Privacybeleidskader Gemeente Lansingerland 2019

Algemeen privacybeleid

Mei 2019
T19.05349

Inhoudsopgave

Definities

AVG (Algemene Verordening Gegevensbescherming) – Europese wet op de verwerking van persoonsgegevens, die rechtstreeks geldt in alle lidstaten.
Bedrijfsproces – gemeentelijke bedrijfsvoering waarbij persoonsgegevens worden verwerkt.
FG (Functionaris voor Gegevensbescherming) – wettelijk toezichthouder voor de naleving van privacywetgeving en bedrijfsvoorschriften
(Gegevens)verwerking – zowel geheel of gedeeltelijk geautomatiseerde operationele informatieverwerking (bijvoorbeeld archiveren, analyseren, doorgeven, raadplegen) als ieder geheel daarvan (bijvoorbeeld de salarisadministratie, gemeentebelastingen of thuiszorg).
Persoonsgegevens – gegevens over personen en waarvan de gegevensverwerking door herleidbaarheid gevolgen heeft in de persoonlijke levenssfeer (privacy impact heeft).
PIA (privacy impact assessment) – een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico's vanuit privacyoptiek, resulterend in een lijst van passende beheersmaatregelen (waarborgen)
Risicoscore – getalsmatige classificatie van mogelijke impact van een gegevensverwerking
PIT – het privacy- en informatiebeveiligingsteam dat het college en proceseigenaren ondersteunt
Portefeuillehouder privacy – het lid van het college van B&W dat verantwoordelijk is voor de uitvoering en naleving van privacywetgeving met behulp van het privacybeleidskader
Privacybeleidskader - het algemeen privacybeleid van een organisatie
Privacy-audit – controles op de naleving van privacybeleid en privacywetgeving
Privacybeleid - het privacybeleidskader en alle nadere uitwerkingen hiervan
Privacybeleidsvoering – sturing op privacy door het management ('governance')
Privacy-incidenten – incidenten waarbij een onrechtmatige gegevensverwerking plaatsvindt.
Privacywetgeving – wetgeving die verwerking van persoonsgegevens regelt, in het bijzonder de AVG.
Procesdoel – een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens
Proceseigenaren – lijnmanagers i.c. de afdelingshoofden die verantwoordelijk zijn voor uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen en veiligheid.
Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een PIA)
Privacy officer – degene die namens de portefeuillehouder privacy uitvoering geeft aan het privacybeleid.
Servicepunt – het contactpunt voor personen waar zij terecht kunnen voor het uitoefenen van hun privacyrechten.

1 Privacymanagement

1.1 Inleiding

Het Privacybeleidskader Gemeente Lansingerland 2018 biedt een kader voor het vormgeven van privacybeheersmaatregelen. Naast een procesbeschrijving voor privacyborging oftewel privacymanagement, beschrijft dit document het generieke deel van de benodigde maatregelen. Dit betreft de maatregelen die moeten worden genomen door de eindverantwoordelijke binnen de gemeentelijke organisatie, het college van B&W. Het privacybeleidskader dient te worden aangevuld met specifieke beheersmaatregelen die horen bij de afzonderlijke werkprocessen.

1.2 Doel

Het doel van dit beleidskader is ervoor te zorgen dat Gemeente Lansingerland de privacywetgeving naleeft. Dit betekent concreet dat persoonsgegevens rechtmatig, behoorlijk en transparant worden verwerkt.

1.3 Voor wie?

Het Privacybeleidskader Gemeente Lansingerland bevat in aanvulling op algemene uitgangspunten voor privacymanagement, afspraken tussen het college, de proceseigenaren, de privacy officer en de Functionaris Gegevensbescherming. De afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens worden gebruikt, opgeslagen of uitgewisseld (‘verwerking van persoonsgegevens’).

1.4 Visie

Gemeente Lansingerland ziet de bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. Het streven is gericht op het veilig uitwisselen en delen van persoonsgegevens wanneer dit wenselijk, nuttig en noodzakelijk is. Inwoners en medewerkers moeten erop kunnen vertrouwen dat persoonsgegevens rechtmatig, zorgvuldig en veilig worden verwerkt. Het college van B&W schept de voorwaarden voor een privacy bewuste organisatiecultuur en voert in dat kader adequaat privacybeleid. We zijn transparant over onze gegevensverwerking en de manier waarop wij persoonsgegevens beschermen. Bij dilemma’s met betrekking tot de verwerking van persoonsgegevens gaan wij de dialoog met betrokkenen aan en zoeken waar mogelijk gezamenlijk naar oplossingen.

1.5 Uitgangspunten

Binnen Gemeente Lansingerland is het college eindverantwoordelijk voor het zorgvuldig en verantwoord omgaan met de persoonsgegevens die door burgers, medewerkers en derden aan de organisatie zijn toevertrouwd. Hierbij gelden de volgende uitgangspunten:

College van B&W

1) Het college voorziet in een team van professionals dat het college en de proceseigenaren ((de teammanagers) ondersteunt in de privacybeleidsvoering.
2) Het college faciliteert bewustwording en training op het gebied van privacy voor alle medewerkers.
3) Gemeente Lansingerland beschikt over mechanismen voor privacy-incidentmanagement. Deze maken onderdeel uit van een incidentprotocol (T17.37881).
4) Het college houdt een register van de gegevensverwerkingen bij die onder zijn verantwoordelijkheid plaatsvindt zoals bedoeld in artikel 30 Algemene Verordening Gegevensbescherming (AVG).
5) Het college is verantwoordelijk voor de naleving van de privacywetgeving en voert proactief privacybeleid dat past binnen dit beleidskader.
6) Het college brengt het onderwerp Privacy en Informatiebeveiliging onder in de planning en control-cyclus van Gemeente Lansingerland.

