelijk van taak en doel waarvoor zij beschikbaar moeten blijven. Dit document gaat hierop daarom niet in. De standaard biedt wel een manier om hiermee om te gaan (profiel).

Dit geldt bijvoorbeeld ook voor het bewaren van gegevens in het kader van de archiefwet. De logging die voorhanden is kan daarvoor gebruikt worden, maar dit document heeft geen oordeel over de vraag óf gegevens in het kader van de archiefwet bewaard dienen te blijven, noch voor de termijn daarvan.

Omdat het document neutraal staat ten opzichte van de doelen waarvoor de logging wordt benut, zijn ook eventuele maatregelen als gevolg van specifiek gebruik, bijvoorbeeld gelimiteerde toegang bij monitoring / soc of extra beveiligingsmaatregelen op de logging buiten de scope.

In de het laatste hoofdstuk van dit document is het beleid voor de standaard Logboek Dataverwerkingen opgenomen in de vorm van ‘leidende principes’. Hiermee kunnen gebruikers binnen de context van hun specifieke situatie de bedoeling van de standaard interpreteren en toepassen. Dit beleid sluit aan bij dit verantwoordingsdocument en bouwt daarop voort.

1.2 De overheid moet zich verantwoorden over de uitvoering van haar taken

De overheid staat bij alles wat zij doet in dienst van de maatschappij en legt daarover verantwoording af. Publieke verantwoording is onderdeel van goed openbaar bestuur.

De overheid en de daarmee verbonden organen leggen publieke verantwoording af over:

- de rechtmatigheid van de inning, het beheer en de besteding van publieke middelen,
- de effectiviteit en doelmatigheid van beleid en de behartiging van publieke taken, waaronder de besluiten die zij neemt,
- de integriteit van de organisatie en haar medewerkers, en het ‘in control’ zijn.

Er is niet op één centrale plek in de wet een verantwoordingsplicht voor overheden opgenomen. Verantwoordingsplichten zijn opgenomen in een breed scala van wetten en beginselen, waaruit volgt dat verantwoorden in zijn algemeenheid belangrijk is.

1.2.1 Algemene verplichtingen tot verantwoording

Een belangrijke wet in dit verband die generieke verantwoording verlangt is de Comptabiliteitswet, op basis waarvan de overheid zich dient te verantwoorden over de doelmatige inzet van toegekende financiële middelen.

Ook van belang is de Algemene wet bestuursrecht (hierna: Awb), waarin onder meer is vastgelegd dat overheden bij besluitvorming zorgvuldig te werk moeten gaan en hun (individuele) handelingen deugdelijk moeten motiveren.

Tevens dient de overheid te verantwoorden dat de informatie waarmee zij werkt om haar taken te vervullen, goed is beveiligd. Regels over informatiebeveiliging worden gesteld in de Baseline Informatiebeveiliging Overheid en op basis van de implementatie van de NIS2-richtlijn. Tevens gelden de regels van de AI -en datagovernance verorderingen.

Omdat de overheid bij de invulling van haar taken persoonsgegevens verwerkt, geldt dat zij de zorgvuldige verwerking van persoonsgegevens op basis van de Algemene Verordening Gegevensbescherming (hierna: AVG) dient te verantwoorden.

Deze verplichtingen richten zich op de bedrijfsvoering van de individuele overheden (want daar wordt de informatie verwerkt) en de wijze waarop zij met elkaar samenwerken in het publieke belang.

1.2.2 Specifieke verantwoording

Naast de bovengenoemde verantwoordingsverplichtingen die voor de bedrijfsvoering van elke overheidsorganisaties gelden, bestaan er domeinspecifieke verantwoordingsverplichtingen in domeinwetgeving (bijvoorbeeld zorg), of verantwoordingsverplichtingen op basis van specifieke problematiek (bijvoorbeeld mededingingsvraagstukken).

1.3 De overheid verwerkt voor haar taken informatie

Om taken te kunnen vervullen is het voor overheidsorganisaties noodzakelijk om informatie te verwerken. Informatie en de wijze waarop deze wordt gebruikt ligt daarmee aan de basis voor een goed openbaar bestuur. Het vormt een van de pijlers van de democratische rechtstaat en geeft mede vorm aan de relatie met burgers.

Daarnaast is een goede informatiehuishouding van belang om burgers en bedrijven van betrouwbare informatie te kunnen voorzien en om als overheid efficiënt en effectief te kunnen werken.

1.4 De overheid moet zich kunnen verantwoorden over de wijze waarop informatie wordt verwerkt

1.4.1 Informatie als middel om te verantwoorden

Uit het voorgaande volgt dat, wil een overheidsorganisatie zich adequaat kunnen verantwoorden over haar taken, de informatiehuishouding op orde moet zijn en dat inzichtelijk moet zijn welke informatie zij bij de invulling van haar taken heeft gebruikt, hoe deze informatie is vergaard en hoe deze informatie bij de beslissingen is (af)gewogen.

Dit geldt op alle niveaus van informatieverwerking. Het dient inzichtelijk te zijn hoe bijvoorbeeld beleidsvorming – vaak op hoofdlijnen – tot stand is gekomen. Ook is het bij individuele besluiten die gevolgen hebben voor burgers belangrijk dat voor de burger inzichtelijk is welke gegevens een

overheidsorganisatie bij het besluit heeft gebruikt, hoe deze gegevens zijn gebruikt en bij welke overheidsorganisatie op welk moment deze zijn verzameld.

§ 1.4.2 Verantwoording over de rechtmatige verwerking van informatie

Wettelijk is geregeld welke informatie – zeker daar waar het persoonsgegevens betreft – overheden voor de uitvoering van hun taken mogen verwerken. Welke informatie dat is, zal per overheidsorganisatie verschillen. Immers, hun taken verschillen, en de informatie om deze taken uit te voeren ook.

Iedere overheidsorganisatie dient, op basis van de verwerkingsgrondslagen die zijn toegekend en toegespitst op de vervulling van de opgedragen taak, te verantwoorden dat informatie in overeenstemming met deze grondslagen is verwerkt. Ook dient de overheid aan te tonen dat voldaan is aan verplichtingen die gelden, bijvoorbeeld ten aanzien van de verwerking of beveiliging van persoonsgegevens en de vertrouwelijkheid van bedrijfsinformatie.

§ 1.5 Belang van goede verantwoording en verbetering daarvan

Digitalisering maakt een efficiëntere en effectiever werkende overheid mogelijk. Dat komt door de toenemende mogelijkheden om gegevens te verwerken en onderling als overheidsorganisaties samen te werken. Dienstverlening aan burgers en bedrijven kan sneller en meer op maat plaatsvinden.

Aan deze mogelijkheden zit ook een andere kant, die vergt dat de overheid goed inzicht houdt – ook over organisaties heen - in hoe deze informatieverwerking en uitwisseling heeft plaatsgevonden. Dat is nodig om de steeds verder toenemende informatie-uitwisseling te kunnen verantwoorden. Maar ook om – op het moment dat zich in deze dienstverlening problemen voordoen – goed in staat te zijn om deze op te lossen. Want problemen in dienstverlening kunnen door automatisering in korte tijd ontstaan en omvangrijk worden.

