De algemene beginselen van behoorlijke gegevensverwerking

Versie 1.0 | mei 2020

Considerans

In dit document staan de algemene beginselen van behoorlijke gegevensverwerking (ABBG). De ABBG zijn ontstaan vanuit de behoefte om in samenwerkingsverbanden, zoals tussen de provincies en SNN, eenduidige afspraken te maken omtrent gegevensverwerkingen. De ABBG zorgen ervoor dat partijen dezelfde uitgangspunten hanteren bij gegevensverwerkingen. De ABBG vormen een algemeen kader dat kan worden aangevuld met specifieke afspraken, voor zover deze niet al volgen uit wet- of regelgeving of een toepasselijke regeling, besluit of overeenkomst.

Partijen

Iedere overheidspartij (of uit overheden samengestelde partij) is bevoegd zich aan te sluiten bij deze verklaring en te verlangen dat gezamenlijke verantwoordelijken zich aan de bepalingen conformeren.

Definities

De in dit document gebruikte definities zijn overeenkomstig de Algemene Verordening Gegevensbescherming (AVG) en Baseline Informatiebeveiliging Overheid (BIO).

Overwegende dat

- Partijen persoonsgegevens verwerken, die een (gezamenlijke) verwerkingsverantwoordelijkheid met zich mee kunnen brengen;
- De verwerkingsverantwoordelijkheid en daarmee de eventuele gezamenlijkheid daarvan afhankelijk is van de regeling en/of overeenkomst op grond waarvan de verwerking van persoonsgegevens plaatsvindt;
- Dat partijen afspraken moeten maken om tot een verantwoorde en veilige verwerking van persoonsgegevens te komen;
- Partijen daartoe de algemene beginselen van behoorlijke gegevensverwerking vaststellen, teneinde de verwerking van persoonsgegevens nader vorm te geven.

Beginselen

De verwerkingen zijn:

1. Rechtmatig, behoorlijk en transparant;
2. Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden;
3. Toereikend, ter zake dienend en noodzakelijk voor de doeleinden;
4. Correct en geactualiseerd;
5. Waar mogelijk geanonimiseerd of gepseudonimiseerd; en
6. Voorzien van passende technische en organisatorische maatregelen.

Grondslag en Verwerkingsregister

1. Er vindt géén gegevensverwerking plaats zonder dat daarvoor enige rechtmatige grondslag is.
2. Partijen nemen de (gezamenlijke) verwerkingen op een vergelijkbare wijze, inclusief de grondslag, op in het eigen Verwerkingsregister.

Doelbinding

1. Een verwerking die verder gaat dan het oorspronkelijke doel, is slechts toegestaan voor zover het hiermee verenigbaar is, een wettelijke uitzondering kent en/of wordt gerealiseerd ten behoeve van wetenschappelijk onderzoek, historisch onderzoek, het algemeen belang en/of statistische doeleinden.

2. Indien een partij voornemens is de persoonsgegevens voor een ander doel te gebruiken dan expliciet uit de bestaande afspraken blijkt, legt deze de overwegingen omtrent het gebruik voor een ander doel vast en geeft de andere Partij(en) inzage in deze onderbouwing.

Communicatie en onderzoek

1. De wettelijke grondslag van gegevensverwerking brengt met zich mee dat de betrokkene niet vrijelijk diens persoonsgegevens heeft kunnen verstrekken. Derhalve zullen partijen terughoudendheid betrachten inzake ongevraagde communicatie met betrokkene en/of het doorzenden van persoonsgegevens aan derden (o.a. onderzoekspartijen).
2. Communicatie met de betrokkene die niet direct tot de rechtsgrond en/of doeleinden van verwerking te herleiden is, zal slechts plaatsvinden indien de betrokkene daar vooraf, vrijelijk en op ondubbelzinnige wijze toestemming voor heeft gegeven.
3. Het verstrekken van en/of inzage bieden in de persoonsgegevens aan derden (o.a. onderzoekspartijen) geschiedt in geanonimiseerde vorm, tenzij dit verenigbaar is met het oorspronkelijke doel van de verwerking.