7) Het college kan uitleg geven (maatschappelijk en juridisch) over privacybeleidsvoering en beheersmaatregelen en zorgt daarom voor een goede documentatie.
8) Het college ziet erop toe dat informatieveiligheid van Gemeente Lansingerland in lijn met de geldende norm wordt georganiseerd en maakt daartoe onder andere gebruik van de ambtseed en daar waar nodig (d.w.z. indien het risicovolle informatie betreft) andere geheimhoudingsvoorschriften die door medewerkers dienen te worden ondertekend.
9) Het college informeert de raad over de privacybeleidsvoering.
10) Het college heeft een FG aangewezen die toeziet op de naleving van privacywetgeving.
11) Het college evalueert tweejaarlijks de actualiteit en doeltreffendheid van dit beleidskader.

Proceseigenaren (Teammanagers)

1) Proceseigenaren zijn verantwoordelijk voor (een of meer) primaire of ondersteunende processen en houden daar regie en toezicht over.
2) Een proceseigenaar is verantwoordelijk voor de procesinrichting – waaronder met name het vaststellen van passende privacy maatregelen – van het aan hem toegewezen proces.
3) Als in een proces persoonsgegevens worden verwerkt zorgt een proceseigenaar voor een procesplan met daarin een privacy-analyse en benodigde privacymaatregelen. Hij evalueert deze periodiek.
4) Een proceseigenaar ziet erop toe dat binnen een proces alleen persoonsgegevens worden verwerkt die nodig zijn voor het realiseren van het doel van het proces.
5) Proceseigenaren zorgen voor passende waarborgen in geval van verwerking van gegevens voor verenigbare doelen zoals het genereren van managementinformatie. Ook wordt in afstemming met het Privacy en Informatiebeveiligings Team (PIT) voorzien in met passende waarborgen omklede oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.
6) Een proceseigenaar ziet erop toe dat er binnen een proces alleen persoonsgegevens worden verwerkt die - gezien het doel van de verwerking - rechtmatig zijn verkregen.
7) In het procesplan beschrijft de proceseigenaar de garanties voor een eerlijke, veilige en betrouwbare verwerking van persoonsgegevens.
8) Bij privacy-incidenten hanteert de proceseigenaar de procedure melden datalekken (T17.37879).
9) Klachten en vragen over de gegevensverwerking behandelt de proceseigenaar in afstemming met de FG. Binnen vierweken wordt gereageerd op de vraag of klacht.
10) Proceseigenaren doen jaarlijks verslag aan het college van hun privacybeleid, oplossingen en incidenten die onder hun verantwoordelijkheid hebben voorgedaan met afschrift aan de FG.
11) Periodiek zorgt de proceseigenaar dat een audit (zie hoofdstuk 7: Audit) wordt uitgevoerd op privacyborging in processen met hoge privacyrisico's. Hierbij wordt ook het procesplan betrokken.

1.6 Scope

Dit privacybeleidskader kent de volgende scope:

- Het Privacybeleidskader Gemeente Lansingerland is van toepassing op alle bedrijfsvoering van gemeente Lansingerland voor zover hierbij gewerkt wordt met persoonsgegevens en de gemeente daar zeggenschap over heeft.

- Het Privacybeleidskader Gemeente Lansingerland bevat generieke privacy beginselen voor de verwerkingen die de gemeente uitvoert. Het privacybeleidskader is de kapstok voor de vormgeving van proces gebonden privacybeleid, dat in procesplannen wordt uitgewerkt. Daarnaast biedt het uitgangspunten voor gemeentebrede regelingen zoals een procedure voor het faciliteren van privacyrechten.

- Het privacybeleid Gemeente Lansingerland omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil.

- De raad is verantwoordelijk voor het functioneren van de griffie. Ook de griffie verwerkt persoonsgegevens, bijvoorbeeld bij ingekomen brieven die aan de raad zijn gericht. Dit Privacybeleidskader is daarom ook van toepassing op de griffie. De griffier is in dit kader te beschouwen als proceseigenaar.

- Het privacybeleid Gemeente Lansingerland is van toepassing op processen die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert, zoals deelname in een rechtspersoon die voor Gemeente Lansingerland informatiediensten verricht.

- Het privacybeleid Gemeente Lansingerland is van toepassing op gegevensuitwisseling met derden zoals de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders.

- Het privacybeleid omvat de gehele 'data life cycle': van het genereren of verzamelen van gegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.

- Het privacybeleid is van toepassing op de verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

- Het privacybeleid is van toepassing op informatieveiligheidsproblemen.

1.7 Raakvlakken en overlap met andere beleidsthema's

Privacybeleid heeft raakvlakken met verschillende andere beleidsthema's en dient daarom meerdere doelen dan alleen privacycompliance.

Integriteitsbeleid
Privacybeleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid.

Kwaliteitsbeleid
Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteit- en risicomanagement
Privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement omdat privacybeleid afbreuk- en aansprakelijkheidsrisico's tegengaat en voorkomt dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerking een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad).

Informatiebeveiliging
Privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacyincidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens.