Een voorbeeld daarvan is de situatie rond de toeslagenproblematiek. Nadat deze problematiek is ontdekt vergt het vermoedelijk nog jaren om de gevolgen hiervan te herstellen, omdat de puzzel in het overheidshandelen niet eenduidig gelegd kan worden.

Daarnaast moeten bijvoorbeeld (individuele) burgers die slachtoffer worden van fraude of misbruik van hun gegevens beter geholpen kunnen worden. Immers, problemen kunnen zeer snel uitwaaieren over verschillende overheidsorganisaties. Daarbij past dat ook snel kan worden gereageerd, dat gereconstrueerd kan worden wat er is gebeurd en dat de burgers snel en effectief geholpen kunnen worden.

1.6 Tussenconclusie

De overheid moet zich verantwoorden over de aan haar toegekende taken. Dat geldt niet alleen per overheidsorganisatie, maar ook voor “de overheid” als geheel.

Voor de uitvoering van haar taken verwerkt de overheid informatie. De wijze waarop informatie wordt verwerkt en waarop die verwerking wordt vastgelegd, speelt daarom een belangrijke rol bij de verantwoording door overheden. Daarnaast speelt een goede vastlegging van gegevens een belangrijke rol bij het oplossen van problemen als deze zich voordoen als gevolg van informatie-uitwisseling.

Dit betekent dat de wijze waarop de verslaglegging gebeurt, bij de benodigde verantwoording moet aansluiten. De verantwoording is daarmee kaderend.

2. Verschillende overheidsorganisaties en eenduidige verantwoording

2.1 Inrichting van de overheid: divers en verschillend

2.1.1 Verschillen in verantwoordelijkheden, taken

Overheidsorganisaties zijn er in alle soorten en maten. Zo verschilt de Belastingdienst van DUO of de RDW, en verschillen dergelijke organisaties weer van gemeenten.

Dat komt omdat overheidsorganisaties verschillende taken en verantwoordelijkheden toebedeeld hebben gekregen. Er zijn wel groepen organisaties, zoals gemeenten, die vanwege de vergelijkbare taakuitoefening en organisatie-inrichting veel overeenkomstige kenmerken zullen hebben. Echter, overheidsbreed zullen er verschillen zijn.

2.1.2 Verschillende taken en verantwoordingsplichten

Hoe een overheidsorganisatie is georganiseerd en zich moet verantwoorden, hangt af van de opgedragen wettelijke taken die de organisatie heeft gekregen en vaak ook van de bestuurslaag waarbinnen de organisatie is gepositioneerd (Rijks-, provinciaal, gemeentelijk of waterschapsniveau).

Bij wet is nauwgezet vastgelegd wat hun verantwoordelijkheid is, welke taken daarvoor dienen te worden uitgevoerd, en meestal ook welke (persoons)gegevens daarvoor gebruikt mogen worden. Deze kadering bepaalt de wijze waarop overheden zich organiseren en hun processen vormgeven. En, in het verlengde daarvan, de processen waarover zij zich moeten verantwoorden.

2.1.3 Verschillende informatieverwerkingen

De verschillende verantwoordelijkheden en taken leiden tot verschillende soorten informatieverwerkingen. Welke (persoons)gegevens mogen worden verwerkt voor de realisatie van een taak, wordt bij wet vastgelegd. Immers, DUO heeft voor de verwezenlijking van de taken andere gegevens nodig dan bijvoorbeeld UWV. Welke dat zijn en waarvoor informatie mag worden gebruikt is nauwgezet vastgelegd in wet- en regelgeving. Overigens zal er voor wat betreft de informatieverwerking ook overlap zijn en zullen organisaties ook informatie van elkaar gebruiken (gegevensuitwisseling/data bij de bron).

2.2 Eenduidige verantwoording

Om het mogelijk te maken dat “overheidsbreed” verantwoording kan worden afgelegd over de uitvoering van publieke taken en de onderlinge samenwerking die overheidsorganisaties daarin hebben, is het nodig dat de informatieverwerking die daarvoor plaatsvindt op een eenduidige manier wordt vastgelegd. Dat vergt dat tussen overheidsorganisaties wordt afgesproken / geregeld welke informatie wordt vastgelegd en ook wat onder bepaalde informatie wordt verstaan.

2.2.1 Verantwoordingsplicht

Overheden zullen zich in eerste instantie over de uitvoering van hun eigen taken moeten verantwoorden. Dat betekent dat zij moeten kunnen aantonen welke (geautomatiseerde) activiteiten zij hebben verricht, en dat ook hebben vastgelegd. Dat gaat ook over de vraag hoe concrete beslissingen zijn genomen. Het gaat zowel over welke informatie is gebruikt, hoe deze informatie is gebruikt, en tot welke beslissingen of acties dat heeft geleid.

2.3 Tussenconclusie

Overheden hebben verschillende taken en verschillende bestuurlijke inrichtingen. Voor de taken moet verschillende informatie worden verwerkt en kunnen verschillende

verantwoordingsverplichtingen gelden.

Dat maakt dat organisaties hun processen verschillend “op maat” zullen inrichten. Het resultaat is dat overheidsorganisaties in alle soorten en maten bestaan.

Bij het streven om eenduidigheid in de verslaglegging te realiseren zal hiermee rekening worden gehouden. Dat zal betekenen dat afspraken op conceptueel niveau zullen moeten zijn, en niet context- of taakafhankelijk moeten worden ingevuld.

§ 3. Logging als verantwoordingsinstrument

§ 3.1 Kaders voor logging per organisatie

Om zich te kunnen verantwoorden zal een organisatie inzichtelijk moeten kunnen maken dat zij de taken die zij heeft, heeft uitgevoerd in overeenstemming met de voor de betreffende organisatie geldende kaders. Er zal gereproduceerd moeten kunnen worden welk besluit op een bepaald moment is genomen, welke informatie daarvoor is gebruikt, en of deze informatie (waaronder persoonsgegevens) is gebruikt op een wijze die voldoet aan de daarvoor gestelde kaders.

Dit is noodzakelijk voor (interne) verantwoording aan bijvoorbeeld toezichthouders, en om richting burgers en bedrijven te kunnen aantonen dat besluiten zorgvuldig zijn genomen en adequaat gemotiveerd zijn.

§ 3.2 Kaders voor logging tussen organisaties onderling

Het uitgangspunt is dat overheidsorganisaties burgers en bedrijven niet naar de bekende weg vragen. Er geldt dat informatie die reeds bij de overheid beschikbaar is niet opnieuw aan burgers wordt gevraagd. Dit betekent in veel gevallen dat overheidsorganisaties gebruik (moeten) maken van elkaars informatie en daarop moeten kunnen vertrouwen.

Om te kunnen aantonen dat ze besluiten zorgvuldig en met de juiste informatie hebben genomen, dienen organisaties daarom vast te leggen welke informatie zij op welk moment van welke organisatie hebben verkregen. Vice versa vergt dit dat bij de organisatie die heeft geleverd wordt bijgehouden aan welke andere organisaties is geleverd, zodat verantwoording volledig kan worden teruggeleid naar de bron van de informatie.