Rechten van de betrokkene

1. Partijen zijn transparant over de persoonsgegevens die zij verwerken en verstrekken de betrokkene informatie, conform het in artikel 13 en 14 van de AVG bepaalde.
2. Partijen stellen de betrokkene in staat om diens rechten uit te oefenen, zoals beschreven in hoofdstuk 3 van de AVG. Hiertoe worden contactgegevens beschikbaar gesteld op het openbare deel van de eigen website van partijen.
3. De betrokkene mag zich tot één of meer Partijen wenden, teneinde zijn rechten uit te oefenen.
4. De verantwoordelijkheid voor het afhandelen van het verzoek, het melden én monitoren van de termijnen, ligt in beginsel bij de Partij die het verzoek als eerste heeft ontvangen, tenzij deze partij niet de beoogde ontvanger is van het verzoek.
5. Ingeval een Partij niet de beoogde ontvanger van het verzoek is, dient deze binnen vijf werkdagen het verzoek door te sturen naar de beoogde ontvanger.
6. De Partijen informeren elkaar onverwijld over een ontvangen verzoek en beslissen binnen vijf werkdagen welke Partij het verzoek afhandelt.

Gegevensbeschermingseffectbeoordeling (DPIA)

1. Waar nodig voeren Partijen gezamenlijk een DPIA uit, conform de richtlijnen van de Autoriteit Persoonsgegevens.
2. Indien een partij zelfstandig een DPIA houdt op een (deel)verwerking die valt onder gezamenlijke verwerkingsverantwoordelijkheid, deelt deze de uitkomsten met de overige partijen.
3. De verwerkingen die onder gezamenlijke verantwoordelijkheid vallen, worden eenmaal per jaar door de Functionarissen Gegevensbescherming en/of privacy officers van de betrokken Partijen besproken en beoordeeld.

Beveiliging van persoonsgegevens

1. Partijen verklaren ten minste de verplichte maatregelen – zoals genoteerd in de Baseline Informatiebeveiliging Overheid - te hebben geïmplementeerd, tenzij uit een weloverwogen risicoanalyse blijkt dat een maatregel achterwege kon worden gelaten.
2. Partijen geven elkaar over en weer inzicht in de getroffen beveiligingsmaatregelen, met name in geval van afwijkende of niet-toereikende maatregelensets.

Verwerkers

1. Het inschakelen van een externe Verwerker door een Partij gebeurt alleen als dat (strikt) noodzakelijk is en in beginsel in overleg met de betrokken Verwerkingsverantwoordelijken. Die Partij sluit tevens een Verwerkersovereenkomst af, na instemming van de andere Partijen.

Datalekken

1. Onder inbreuk wordt verstaan:
    a. Verlies van persoonsgegevens
    b. Vernietiging van persoonsgegevens
    c. Wijziging van persoonsgegevens
    d. Ongeoorloofde verstrekking van persoonsgegevens
    e. Ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens
2. Ingeval van een datalek, draagt de partij die het eerst bekend is geworden met het incident de verantwoordelijkheid voor het informeren van de partijen.
3. Partijen verklaren elkaar binnen 24 uren te informeren én te beslissen welke partij de leiding neemt voor wat betreft de vereiste onderzoeken en handelingen ingeval van een datalek, waaronder:
    a. Juridisch, organisatorisch en technisch onderzoek;
    b. Primaire maatregelen die de inbreuk doen eindigen en/of de schade reduceren;
    c. De meldplicht richting de Autoriteit Persoonsgegevens.
4. De partijen verklaren elkaar alle mogelijke medewerking te verlenen én de binnen hun organisatie noodzakelijke maatregelen te treffen, teneinde de inbreuk te doen eindigen en/of de schade te reduceren.

Evaluaties

1. Partijen evalueren jaarlijks de bepalingen in deze verklaring en lichten elkander in over inbreuken, risicobeoordelingen, DPIA's en bevindingen.
2. Indien uit de evaluatie een verbeterpunt blijkt, bieden partijen elkaar een redelijke termijn het gebrek te herstellen.

Verantwoordelijkheid

Partijen zijn verantwoordelijk voor het nakomen van deze verklaring en kunnen elkaar daarop aanspreken.