Personeel en organisatie
Het sturen op professionaliteit en betrouwbaarheid van personeel, cultuur en organisatie wordt uitgevoerd vanuit het P&O beleid. Privacy heeft als belangrijk uitgangspunt het bevorderen van een bewuste omgang met persoonsgegevens binnen heel de organisatie, waarmee eveneens een beroep wordt gedaan op professionaliteit.

Communicatie
Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het communicatiebeleid. Vanuit privacywetgeving is het verplicht om transparant te zijn over het inwinnen en gebruiken van

persoonsgegevens, dat betekent dat zowel privacybeleid als communicatiebeleid een duidelijk georganiseerde informatievoorziening nastreven.

2 Privacygovernance

In dit hoofdstuk wordt het proces van privacygovernance met de bijbehorende rollen beschreven. Daarmee wordt geduid hoe er binnen Gemeente Lansingerland gestuurd wordt op het borgen van privacy.

2.1 Rollen

De wet wijst het college aan als de probleemeigenaar van privacybeleidsvoering, maar het college zal op zijn beurt verantwoordelijkheden aan anderen moeten opdragen. Ook op lager niveau dienen rollen en verantwoordelijkheden duidelijk te zijn, en zijn er afspraken nodig over het afleggen van interne verantwoording. Uiteindelijk is iedereen op zijn eigen manier mee verantwoordelijk voor geslaagde privacybeleidsvoering. Het college blijft in alle gevallen eindverantwoordelijk voor de verwerkingen van gegevens van zowel burgers, medewerkers als derden, en voor de vereiste privacyborging op organisatieniveau.

Een 'RASCI-tabel' helpt om rollen en verantwoordelijk rond privacyborging inzichtelijk te maken:[1]

RASCI	Vertaald naar privacy	Concreet
R **Responsible**	Feitelijk verantwoordelijk	**1e lijn** • Proceseigenaren (teammanagers, griffier) • Medewerkers • Ketenpartners bij inkoop/outsourcing (zoals gemeenschappelijke regelingen)
A **Accountable**	Eindverantwoordelijk	**1e lijn** • College van B&W (portefeuillehouder)
S **Supportive**	Ondersteunend	**2e lijn** • Informatieadviseurs • Beveiligingsbeheerders • Juristen • Kwaliteitsmanagers • Privacy officer
C **Consulted (hier: controlerend)**	Toezicht	**3e lijn/4e lijn (intern/extern)** • Functionaris Gegevensbescherming • Auditor • Accountant • Controller
I **Informed**	Geïnformeerd	**5e lijn** • Inwoners • Medewerkers • Gemeenteraad • Autoriteit Persoonsgegevens[2]

[1] RASCI staat voor Responsible, Accountable, Supporting, Consulted (hier tegelijkertijd: Controlerend) en Informed.

[2] De AP hoort óók thuis bij 'controlerend' maar komt door aanwijzing van een FG meer op afstand te staan.

2.2 Managementstructuur

Het college is verantwoordelijk voor het voorzien in passende privacywaarborgen bij de uitvoering van gemeentelijke taken. Daarbij doet zij een beroep op diverse rollen die binnen Gemeente Lansingerland aan medewerkers zijn toegewezen.

Portefeuillehouder privacy
Privacy valt onder de verantwoordelijkheid van het college van B&W, en wordt gemandateerd aan de wethouder die voor informatiemanagement verantwoordelijk is. Deze wethouder neemt de rol van portefeuillehouder privacy op zich.

Proceseigenaren
Voor ieder primair of ondersteunend proces binnen Gemeente Lansingerland is een proceseigenaar aangewezen die zorgdraagt voor de vormgeving, uitvoering en monitoring van privacybeheersmaatregelen voor het toegewezen werkproces en die aanspreekbaar is op het effectief waarborgen van privacy in het betreffende verwerkingsproces. Een proceseigenaar kan één of meerdere processen toegewezen krijgen.

In het geval dat een verwerkingsproces onder verantwoordelijkheid zou vallen van meerdere proceseigenaren heeft de domeindirecteur de rol van proceseigenaar. Hij/zij kan ook een proceseigenaar aanwijzen voor het gezamenlijke deel van de gegevensverwerking.

Zie voor een nadere toelichting van de rolinvulling van de proceseigenaar paragraaf 2.3.

Privacy officer
De privacy officer zorgt voor de beleidsvorming en beleidsbewaking op het thema privacy en is binnen Gemeente Lansingerland adviseur op het gebied van privacyvraagstukken. De privacy officer wordt functioneel aangestuurd door de teammanager. Zie verder paragraaf 2.4.

Interne toezichthouder
Het college wijst een wettelijk verplichte Functionaris voor de Gegevensbescherming (FG) aan als interne toezichthouder op de uitvoering van privacybeleid en als adviseur bij voorkomende privacyvraagstukken. Zie verder paragraaf 2.5.

Privacy en Informatieveiligheidsteam (PIT)
Ter ondersteuning van de privacy officer wordt een Privacy- & Informatieveiligheidsteam (PIT) samengesteld. Het PIT wordt samengesteld met professionals op het gebied van bijvoorbeeld (privacy-) juridische zaken, informatiebeveiliging, informatiemanagement, audit en communicatie. Het PIT adviseert en ondersteunt proceseigenaren bij het vormgeven en implementeren van privacybeheersmaatregelen.