Dit vergt dat de handelingen worden gelogd, en dat afspraken worden gemaakt om te zorgen dat de logging over overheidsorganisaties heen adequaat is vormgegeven om reproductie overheidsbreed

mogelijk te maken.

De hier beschreven kaders dragen tevens bij aan de benodigde interoperabiliteit die tussen organisaties moet worden bewerkstelligd.

§ 3.3 Soorten logging

Met logging in het kader van dit document wordt de logging bedoeld die nodig is om verantwoording af te leggen over de processen en beslissingen die de overheid neemt (functionele logging). Organisaties zullen daarnaast ook logging hebben die de technische werking van systemen of de werking van applicaties betreft. Deze typen logging kunnen overlap vertonen met de functionele logging, maar dat hoeft niet zo te zijn.

> Als in dit document gesproken wordt over applicatie wordt verwezen naar de definitie van het woord "applicatie" in de standaard Logboek Dataverwerkingen.

§ 3.4 Tussenconclusie

Voor een goed inrichting van logging als verantwoordingsmogelijkheid is het van belang dat binnen organisaties logging op eenduidige wijze – conceptueel – wordt ingericht. Daarnaast is het van belang dat de wijzen van vastlegging van handelingen ten aanzien van informatie adequaat op elkaar aansluiten.

§ 4. Eenduidige verantwoording en logging ten behoeve van de uitvoering van verplichtingen

§ 4.1 Overheidsbreed verantwoorden is samenwerken

Organisaties hebben informatie nodig van elkaar om zichzelf te kunnen verantwoorden.

In de eerste plaats dienen zij zelf vast te leggen welke handelingen zij verrichten bij het nemen van besluiten of het uitvoeren van feitelijke handelingen.

Daarnaast zullen zij vastleggen welke informatie zij op welk moment van een andere overheidsorganisatie (de “verstrekkende” organisaties) hebben ontvangen om een bepaald besluit te

nemen. Eenduidige logging kan helpen bij de uitvoering van verschillende plichten, door te zorgen dat de verstrekkende organisatie op dezelfde wijze de verstrekking logt. Zo zijn de “gegevensvraag” en de “gegevenslevering” als dat nodig is te koppelen en te verantwoorden. Deze verplichtingen kaderen de logging en daarmee de standaardisatie van logging.

§ 4.2 Informatieverplichtingen

In het voorgaande is besproken welke gegevens organisaties mogen verwerken om hun taken uit te voeren en zich over deze taken te verantwoorden. Dit “begrenst” de gegevens waarover zij mogen beschikken.

Ten aanzien van de gegevens waarover zij mogen beschikken in het kader van reguliere taken kunnen, naast verantwoording, nog andere verplichtingen rusten. Persoonsgegevens vormen een belangrijke categorie binnen de totale set aan gegevens die voorhanden zijn. Op deze gegevens is de AVG van toepassing. Dit betekent dat diverse informatieverplichtingen, zoals bij het inzagerecht, van toepassing zijn. Deze verplichtingen, die van invloed kunnen zijn op de wijze waarop gegevens worden gelogd, worden hieronder besproken.

§ 4.3 Informatieverplichtingen in de AVG

De AVG geeft aan betrokkenen – degenen over wie de persoonsgegevens gaan - verschillende rechten in het kader van inzage en correctie. Denk hierbij aan het recht op informatie (art. 13 en 14 AVG), het recht op inzage (art. 15 AVG), het recht op rectificatie (art. 16 AVG) en het recht op gegevenswissing (art. 17 AVG).

Deze rechten kan de betrokkene inroepen tegenover de zogenoemde ‘verwerkingsverantwoordelijke’, dat is de organisatie die het doel en de middelen van de gegevensverwerking bepaalt.

Hieronder worden deze rechten kort besproken, waarbij wordt toegelicht welke invloed deze rechten hebben op de wijze waarop gegevens gelogd moeten worden. Belangrijke notitie is dat er geen extra gegevens mogen worden gelogd om uitvoering te geven aan deze rechten. Dat is op grond van de AVG niet toegestaan, omdat de uitvoering van de AVG op zichzelf geen extra verwerkingen mag veroorzaken. Echter het kan wel zo zijn dat de rechten, om deze adequaat te kunnen uitvoeren, van invloed zijn op de wijze waarop de handelingen ten aanzien van persoonsgegevens worden gelogd.

§ 4.3.1 Recht op informatie (bij verzamelen persoonsgegevens)

De informatie die een verwerkingsverantwoordelijke moet aanleveren op basis van het recht op informatie (ex. artikel 13 en 14 AVG) dient uit eigen beweging door verwerkingsverantwoordelijke te worden aangeleverd aan de betrokkene. Voor de andere rechten geldt dat deze uitgaan van een verzoek van betrokkene.

§ 4.3.2 Actieve informatieplicht (recht op informatie bij verzamelen, art. 13 en 14 AVG)

Een verwerkingsverantwoordelijke is verplicht een betrokkene te informeren over wat ze doet met de persoonsgegevens van betrokkene.

Gegevens direct afkomstig van betrokkene zelf (art. 13 AVG)
Als de gegevens van betrokkene zelf afkomstig zijn, dan moet de informatie worden gegeven voordat de betrokkene de gegevens verstrekt. De verwerkingsverantwoordelijke moet kunnen aantonen dat een betrokkene actief is geïnformeerd. De informatieplicht geldt niet in het geval dat de betrokkene al op de hoogte is van alle informatie. Dit moet een organisatie zeker weten om zich hierop te mogen beroepen en om dat te kunnen aantonen, moet de organisatie dit vastleggen.

Gegevens niet direct afkomstig van betrokkene (art. 14 AVG)
Als de gegevens niet afkomstig zijn van de betrokkene zelf, maar van een andere organisatie, dan moet de betrokkene ook worden geïnformeerd. De manier waarop hangt af van hoe groot de groep mensen is waarvan de gegevens zijn doorgekregen en wat de meest adequate manier is om te informeren. Gaat het om een kleine groep mensen, dan moet de organisatie ieder van deze betrokkenen persoonlijk informeren. Bij een grote groep is het voldoende als de organisatie informatie geeft via bijvoorbeeld een krant of online middel. Maar dan moet de organisatie wel iedereen van de groep bereiken. Als de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, moet de informatie worden gegeven uiterlijk op het moment van het eerste contact met de betrokkene; of indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

Als de persoonsgegevens niet direct afkomstig zijn van betrokkene, kan het zijn dat het onevenredig veel inspanning kost om de betrokkene te bereiken. Bijvoorbeeld indien het adres van betrokkene achterhaald moet worden. De verwerkingsverantwoordelijke moet dan wel vastleggen waar de betreffende persoonsgegevens vandaan komen.

Ook hiervoor geldt dat de verwerkingsverantwoordelijke dit moet kunnen aantonen, en dus vastleggen.