Informatiebeveiligingsfunctionaris
Vanuit de informatiebeveiliging (IB) ondersteunt een informatiebeveiligingsfunctionaris (Chief Information Security Officer de zgn. CISO) het primaire proces. Hij houdt toezicht en adviseert het college, proceseigenaren en medewerkers op het gebied van de informatiebeveiliging. Daarvoor heeft hij de juiste kennis en kunde op het gebied van IB, en waar nodig aangevuld met trainingen en certificaten.

De CISO speelt een belangrijke rol in de totstandkoming van informatiebeveiligings-beleid, de implementatie en evaluatie daarvan. Daarnaast geeft hij advies over uiteenlopende vraagstukken op het gebied van informatiebeveiliging en voert hij periodiek beveiligingsaudits uit. De CISO werkt nauw samen met de privacy officer en de FG en maakt deel uit van het PIT.

2.3 De proceseigenaar

Proceseigenaren zijn ervoor verantwoordelijk dat de gemeentelijke taakuitoefening waarvoor zij verantwoordelijk zijn, binnen de grenzen van dit privacybeleidskader plaatsvindt en rapporteren over dit laatste aan het college.

- Er is per werkproces één proceseigenaar aangewezen die verantwoordelijk is voor een privacy conforme inrichting van het proces, die de betreffende documentatie vastlegt in een procesplan, zorgdraagt voor de uitvoering van daarin beschreven privacybeheersmaatregelen en die hierover verantwoording afdraagt aan het college van B&W.
- Het college blijft eindverantwoordelijk voor de privacybestendigheid van processen als de 'verwerkingsverantwoordelijke' in de zin van de AVG, met dien verstande dat de raad de verantwoordelijke is voor het functioneren van de griffie.

Regie en toezicht
Proceseigenaren voeren regie over hun proces(sen) op basis van procesplannen (zie hierna in hoofdstuk 4.1) die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een procesplan dient te passen binnen dit privacybeleidskader en is steeds in overeenstemming met de feitelijke situatie.

Een proceseigenaar houdt proactief toezicht op de privacybestendige organisatie van zijn proces en documenteert keuzes en oplossingen als bijlagen van het procesplan.

Mandatering
Een proceseigenaar kan proceseigenaarschap mandateren aan een subproceseigenaar binnen de gemeente. Bij mandatering blijft de opdrachtgevende proceseigenaar verantwoordelijk voor de privacybestendigheid van de aanpak door de subproceseigenaar.

Uitbesteding
Een proceseigenaar kan proceseigenaarschap mandateren aan een partij buiten de gemeentelijke organisatie mits deze voldoen aan de vereisten voor gegevensbescherming die voor het proces gelden. Het mandaat kan blijken uit een inkoopcontract, de deelname in een gemeenschappelijke regeling of gebruikmaking van een landelijke voorziening. Bij externe ketensamenwerking blijft de opdrachtgevende proceseigenaar namens het college verantwoordelijk voor de privacybestendigheid van de aanpak door hem ingeschakelde ketenpartner(s) en houdt hierop toezicht. De wet kan dwingende bepalingen bevatten over wederzijdse verantwoordelijkheden bij ketensamenwerking.

2.4 Coördinatie

De privacy officer is de rechterhand van de portefeuillehouder privacy en ontwikkelt en bewaakt het privacybeleid. Daarnaast geeft hij/zij samen met het PIT advies aan de proceseigenaren over een privacybestendige uitvoering van de processen. In hoofdlijnen is hij/zij belast met de volgende taken:

- Ondersteunen bij privacy-analyses waaronder het aanwijzen van passende beheersmaatregelen
- Ontwikkelen van toegepast privacybeleid en -procedures
- Inschakelen van deskundigen (intern/extern)
- Stimuleren van bewustwording en training van medewerkers van Gemeente Lansingerland
- Opstellen van een werkprogramma/ jaarplan met betrekking tot privacy
- Monitoren en rapporteren over de uitvoering van het beleid en het werkprogramma
- Evalueren van het privacybeleidskader en doen van aanbevelingen over wijzigingen ten aanzien daarvan aan het college.

De privacy officer is (juridisch) privacyspecialist te zijn en dient daarbij voldoende affiniteit en basiskennis van privacy (-management) te hebben om zijn rol te kunnen vervullen en ondersteuning te bieden aan de vakteams.

2.5 Interne toezichthouder

De Functionaris voor Gegevensbescherming (FG) is de interne toezichthouder van Gemeente Lansingerland op naleving van privacywetgeving conform artikel 37-39 AVG. Het college informeert interne en externe doelgroepen over de FG en communiceert zijn contactgegevens aan de Autoriteit Persoonsgegevens.

De FG wordt aangewezen op grond van: (a) zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de privacy management-praktijk; (b) zijn vermogen om de onderstaande taken te vervullen en (c) zijn onafhankelijkheid – met name de afwezigheid van belangenconflict.

Taken
De FG:
- informeert en adviseert het college, proceseigenaren en het PIT over de werking van het privacybeleid van Gemeente Lansingerland en nakoming van achterliggende wettelijke verplichtingen (heeft de lead in interpretatie van privacywetgeving);
- houdt toezicht op de nakoming van het privacybeleid en achterliggende wettelijke verplichtingen;
- helpt privacyklachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacyincidenten over ernst en omvang;
- beheert het Privacybeleidskader Gemeente Lansingerland;
- ziet toe op het beheer door het college van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door Gemeente Lansingerland en ketenpartners, eventueel ook in samenwerking met auditors;
- helpt het privacybeleid uit te dragen bij interne en externe doelgroepen;
- is het contactpunt voor privacytoezichthouders zoals de Autoriteit Persoonsgegevens.
- De FG doet jaarlijks verslag van zijn werkzaamheden aan het college van B&W.

Kaders
De FG krijgt de nodige ruimte voor professionele uitvoering van taken.
- Het college en proceseigenaren zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens;
- De FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen Gemeente Lansingerland waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan;
- Het college en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek;
- De FG mag niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, gestraft of ontslagen.
- De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van privacywetgeving door de gemeente, onverminderd de opvattingen van landelijke toezichthouders.

3 Privacycompliance

In dit hoofdstuk wordt de grondslag van de gegevensverwerking binnen Gemeente Lansingerland verhelderd.

3.1 Algemeen

Gemeente Lansingerland is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden:

- voert Gemeente Lansingerland proactief privacybeleid op basis van dit privacybeleidskader;
- faciliteert Gemeente Lansingerland de uitoefening van rechten van personen;
- bewaakt Gemeente Lansingerland de goede nakoming van wet- en regelgeving op het gebied van privacybescherming.

3.2 Noodzakelijke gegevensverwerking

Proceseigenaren verwerken persoonsgegevens uitsluitend voor gespecificeerde doeleinden die een rechtmatige grondslag hebben in de wetgeving, voor zover dit valt binnen hun mandaat en noodzakelijk of gewenst is. Afhankelijk van de situatie kan sprake zijn van verschillende grondslagen van gegevensverwerking:

1. de uitoefening van publieke taken;
2. de nakoming van wettelijke plichten;
3. de vrijwaring van vitale belangen voor de betrokkene(n);
4. de totstandkoming of uitvoering van een overeenkomst waarbij een betrokkene partij is;
5. de behartiging van een gerechtvaardigd belang van Gemeente Lansingerland of een derde aan wie gegevens worden verstrekt tenzij het recht op de bescherming van de persoonlijke levenssfeer prevaleert.

3.3 Kapstokregeling

Dit Privacybeleidskader Gemeente Lansingerland heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten. Proceseigenaren geven door middel van procesplannen met privacybeheersmaatregelen nadere invulling aan dit privacybeleidskader, waarbij ze ondersteund worden door de privacy officer en de FG. De genoemde rollen worden in hoofdstuk 2 nader besproken.

Procesplannen geven een beschrijving van werkprocessen, van de bijbehorende gegevensverwerking en van de privacywaarborgen waarmee de werkprocessen omkleed zijn, zodat een privacybestendige aanpak ontstaat. Procesplannen zijn aan de orde voor ieder gemeentelijk werkproces waarbinnen persoonsgegevens worden verwerkt. Hierbij wordt gekozen voor een onderverdeling van verwerkingen in de volgende primaire processen:

- veiligheid en openbare orde
- maatschappelijke opvang
- jeugd en onderwijs
- maatschappelijke ondersteuning
- gemeentelijke belastingheffing
- werk en inkomen
- HRM
- leefomgeving
- milieu en duurzaamheid
- ruimte en bereikbaarheid
- lokale economie

- cultuur en sport

Het privacybeleidskader, de procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid Gemeente Lansingerland. Voorliggend privacybeleidskader is daarbij leidend.

3.4 Inachtneming bijzondere wettelijke voorschriften

Met de vaststelling van het Privacybeleidskader Gemeente Lansingerland geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming die vereist dat er privacybeleid wordt vastgesteld om te borgen dat er overeenkomstig de wet wordt gewerkt. Van belang om te weten is, dat er naast de AVG bijzondere wettelijke voorschriften bestaan waarmee rekening moet worden gehouden – met name privacy-relevante bepalingen in de Wet basisregistratie personen, de Telecommunicatiewet, de Participatiewet, de Jeugdwet, de Wet maatschappelijke ondersteuning en de Wet gemeentelijke schuldhulpverlening.

4 Procesplan-aanpak

Dit hoofdstuk beschrijft de werkwijze die gevolgd dient te worden om privacybestendige werkprocessen te realiseren en te garanderen.

4.1 Rol van proceseigenaren

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support door het PIT en de FG. Het college spant zich in om proceseigenaren hierbij van de nodige randvoorwaarden te voorzien, teneinde binnen Gemeente Lansingerland een privacybestendige cultuur te realiseren.

Proceseigenaren zorgen voor passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen ('privacywaarborgen') en documenteren die maatregelen in procesplannen.

De privacy officer zorgt voor het bijhouden van een 'artikel 30-register' (zie §4.4) bij van de gegevensverwerkingen die onder de eindverantwoordelijkheid van het college vallen. Proceseigenaren helpen om het register volledig en actueel te laten zijn door middel van 'artikel 30-formulieren', waarmee de vereiste kenmerken voor het register kunnen worden aangeleverd en zo nodig geactualiseerd.

Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeente gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking, door benodigde gegevens die zij verwerken volgens de bestaande procedures beschikbaar te stellen.

Het college en proceseigenaren dragen het belang uit van privacybeleidsvoering en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt.