§ 4.3.3 Inzagerecht (art. 15 AVG)

Iedereen heeft recht op inzage in de persoonsgegevens die organisaties over hen verwerken. De verzoeker heeft bij een inzageverzoek in principe recht op alle persoonsgegevens die worden verwerkt, waaronder persoonsgegevens in registraties, maar ook persoonsgegevens in correspondentie, zoals e-mails. De overheidsorganisatie moet daarbij inzage bieden in de doelen waarvoor de gegevens worden verwerkt (de wettelijke taken), aan welke (soorten) organisaties de persoonsgegevens zijn doorgegeven, hoe gegevens verzameld zijn en lang deze worden bewaard. Ook moet de organisatie inzicht bieden in of de persoonsgegevens gebruikt worden voor automatische besluitvorming, wat de logica daarvan is en welke gevolgen dat heeft.

Om dit inzicht in concrete gevallen te kunnen bieden is het nodig dat de verwerkingen van de specifieke persoonsgegevens van de betrokkenen gelogd worden. Let op: het gaat hierbij om de verwerkingen die ten aanzien van gegevens zijn uitgevoerd.

§ 4.3.4 Correctierecht

Een betrokkene heeft het recht om gegevens die niet (meer) kloppen te corrigeren. Ook heeft de betrokkene het recht om de gegevens aan te laten vullen wanneer deze incompleet zijn. Het gaat dus om het recht op het corrigeren van incorrecte of incomplete gegevens.

Om te kunnen vaststellen of gegevens (niet) kloppen, dient vastgesteld te zijn wat de kwaliteit van de gegevens is (welke controles zijn uitgevoerd). En indien aan de orde, wat de herkomst van de gegevens is (van welke organisaties zij de gegevens verkregen, op welk moment, en welke controles zijn gedaan). De conclusie van de vaststelling kan ook zijn dat de correctie niet wordt doorgevoerd.

Om dit te kunnen doen is het nodig dat de verwerkingshandelingen worden vastgelegd. Om deze wijze kunnen ook (doorwerkende) gevolgen van de onjuiste gegevens worden gecorrigeerd.

De verwerkingsverantwoordelijke moet, indien er redenen zijn om gegevens te wijzigen, ook eventuele ontvangers van de gegevens (andere organisaties waaraan de gegevens zijn verstrekt) informeren over de wijziging (kennisgevingsplicht). Om dit te kunnen doen moet de verwerkingsverantwoordelijke weten aan welke organisatie en op welk moment gegevens zijn verstrekt. Deze gegevens zullen dan ook gelogd moeten worden.

In de sectorspecifieke wetgeving omtrent een openbaar register zijn bepalingen opgenomen over correctie van gegevens. In zo’n geval zal in de betreffende wetgeving gekeken moeten worden hoe correctie doorgevoerd kan worden. zie ook het recht op rectificatie

Dit correctierecht is van groot belang in het kader van het herstel van dienstverlening en de bestrijding van identiteitsdiefstal.

§ 4.3.5 Beperkingen op informatieplichten

Zwaar(der)wegende algemene belangen
De rechten van betrokkenen gelden niet als er een zwaarwegend belang is om niet te informeren, bijvoorbeeld om strafbare feiten te voorkomen of om de vrijheden van anderen te beschermen. Dit is mogelijk als wordt voldaan aan een van de uitzonderingen uit artikel 41 UAVG. Dit betreft situaties waarin (kort samengevat) nationale/openbare veiligheid of de opsporing van strafbare feiten zwaarder moet wegen.

Om te kunnen weten of er (mogelijk) sprake is van een algemeen belang dat zwaarder moet wegen dan het belang van de betrokkene op informatie, dient de verwerkingsverantwoordelijke dit te kunnen achterhalen. Dit houdt in dat de situatie waarin daar mogelijk sprake van kan zijn, zoals verstrekking van gegevens aan bijvoorbeeld een opsporingsinstanties, voor de verwerkingsverantwoordelijke herleidbaar moet zijn. Dit betekent dat dit op enige manier moet zijn vastgelegd.

Ook moet de verwerkingsverantwoordelijke kunnen vaststellen of er – bijvoorbeeld door tijdsverloop - nog wel reden is om de beperking op informatie te handhaven, of dat het belang niet meer aan de orde is (bijvoorbeeld als een strafrechtelijk onderzoek is afgerond).

Zwaar(der) wegende belangen van betrokkene of rechten van anderen
Het kan voorkomen dat persoonsgegevens van een betrokkene, als deze ter inzage worden aangeboden, ook informatie over een ander persoon (een derde) bevat, en deze derde daardoor in zijn recht of vrijheid kan worden aangetast, bijvoorbeeld in het geval van informatie over een verblijfplaats. Het kan dan in voorkomende gevallen noodzakelijk zijn om informatie dan niet aan een betrokkene ter inzage te bieden.

Echter, om deze afweging te kunnen maken zal nodig zijn dat is vastgelegd of daarvan sprake zou kunnen zijn. Dit is bijvoorbeeld het geval als informatie is verstrekt aan of verkregen is van instanties die zich bezighouden met de uitvoering of het waarborgen van beschermende maatregelen.

§ 4.3.6 Inbreuken op persoonsgegevens (datalekken) en melding

Als er sprake is van een datalek, dan moet dat bij de Autoriteit Persoonsgegevens (AP) gemeld worden. In sommige gevallen moet ook informatie verstrekt worden aan betrokkenen.

Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is, waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

De verplichtingen ten aanzien van een datalek veronderstellen dat een organisatie maatregelen heeft genomen om te kunnen constateren dat een datalek heeft plaatsgevonden, wanneer dat heeft plaatsgevonden en welke (onrechtmatige) verwerkingen van persoonsgegevens dat tot gevolg heeft gehad. Dit betekent dat het doorbreken van beveiligingsmaatregelen dient te worden gelogd, en ook de verwerkingshandelingen die ten aanzien van de persoonsgegevens hebben plaatsgevonden. Organisaties dienen maatregelen te treffen om ingeval van problemen deze zo snel mogelijk te kunnen herkennen, en in het verlengde daarvan, ook te kunnen herstellen. Ook dit vergt dat wordt vastgelegd welke gegevens op welk moment zijn verwerkt, ontvangen, verstrekt, et cetera. Op deze wijze kunnen organisaties in gevallen waarbij voor betrokkene mogelijk ook schade kan ontstaan, daarmee rekening houden en zo nodig maatregelen treffen.

§ 4.4 Zorgvuldigheidsverplichtingen

§ 4.4.1 Inleiding

Bij het verkeer tussen bestuursorganen en burgers, vormen de algemene beginselen van behoorlijk bestuur een belangrijk fundament. Deze deels geschreven, deels ongeschreven algemene rechtsbeginselen zijn gedragsregels voor de overheid. Ze gaan bijvoorbeeld over de manier waarop de overheid besluiten neemt, maar ook op overig handelen van de overheid zijn ze in principe van toepassing (art. 3:1, tweede lid, Awb). Voorbeelden van deze beginselen zijn de beginselen van zorgvuldige voorbereiding en belangenafweging (art. 3:2 respectievelijk art. 3:4 Awb) en het motiveringsbeginsel van besluiten (art. 3:46 Awb).