4.1 Inhoud procesplan

Iedere proceseigenaar is verantwoordelijk voor het opstellen van procesplannen voor de gegevensverwerkingen die plaatsvinden. In een procesplan staan de volgende onderwerpen gedocumenteerd:

1) Privacy-analyse/ PIA-rapport
2) Concrete privacybeheersmaatregelen
3) Kritische Prestatie Indicatoren (KPI's)
4) (eventueel:) FG-verklaring

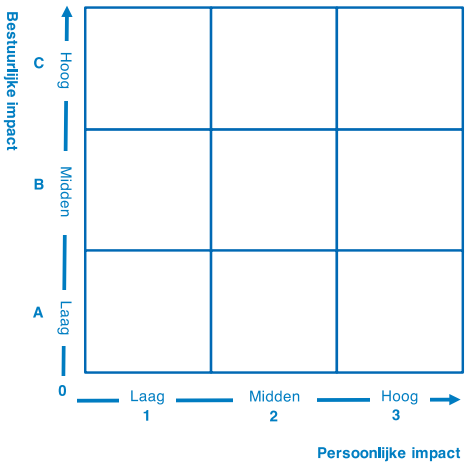
4.1.1 Ontwerp van het procesplan

Aan een procesplan ligt een eerste risico-inschatting, en vervolgens een privacy-analyse of PIA (Privacy Impact Assessment) ten grondslag.[3]

De privacy-analyse of PIA is instrumenteel voor het kunnen bepalen van passende beheersmaatregelen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de privacy-analyse of PIA.

[3] Een PIA dient volgens de AVG uitgevoerd te worden wanneer de verwerking een hoog risico voor de betrokkenen met zich meebrengt. Een PIA is een uitgebreide privacy-analyse waarbij de wet vormvereisten benoemd.

Voor het bieden van een volledig beeld hanteert Gemeente Lansingerland een systeem waarbij zowel mogelijke persoonlijke impact op betrokkenen als mogelijke bestuurlijke impact op de organisatie wordt ingeschat. Hoe hoger de geschatte impact, hoe robuuster de beheersmaatregelen (privacywaarborgen). Deze scores worden bepaald aan de hand van de hiernaast afgebeelde matrix. Proceseigenaren volgen het advies van het PIT bij de vaststelling van hun risico-score.



Proceseigenaren hanteren onderstaande tabel om te bepalen wat voor toets vooraf dient te gaan aan het opstellen van het procesplan zodat beheersmaatregelen kunnen worden verantwoord.

PIA-Score	Procesplan	Akkoord FG
A1	-	-
A2	Privacy-analyse maakt deel uit van procesplan	Aanbevolen
A3	PIA-rapport maakt deel uit van procesplan	Verplicht
B1	Privacy-analyse maakt deel uit van procesplan	Aanbevolen
B2	Privacy-analyse maakt deel uit van procesplan	Aanbevolen
B3	PIA-rapport maakt deel uit van procesplan	Verplicht
C1	PIA-rapport maakt deel uit van procesplan	Verplicht
C2	PIA-rapport maakt deel uit van procesplan	Verplicht
C3	PIA-rapport maakt deel uit van procesplan	Verplicht

PIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG, dat houdt in dat de volgende aspecten worden gedocumenteerd:

a) Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden (formuleer hierbij categorieën van betrokkenen en categorieën van persoonsgegevens zie bijlage 1);
b) Een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden;
c) Een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
d) De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van de persoonsgegevens te garanderen en om aan te tonen dat aan de privacywetgeving is voldaan.

Proceseigenaren leggen vast in hun procesplannen hoe zij op een praktische manier in passende organisatorische en technische privacybeschermende maatregelen voorzien – waarmee de volgende fouten zoveel mogelijk worden voorkomen:

1. **Illegale/onrechtmatige gegevensverwerking:** gebruik, opslag of uitwisseling van informatie is bij wet verboden (middels een rechtstreeks verbod of een beperking van het toegestane gebruik).
2. **Disproportionele gegevensverwerking:** gebruik, opslag of uitwisseling van informatie is (a) ontoereikend of juist overmatig of (b) het organisatiebelang bij de gegevensverwerking is onevenredig klein terwijl de impact op personen onevenredig nadelig kan zijn.
3. **Irrelevante gegevensverwerking:** de gebruikte, opslagen of uitgewisselde informatie dient geen bedrijfsdoel, doet niet ter zake of is verouderd.
4. **Onnauwkeurige gegevensverwerking:** de gebruikte, opgeslagen of uitgewisselde informatie is geen juiste weergave van de werkelijkheid.
5. **Onveilige gegevensverwerking:** de gebruikte, opslagen of uitgewisselde informatie dreigt te gemakkelijk toegankelijk te zijn voor onbevoegden, gemanipuleerd te worden of onbeschikbaar te zijn.
6. **Niet-inachtneming van bijzondere wettelijke voorschriften:** bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.[4]
7. **Onbewaakte gegevensverwerking:** de proceseigenaar verzuimt om te controleren of de privacywaarborgende maatregelen daadwerkelijk zijn geëffectueerd of te evalueren in hoeverre zijn procesplan bijstelling behoeft.

Voor A1-processen volstaan generieke oplossingen. Zolang een proces als A1 gekwalificeerd is, is daarvoor in mindere mate aandacht nodig. Het PIT publiceert ter informering van proceseigenaren een lijst van A1-processen.

De werkelijkheid dient in overeenstemming te zijn met het procesplan. Veranderingen in de bedrijfsvoering noodzaken tot aanpassing van procesplannen, waarvoor opnieuw een PIA nodig kan zijn.