§ 4.4.2 Zorgvuldige voorbereiding en belangenafweging

Bestuursorganen dienen besluiten zorgvuldig voor te bereiden. Bij de voorbereiding van besluiten worden vaak (persoons)gegevens van burgers en bedrijven gebruikt. Verder zijn die gegevens vaak afkomstig van veel verschillende instanties. Bij de aanvraag van een parkeervergunning komen er bijvoorbeeld gegevens over de wijk waarin je woont uit de BRP en komen er gegevens over de auto die je bezit uit het kentekenregister. Ook moeten bestuursorganen zorgvuldig alle betrokken belangen afwegen. Hierbij mogen de gevolgen voor een specifieke persoon (of groep) niet

onevenredig zijn. Ook om deze afweging zorgvuldig te kunnen maken, verwerkt de overheid (persoons)gegevens.

4.4.3 Motiveringsbeginsel

Verder dient een bestuursorgaan een besluit goed te motiveren. Burgers en bedrijven moeten kunnen weten welke factoren hebben meegewogen bij het nemen van een besluit. Dit gaat om welke argumenten zijn gebruikt, en welke juridische grondslagen het besluit op is gebaseerd, maar ook om welke gegevens de basis vormen voor het besluit.

4.4.4 De beginselen in de context van verwerkingenlogging

In de context van verwerkingenlogging is het van belang om de hierboven genoemde beginselen in samenhang te bezien. Het goed kunnen voldoen aan een van de verplichtingen, is noodzakelijk voor het voldoen aan de andere. Chronologisch wordt een besluit eerst zorgvuldig voorbereid, waarbij alle betrokken belangen zorgvuldig worden afgewogen en onevenredig benadeelde groepen niet uit het oog worden verloren. De motivering gebeurt gedurende het gehele proces, en vormt een volledige en betrouwbare reconstructie wanneer het proces is afgerond. Een gestandaardiseerde manier van verwerkingenlogging ondersteunt dit hele proces. Tijdens de voorbereiding van een besluit wordt goed bijgehouden welke gegevens worden gebruikt, waar ze vandaan komen en voor welke reden ze zijn opgevraagd. Zo is achteraf altijd goed duidelijk hoe een besluit tot stand is gekomen en kan het bestuursorgaan dit altijd goed motiveren. Verwerkingenlogging helpt de bestuursorganen om zich goed te kunnen verantwoorden.

4.5 Informatiebeveiligingsverplichtingen

4.5.1 Baseline Informatiebeveiliging Overheid (BIO)

De BIO legt overheden diverse beveiligingsverplichtingen op, om de informatie te beschermen die wordt verwerkt. Informatie die wordt verwerkt om de taken, verantwoordelijkheden en informatieverplichtingen zoals in het voorgaande besproken goed te kunnen uitvoeren.

De BIO verplicht om bepaalde gebeurtenissen in informatiesystemen vast te leggen (par. 12.4). Daarbij gaat het om logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen daarop en informatiebeveiligingsgebeurtenissen (beveiligingsincidenten) vastleggen.

Dit betreft systeemgebeurtenissen, maar deze zullen ook, op applicatieniveau, direct te relateren zijn aan verslaglegging die overheden in het kader van hun verantwoording (ook) moeten vastleggen. De standaard dekt in principe niet de BIO logging af, maar de standaard kan hierbij wel helpen.

De BIO bepaalt de informatie die een logregel ten minste moet bevatten, waaronder de gebeurtenis, de informatie die nodig is om incidenten te herleiden tot natuurlijke personen, het resultaat van de gebeurtenis en het tijdstip.

Deze informatie is nodig om in geval van problemen, deze tijdig te kunnen herkennen en te kunnen herstellen.

§ 4.5.2 Toegangsbeveiliging en beheer

Toegangsbeveiliging en het beheer van toegang is een algemeen beginsel dat voor alle gegevensverzamelingen en gegevensuitwisseling cruciaal is. Het vormt de basis van het vertrouwen in de overheid en het spreekt voor zich dat dezelfde strenge wetten, regels, standaarden en normen die van toepassing zijn op de gegevens zelf en de uitwisseling van gegevens ook van toepassing zijn op de logs (en back-ups) die er zijn van de gegevens. Ook hiervoor geldt dat de standaard in principe niet de BIO logging afdekt, maar hierbij wel kan helpen.

§ 4.6 Verantwoordingsbehoeften van toezichthouders

§ 4.6.1 Verantwoording over verschillende onderwerpen

Het verantwoorden over hun handelen doen overheidsorganisaties niet alleen publiekelijk of in de richting van (individuele) burgers en bedrijven of zaken die hen raken. Organisaties dienen zich ook met “algemene informatie” over beleidsvorming en onderbouwing daarvan, informatie over financiën, prestaties, bedrijfsvoering en maatschappelijke verantwoordingsinformatie te verantwoorden.

Hoewel de verantwoording hier ook vaak zal gaan over de inhoudelijke onderbouwing van gemaakte keuzes en gevoerde beleidsrichting zal het ook gaan om informatie die op geaggregeerd niveau uit de (logging) van de dagelijkse handelingen van organisaties voortvloeien. Dat geldt bijvoorbeeld voor verantwoording over de prestaties.

Het is wenselijk om waar mogelijk kengetallen te gebruiken om de prestaties van de instelling in beeld te brengen. Bij het gebruik van kengetallen is het van belang dat ze de juiste informatie

overbrengen, dat het aantal kengetallen beperkt is, en dat ze worden toegelicht.

De informatie over de prestaties moet zo concreet mogelijk zijn, dus afhankelijk van het soort prestatie, en moet inzicht geven in aantallen, omvang of bedragen. De waarde van deze informatie voor de gebruiker wordt groter als ze vergeleken kan worden met de prestaties en kosten in voorgaande jaren of met de prestaties van vergelijkbare instellingen. Het is ook wenselijk dat een relatie met de strategische doelstellingen wordt gelegd.

Hoewel dergelijke verantwoordingsdoelen op het eerste gezicht niet direct een relatie lijken te hebben met de verslaglegging van de dagelijkse taken van de organisaties, vloeit de informatie om deze doelen te realiseren daar uiteindelijk wel uit voort.

§ 4.7 Tussenconclusie

Logging die wordt vastgelegd kan vele verschillende doelen dienen, zoals de invulling van specifieke informatieverschaffing aan burgers, of de verantwoording over de zorgvuldigheid van overheidshandelen.

Belangrijk is dat de conceptuele invulling van afspraken over logging zodanig wordt ingericht dat zij breed toepasbaar is, maar tegelijkertijd ruimte laat om specifieke invulling (“aanbouw”) van afspraken op specifieke doelen te ondersteunen.

§ 5. Eenduidigheid bevorderen is standaardiseren

§ 5.1 Standaardisatie van logging binnen organisaties

In het voorgaande is naar voren gekomen dat overheden bij de uitvoering van hun taken (persoons)gegevens verwerken. Daarbij zullen zij gegevens verwerken die zij zelf verzamelen en beheren, en op basis daarvan conclusies trekken en besluiten nemen.

Hoewel organisaties verschillende taken kunnen hebben, en afhankelijk daarvan ook verschillende soorten gegevens verwerken en verschillende soorten besluiten nemen, zal de wijze waarop zij zich over de uitvoering ervan moeten verantwoorden, minder divers zijn.

Gelet op de verantwoordingsverplichtingen – zoals de beginselen van behoorlijk bestuur – die zijn vastgelegd in de Awb en bijvoorbeeld de AVG, maakt de wijze waarop de verwerkingen van gegevens worden vastgelegd niet uit.

In alle gevallen zal de herkomst van de gegevens die worden gebruikt moeten worden gelogd, waaronder (meta)gegevens over de kwaliteit van deze gegevens. Ook het moment waarop de gegevens worden gebruikt om te komen tot een besluit, en de wijze waarop de gegevens worden gebruikt, zal moeten worden vastgelegd (motivering).

Het zal bij organisaties vermoedelijk vaak voorkomen dat gegevens die worden gebruikt, in verschillende (deel)verwerkingen worden vastgelegd. Een overzicht van de verschillende registraties die worden gebruikt (ook als daar geen persoonsgegevens in opgenomen zijn) zal daarom noodzakelijk zijn. Ook zal nodig zijn dat er over de verwerkingen heen een relatie kan worden gelegd tussen de gegevens die ten behoeve van een specifiek besluit zijn gebruikt, en aan welke (natuurlijke) persoon dit besluit is gericht.

Om te zorgen dat overheidsorganisaties dit op een eenduidige (gestandaardiseerde) wijze doen, ligt het voor de hand daarover regels te stellen in een op te leggen standaard.

§ 5.2 Standaardisatie van logging tussen organisaties (informatie-uitwisseling)

Bij de uitvoering van hun taken zullen organisaties regelmatig gebruik maken van gegevens van andere overheidsorganisaties. Onder meer omdat het uitgangspunt is dat gegevens die bij de overheid bekend zijn, niet nogmaals bij burgers of bedrijven mogen worden uitgevraagd.

Dit betekent dat overheden, naast de uitvoering van de eigen taken, met regelmaat ook ondersteunend voor de taakuitvoering voor collega-overheidsorganisaties zullen zijn. Zij zullen daarbij zowel ontvanger als leverancier van informatie zijn. En dat betekent dat de wijze van hun eigen verantwoording (en logging) van belang is voor de verantwoording van andere overheidsorganisaties. Daarom is het van belang om ook afspraken te maken over de wijze waarop gegevens aan andere overheidsorganisaties worden verstrekt, of worden ontvangen.

Om deze koppeling goed te kunnen leggen, en daarmee de overheidsbrede verantwoording goed te kunnen vormgeven, is het belangrijk om afspraken te maken over de gebeurtenissen waarvoor de gegevens worden verstrekt, het tijdstip waarop dit gebeurt en de waarborgen die zijn getroffen. Overigens is dit niet alleen nodig ter verantwoording, maar ook om ingeval van problemen bij het gebruik van onjuiste gegevens deze snel te kunnen herkennen en herstellen, ook als de problemen organisatie-overstijgend zijn.

§ 5.3 Tussenconclusie

Om eenduidigheid te bevorderen, ook ten aanzien van de wijze van verslaglegging, is het nodig om afspraken te maken die zorgen dat verschillende organisaties logging op eenzelfde manier

inrichten. Daarmee wordt een werkwijze of handeling gestandaardiseerd. Dat begint met afspraken over de wijze waarop organisaties zelf handelen binnen de eigen verantwoordelijkheid om verslaglegging te doen, maar ook hoe zij deze verslaglegging op elkaar laten aansluiten en waar de grenzen liggen.

6. Een standaard opstellen om deze kaders te faciliteren

6.1 Afspraken over logging maken

6.1.1 Behoud van verantwoordelijkheid van elk overheidsorgaan

Een belangrijk uitgangspunt is dat elke overheidsorganisatie verantwoordelijk is voor de uitvoering van haar eigen taken. Niet meer en niet minder. Dit is in de eerdere hoofdstukken ook vastgesteld. In het verlengde daarvan is het belangrijk dat dit ook voor de logging van de eigen taken wordt doorgevoerd. Organisaties loggen de gegevensverwerkingen die zij ten behoeve van zichzelf uitvoeren. Daaronder valt tevens de ontvangst van gegevens van andere overheidsorganisaties, of gegevens die zij aan andere organisaties geleverd hebben.

6.1.2 Grote gemene deler in verplichtingen zoeken

Standaardiseren betekent dat bezien moet worden welke afspraken voor elke organisatie zouden moeten gelden, en waarover het verstandig is om afspraken te maken. Zoals hiervoor beschreven heeft elke organisatie zijn eigen taak en op basis van die taak processen ingericht.

De informatie die een organisatie verwerkt, en waarvoor moet worden gelogd ten behoeve van verantwoording, verschilt ook. De grote gemene deler zit dus niet in het voorschrijven van specifieke gegevens die moeten worden gelogd, het doel waarvoor moet worden gelogd, of de termijn waarop moet worden gelogd.

Wat echter voor elke organisatie op dezelfde wijze kan plaatsvinden, los van de taak of het doel, is de wijze waarop verwerkingen ten aanzien van gegevens worden vastgelegd (het feit dat er een verwerking heeft plaatsgevonden), ten behoeve van onderlinge relateerbaarheid, zowel binnen als buiten de organisatiegrenzen.

6.1.3 Baseline voor logging voor organisaties

De standaard dient daarom interoperabiliteit van logging van dataverwerkingen te realiseren, door voor een aantal loghandelingen de koppelvlakken en werkwijze voor te schrijven. Daarmee wordt de basis gelegd voor een uniforme wijze van logging door verschillende systemen in de organisatie, die relateerbaar is.

De standaard dient voorschriften te bevatten over het vastleggen van logs, over het aan elkaar relateren van deze logs en over het aan elkaar relateren van dataverwerkingen over grenzen van systemen (binnen organisaties).

Op deze manier is de logging zelf “neutraal” (doel en toepassing maakt voor de logging en relateerbaarheid niet uit). De logging maakt het echter wel mogelijk om voor verschillende doelen of toepassingen te worden ingezet.

Een organisatie kan desgewenst vanuit dit vertrekpunt extensies maken op de standaard op basis van de specifieke behoefte die zij heeft. Op deze manier kan een organisatie de eigen behoefte aan logging “op maat inrichten”. Organisaties en sectoren die dit doen moeten deze extensie conform het beheerproces van de standaard laten vaststellen. Dit ter voorkoming van dialecten binnen de standaard en mogelijkheden tot breder gebruik.

6.2 Logging van informatie-uitwisseling

Zoals hiervoor is besproken kunnen dataverwerkingen ten behoeve van taken verschillende verantwoordelijkheden overstijgen (en dus organisatie-overstijgend zijn). Doordat elke organisatie op basis van de standaard op dezelfde wijze én binnen de reikwijdte van de eigen organisatie logt, vallen er in de logging geen gaten en is de onderlinge verbondenheid in verantwoordelijkheden geborgd.

Immers vallen onder de verantwoordelijkheid om te loggen tevens de ontvangst van gegevens van andere overheidsorganisaties, of de gegevens die zij aan andere organisaties geleverd hebben. Daardoor is de informatie-uitwisseling als geheel gelogd en wordt voorkomen dat “dubbele logging” ontstaat. Dat brengt naast doelmatigheid ook een beperking van de kans op fouten of strijdige logging met zich mee.