4.1.2 Lijst van KPI's

Proceseigenaren vatten, in samenspraak met het PIT en zo nodig de FG, hun procesplannen samen in een lijst van kritische prestatie indicatoren (KPI's) voor sturingsdoeleinden en controle.

Risico-score	KPI's	Samenspraak PIT	Samenspraak FG
A1	-	-	-
A2	Ja	Ja	Aanbevolen
A3	Ja	Ja	Verplicht
B1	Ja	Ja	Aanbevolen
B2	Ja	Ja	Aanbevolen
B3	Ja	Ja	Verplicht
C1	Ja	Ja	Verplicht
C2	Ja	Ja	Verplicht
C3	Ja	Ja	Verplicht

Proceseigenaren nemen de lijst van KPI's op aan het einde van het procesplan.

4.1.3 FG-verklaring

Een evenwichtig procesplan beschrijft een behoorlijke en zorgvuldige aanpak, in overeenstemming met de wet. De FG bevestigt dit aan de hand van een verklaring waarbij hij eventueel ook aanbevelingen doet voor verdere optimalisering van de bedrijfsvoering. Dit is verplicht voor de PIA en aanbevolen voor de (beknoptere) privacy-analyse. Proceseigenaren nemen de afgegeven FG-verklaring op aan het einde van het procesplan.

[4] Niet-nakoming van: meldplichten, bijzondere regels voor internationaal gegevensverkeer, wettelijke termijnen, verplicht voorafgaand onderzoek AP, toestemmingsverplichtingen

4.1.4 Beheer procesplan

De proceseigenaar is verantwoordelijk voor het beheer van zijn procesplan. Een procesplan wordt bijgesteld als in de praktijk blijkt dat de maatregelen onvoldoende passend zijn naar aanleiding van klachten of incidenten.

Hoe dan ook evalueert de proceseigenaar een procesplan periodiek en vraagt zo nodig de FG om hierbij advies uit te brengen.

Risico-score	Evaluatie	Advies FG
A1	4 jaarlijks	-
A2	3 jaarlijks	Aanbevolen
A3	jaarlijks	Verplicht
B1	3 jaarlijks	Aanbevolen
B2	2 jaarlijks	Aanbevolen
B3	jaarlijks	Verplicht
C1	jaarlijks	Verplicht
C2	jaarlijks	Verplicht
C3	jaarlijks	Verplicht

4.2 Artikel 30-formulieren

Proceseigenaren vatten hun procesplan samen in een ‘artikel 30-formulier’ dat zij opnemen aan het begin van het procesplan en waarvan zij een afschrift verstrekken aan de privacy officer voor opname in het artikel 30-register. Proceseigenaren melden veranderingen voor het artikel 30-register onmiddellijk aan de hand van wijzigingsformulieren.

Artikel 30-formulieren bevatten de volgende informatie:

1) Een beschrijvende aanduiding (naam) van het proces en de bijbehorende gegevensverwerking.
2) De naam, contactgegevens en het mandaat van de proceseigenaar.
3) Indien van toepassing: de contactgegevens van degene die die proceseigenaar assisteert in privacy-aangelegenheden.
4) De risico-inschatting of PIA-score.
5) De (bedrijfs-)doelen die met het proces zijn gediend.
6) Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens.
7) De categorieën van ontvangers van de persoonsgegevens en, indien van toepassing, informatie over internationaal gegevensverkeer.
8) Informatie op hoofdlijnen over genomen beheersmaatregelen– met name termijnen voor gegevensvernietiging en de aanpak op het gebied van informatiebeveiliging.
9) De FG-verklaring, indien afgegeven.

5 Privacyrechten

Dit hoofdstuk beschrijft de privacy gerelateerde rechten van personen van wie gegevens worden verwerkt en de werkwijze die Gemeente Lansingerland volgt wanneer personen een beroep doen op hun rechten.

5.1 Rechten

Personen hebben er onder meer recht op:
- dat Gemeente Lansingerland conform het voorliggende privacybeleidskader handelt;
- dat Gemeente Lansingerland de contactgegevens van de FG bekend maakt;
- dat Gemeente Lansingerland informatie verschaft over doelen van informatieverwerking en privacybeleidsvoering;
- dat zij inzage in hun *eigen* gegevens hebben[5];
- dat zij – in geval van fouten – hun gegevens kunnen (laten) rectificeren of verwijderen;
- om tegen het gebruik van hun gegevens verzet aan te tekenen, wat Gemeente Lansingerland verplicht tot het kenbaar maken van een afweging;
- dat zij Gemeente Lansingerland bij niet-naleving van het gemeentelijk privacybeleid (of de wet) hierop mogen aanspreken.

5.2 Vragen

Bij vragen:
- hebben personen het recht om zich te wenden tot hiervoor aangewezen servicepunt;
- vragen worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld;
- een servicepunt kan het PIT om advies over de beantwoording vragen;
- een niet tot tevredenheid afgehandelde vraag geeft personen het recht om zich opnieuw te wenden tot een servicepunt. Het servicepunt registreert in dat geval de vraag als een klacht.