6.3 Ketenlogging

Zoals aangegeven is de logging op basis van de afspraken “neutraal”. De logging zorgt voor uniforme vastlegging door organisaties van gegevensverwerkingen en voor onderlinge

relateerbaarheid van deze verwerkingen. De logging is dus niet gebonden aan een specifieke organisatie of aan organisaties die met elkaar samenwerkingen (“ketens”).

Het is echter mogelijk om, als een organisatie dat wil, door middel van extensies op de standaard aanvullingen te doen op de logging, of aanvullende afspraken te maken met andere overheden waarmee specifiek wordt samengewerkt. Sectorale aanvullingen binnen “samenwerkende ketens van organisaties” zijn mogelijk bovenop de basis die de standaard legt.

§ 6.4 Functionele invulling

Om de hiervoor besproken uitgangspunten – eenduidige wijze van logging, scope van logging en onderlinge relateerbaarheid van logging – te bereiken, zullen functionele afspraken gemaakt moeten worden. Door de functionele logging tot het niveau van relateerbaarheid te beperken betekent het ook dat de standaard in de basis deze aspecten dient te adresseren.

Dit houdt in dat voor logging afspraken moeten worden gemaakt over de identificatie van transacties en/of mutaties (deze moeten functioneel herkenbaar of afgebakend zijn om als generieke basis voor logging te kunnen dienen).

Verder moet de relatie met eerdere en onderliggende transacties of mutaties duidelijk zijn. Dat zorgt ervoor dat de transactie in de juiste context en onder de juiste verantwoordelijkheid geplaatst kan worden. Ook moet een referentienummer worden toegekend voor koppeling tussen verschillende organisaties.

§ 6.5 Technisch operationele invulling

De technische en operationele invulling moet zodanig plaatsvinden dat de functionele behoefte adequaat wordt ingevuld. Daarnaast dient ervoor gezorgd te worden dat de niet-functionele randvoorwaarden (zoals privacy en beveiligingsvereisten, wet- en regelgeving) adequaat worden ingevuld. Deze niet-functionele randvoorwaarden liggen in feite besloten in dit document (kadering). Binnen deze ruimte is de technische invulling vrij, als middel om een aan het bovenliggend doel te voldoen.

§ 6.6 Tussenconclusie

Bij de inrichting van een standaard die aan de basis ligt om verslaglegging (logging) te standaardiseren, is een belangrijk uitgangspunt dat de verantwoordelijkheid van elke organisatie als

uitgangspunt wordt genomen, inclusief de grens daarvan. Dat vormt de “scope” per organisatie. Op basis daarvan kan een basis (baseline) worden afgesproken waarop kan worden voortgebouwd.

7. Beschrijving van de standaard

7.1 Doel van de standaard

Om verantwoording te kunnen afleggen, zowel als overheidsorganisatie, maar met name ook om als “de overheid” te kunnen verantwoorden, dat wil zeggen als “samenwerkende overheidsorganisaties”, is het van belang dat de wijze waarop overheden verslag leggen van hun activiteiten eenduidig is, en dat de verschillende verslagleggingen aan elkaar te relateren zijn. Dat is de basis voor onderlinge samenwerking op dit terrein.

De standaard “Logboek Dataverwerkingen” zorgt daarvoor.

De standaard beoogt (technische) interoperabiliteit van loggen van dataverwerkingen te realiseren, door voor een aantal loghandelingen de koppelvlakken en werkwijze voor te schrijven:

- Het vastleggen van logs van dataverwerkingen
- Het aan elkaar relateren van deze logs.
- Het aan elkaar relateren van dataverwerkingen over grenzen van systemen (binnen organisaties) en verantwoordelijkheden (organisatie-overstijgend)

De standaard is ontwikkeld vanuit de behoefte om als overheid eenduidige verantwoording over overheidsorganisaties heen te kunnen realiseren. Echter, de systematiek zoals beschreven is breder toepasbaar voor organisaties buiten de overheid, die de verslaglegging onderling willen afstemmen en relateren.

7.2 Beschrijving van systematiek van processen in organisaties

Organisaties hebben taken toebedeeld gekregen. Om deze taken uit te voeren is het nodig om (persoons)gegevens te verwerken.

De standaard schrijft voor dat deze per taak als “verwerkingsactiviteit” worden onderkend. Om de verschillende taken uit te voeren heeft een organisatie in de regel meerdere verwerkingsactiviteiten onderkend.

De standaard schrijft voor dat deze verwerkingsactiviteiten in een “register” moeten worden opgenomen. Daarin wordt onder meer het doel van de verwerkingen opgenomen, zoals dit bijvoorbeeld op grond van de AVG voor verwerkingen van persoonsgegevens al verplicht is. Registers in het kader van de standaard beoogen een bredere reikwijdte dan persoonsgegevens.

Vervolgens schrijft de standaard voor dat binnen de onderkende verwerkingsactiviteiten “dataverwerkingen” worden gelogd. Dit gebeurt door iedere applicatie die een dataverwerking uitvoert, op gestandaardiseerde manier een logregel te laten vastleggen in een Logboek dataverwerkingen.

De handelingen die worden gelogd kunnen alle handelingen betreffen die met gegevens plaatsvinden.

Elke dataverwerking wordt apart gelogd en krijgt een kenmerk (“trace”) toegekend, waardoor bij elkaar horende dataverwerkingen binnen de grenzen van een systeem worden gegroepeerd en kunnen worden gerelateerd. Dit betekent dat de handelingen die ten behoeve van een specifieke taak (context) zijn uitgevoerd aan elkaar te relateren zijn, en daarmee **te verantwoorden** zijn.

Omdat dataverwerkingen kunnen of zullen plaatsvinden voor meerdere taken (contexten, verwerkingsactiviteiten), ook over organisaties heen, is het nodig dat ook de relatie (link) kan worden gelegd tussen de verschillende taken. De standaard realiseert dit door informatie over de “trace”, “verwerkingsactiviteit” en registers (de statische informatie over de dataverwerking) mee te geven aan de uitwisseling van gegevens. Op deze wijze zijn de dataverwerkingen te relateren over verschillende taken en organisaties heen, en kan **verantwoording** worden afgelegd.

§ 7.3 Standaard als basis voor verantwoording: logging is “neutraal”

Op deze wijze wordt door de standaard geborgd dat de dataverwerkingen worden gelogd zonder dat relevant is in welke context of voor welk doel dat gebeurt (de wijze van logging is “neutraal”).

Echter op het moment dat doelen, context en onderlinge samenhang van belang is kan een verband worden gelegd en wordt de logging betekenisvol, bijvoorbeeld om verantwoording af te leggen over een specifieke handeling die is uitgevoerd in het kader van een taak door één of meerdere overheidsorganisaties (basale usecase).

§ 7.4 Extensies: Het gebruik van logging voor verschillende doeleinden

Op basis van de algemene relateerbaarheid die de standaard realiseert over de logging van verschillende dataverwerkingen, is het - naast de algemene verantwoording die op basis daarvan kan worden afgelegd - mogelijk om diverse andere doeleinden en processen te faciliteren. De

standaard maakt dat mogelijk door extensies toe te staan waarmee specifieke functionaliteit wordt toegevoegd aan de standaard.

Een voorbeeld daarvan is de “Extensie Betrokkenen”. Daarmee kan meer precies worden uitgewerkt hoe de identiteit van een betrokkene wordt gerelateerd aan een dataverwerking. Dat maakt het mogelijk om de koppeling te maken tussen de verwerkingen van persoonsgegevens, waarmee bijvoorbeeld inzageverzoeken geautomatiseerd mogelijk gemaakt kunnen worden. Een ander voorbeeld is de “Extensie Inzage”, waarmee de wijze waarop op basis van de logs op een gestandaardiseerde manier de verwerkingen van gegevens over een persoon ter inzage kunnen worden aangeboden (interface).

Organisaties en sectoren die een extensie maken, moeten deze extensie conform het beheerproces van de standaard laten vaststellen waarmee extensie een optioneel onderdeel wordt van de standaard.

§ 7.5 Profielen: beperkingen en verplichtingen in het gebruik van de standaard

De standaard zorgt ervoor dat eenduidige relaties gelegd kunnen worden tussen dataverwerkingen. De standaard legt daar in de basis geen beperkingen of aanvullingen aan op, en ook niet aan de tijdsduur waarbinnen de relaties moeten kunnen worden gelegd (bewaartermijn). Door middel van profielen kunnen dergelijke aanvullingen wel gemaakt worden, bijvoorbeeld door extensies, aanvullende eisen, of bewaartermijnen. Dit kan binnen een organisatie of binnen een groep van organisaties, bijvoorbeeld een sector die op een bepaalde wijze met elkaar samenwerking en afspraken wil maken.

§ 7.6 Integriteit van logging

Een belangrijk aspect bij verantwoording is dat op de informatie kan worden vertrouwd. Dit betekent dat de wijze waarop logging wordt weggeschreven en bewaard zodanig is dat deze beschermd is en dat eventuele manipulaties van de logging kunnen worden aangetoond. Deze onweerlegbaarheid is belangrijk voor de bewijskracht van de logging. Als dit generiek is geregeld hoeven organisaties niet separaat meer aan te tonen of te regelen dat de logging ook daadwerkelijk klopt. Dit aspect zou als extensie kunnen worden toegevoegd.

7.7 Tussenconclusie

Het is van belang dat de wijze waarop overheden hun activiteiten vastleggen eenduidig is, en dat de verschillende verslagleggingen aan elkaar te relateren zijn. Dat is de basis om de onderlinge informatieuitwisseling te kunnen relateren. De standaard bevat om deze reden conceptuele afspraken, bedoeld om rekening te houden met verschillende processen, dataverwerkingen en de wijze waarop deze zijn worden gerelateerd. Dit vormt de basis waarmee het mogelijk is om voor verschillende toepassingen of doelen nadere toevoegingen op de standaard te maken. Daarbij is er ruimte om dit per organisatie of per groep organisaties (sector) aan te vullen afhankelijk van de specifieke behoeften.

8. Beleidskader

Leidende principes bij gebruik en inrichting van de standaard

Eigen verantwoordelijkheid:

1. Iedere overheidsorganisatie verantwoordt zich vanuit goed openbaar bestuur op basis van de verwerkingsgrondslagen die zijn toegekend en toegespitst op de vervulling van de eigen taak, over de door haar zelf uitgevoerd verwerking van (persoons)gegevens. Overheidsorganisaties die gebruik maken van de standaard Logboek dataverwerkingen om de verwerking van gegevens gestandaardiseerd te loggen zijn zelf verantwoordelijk voor implementatie en inrichting van de standaard, de logs en de informatie die erin te vinden is.
2. Enkel de gegevens die voor verantwoording nodig zijn worden vastgelegd.

Basis + extensies:

3. Ongeacht de verschillen in (taken van) overheidsorganisaties vindt de verantwoording van het loggen van verwerkingen middels de standaard Logboek dataverwerkingen op eenduidige wijze plaats. Organisaties en sectoren die de standaard gebruiken, kunnen deze aanvullen met (zelf ontwikkelde) specifieke extensies. Organisaties en sectoren die dit doen moeten deze extensie conform het beheerproces van de standaard laten vaststellen. Dit ter voorkoming van dialecten binnen de standaard. Het vaststellen van de extensie verloopt via de organisatie die de standaard beheerd.

Logging van informatieketens:

4. Bij het loggen van de verwerking van gegevens in ketens is elke overheidsorganisatie verantwoordelijk voor haar eigen deel van de keten met als afbakening de ontvangst van

gegevens van (een) ketenpartner(s) en het verstrekken van gegevens aan (een) andere ketenpartner(s) of het nemen van het besluit. Door het uniformeren van de logging kunnen gegevensvraag en gegevenslevering aan elkaar gekoppeld worden. Hierbij worden door gebruik van de standaard Logboek dataverwerkingen afspraken gemaakt over de relateerbaarheid en herkenbaarheid van transacties.

Wettelijke informatieverplichtingen:

5. De organisatie borgt dat de standaard Logboek Dataverwerkingen optimaal ingericht wordt ten behoeve van ondersteuning van aan een aantal wettelijke informatieverplichtingen, zoals:
    - de zorgvuldigheidsverplichting en het motiveringsbeginsel uit de AWB
    - het recht op informatie, het recht op inzage, het recht op rectificatie en het recht op gegevenswissing uit de AVG
6. Persoonsgegevens vastleggen enkel ten behoeve van het loggen is niet toegestaan op basis van de AVG.
7. De standaard Logboek Dataverwerking dient zodanig ingericht te worden dat deze voldoet aan de inhoudelijke loggingsverplichtingen als benoemd in de BIO (of hierop volgende wetgeving).

Zwaarder wegende belangen:

8. De standaard Logboek Dataverwerkingen heeft een sterke relatie met het Register van Verwerkingsactiviteiten. De standaard logt, het register geeft aan over welke activiteit deze gaat. Bij de inrichting van het Register van Verwerkingsactiviteiten wordt rekening gehouden met zwaarder wegende algemene belangen (bijv nationale/openbare veiligheid, opsporing van strafbare feiten) of zwaarder wegende belangen van betrokkene of rechten van anderen (bijv bescherming persoon) waardoor de rechten van betrokken als benoemd in de AVG expliciet niet gelden. Dit kan bijvoorbeeld door bij een verwerkingsactiviteit een vertrouwelijke en niet-vertrouwelijke variant op te nemen, waardoor het vanuit de logfile inzichtelijk of er bij de betreffende verwerking rekening moet worden gehouden met zwaarder wegende belangen.

Aansluiting bij reguliere processen:

9. Beschouw de gecreëerde logfile als persoonsgegevens en pas alle relevante processen en maatregelen die daarop anderszins van toepassing zijn, ook hierop toe (denk aan beveiliging, datalekken, pseudonimisering, correspondentie, inzage, correctie, aansluiting op de BIO).

A. Index

A.1 Begrippen gedefinieerd door deze specificatie

A.2 Begrippen gedefinieerd door verwijzing

↥