5.3 Klachten

Bij klachten:
- hebben personen het recht om zich te wenden tot de klachten coördinator;
- volgen we de geldende informele en formele klachtenprocedure zoals beschreven in de Klachtenregeling Lansingerland 2016;
- meldt de klachtencoördinator de klacht onmiddellijk bij de FG, CISO en privacy officer;
- kan een klager kan zich vervolgens nog wenden tot de FG wanneer hij ontevreden is over de afhandeling van zijn klacht;
- onderzoekt de FG vervolgens de gegrondheid van de klacht, waarbij hij met name nagaat of de klacht betrekking heeft op de naleving van privacywetgeving en/of het privacybeleid van de Gemeente Lansingerland.
- vormt de FG vormt zich een onafhankelijk oordeel over de afhandeling van de klacht en neemt de FG een formeel besluit;
- fungeert het PIT gedurende het gehele proces als advies instantie voor de betreffende klachtbehandelaar;
- klachten worden zo snel mogelijk maar uiterlijk binnen vier weken afgehandeld.

5.4 Beroep

Personen hebben het recht om na afhandeling van een klacht conform 5.3, zich – naar keuze - te wenden tot de Nationale ombudsman of de Autoriteit Persoonsgegevens wanneer zij niet tevreden zijn over de afhandeling van de klacht.

---

[5] Voor het afhandelen van verzoeken om inzage, verbetering, verwijdering en dergelijke stelt de AVG een termijn van één maand, met de mogelijkheid tot een verlenging van nog eens twee maanden in het geval van veel of complexe verzoeken.

6 Auditbeleid

Dit hoofdstuk gaat in op de toetsing (audit) van het functioneren van privacybeleid.

Vragen, klachten en het incident management zijn in wezen steekproefsgewijze toetsing van de privacybeleidsvoering. Om niet voor verrassingen te worden geplaatst, is het zaak dat proceseigenaren ook zelf periodiek (laten) controleren in hoeverre beleidsvoering en feitelijke situatie met elkaar overeenstemmen aan de hand van privacyaudits op de adequaatheid van de procesbeschrijving en op het functioneren van de vastgestelde beheersmaatregelen.

Zie het onderstaande schema voor de benodigde zwaarte en frequentie van privacyaudits.

- Quick scan is een beknopte toets onder de verantwoordelijkheid van de proceseigenaar.
- Zelfevaluatie is een uitgebreidere toets onder de verantwoordelijkheid van de proceseigenaar.
- Externe audit is een audit die de proceseigenaar organiseert in samenwerking met de FG en waarbij eventueel een professionele auditor wordt betrokken.

Wanneer wordt aangegeven dat de betrokkenheid van de FG aanbevolen of verplicht is, is het raadzaam om hem van begin af aan te betrekken in het audittraject. Maar bij verplichte betrokkenheid dient hij in ieder geval medeontvanger te zijn van het auditrapport.

	Type audit	**Frequentie**	**Betrokkenheid FG**	**Afschrift FG**
A1	Quick scan	5 jaarlijks	-	-
A2	Zelfevaluatie	4 jaarlijks	vrijwillig	vrijwillig
A3	Externe audit	3 jaarlijks	ja	ja
B1	Zelfevaluatie	5 jaarlijks	vrijwillig	ja
B2	Zelfevaluatie	4 jaarlijks	ja	ja
B3	Externe audit	3 jaarlijks	ja	ja
C1	Externe audit	4 jaarlijks	ja	ja
C2	Externe audit	3 jaarlijks	ja	ja
C3	Externe audit	2 jaarlijks	ja	ja

7 Invoering privacybeleid

Dit hoofdstuk beschrijft de te volgen aanpak bij het implementeren en beheren van privacybeheersmaatregelen in de organisatie.

7.1 Doel

Gemeente Lansingerland heeft de ambitie om uiterlijk vanaf mei 2018 te voldoen aan de vereisten zoals geformuleerd in de Algemene Verordening Gegevensbescherming. Daarbij heeft de gemeente zich ook ten doel gesteld een privacy-volwassenheid te bereiken op het niveau 'Gemanaged'. De benodigde stappen die de gemeente vanaf haar huidige niveau 'Ad hoc' moet doorlopen worden gestructureerd door middel van het invoeren van voorliggend privacybeleidskader.

Privacy maturity ladder		
Niveau		**Kenmerken**
5	Optimaliserend	De organisatie heeft een privacybeleid dat zich kenmerkt door vanzelfsprekendheid, natuurlijke samenwerking en anticipatie. Optimalisering van maatregelen is een continu proces. De organisatie heeft structureel middelen (mensen, budget) toegewezen om de privacydoeleinden van de organisatie te verwezenlijken. Verschillende afdelingen en functies werken samen om privacy en bescherming persoonsgegevens te verbeteren.
4	Gemanaged	De organisatie beschikt over een privacy control framework met bijbehorende doelen. Er is een hoog bewustzijn op de werkvloer met betrekking tot het belang van privacy en bescherming van persoonsgegevens (o.a. periodieke privacytraining), privacyrisico's worden al in een vroeg stadium van projecten geïdentificeerd en geadresseerd. Bijsturing vindt plaats op basis van periodieke evaluaties (PDCA).
3	Afgebakend	De organisatie beschikt over een privacybeleid en heeft de organisatie daarop ingericht. Het management stelt prioriteiten op het gebied van privacy en bescherming van persoonsgegevens en stelt daar middelen voor beschikking. Processen die het meest in het oog springen worden onderworpen aan privacy impact assessments en security risk assessments en voorzien van de nodige beheersmaatregelen.
2	Herhaalbaar	De organisatie beschikt over een privacybeleid. Er is een algemeen bewustzijn op de werkvloer over het belang van privacy en bescherming van persoonsgegevens, maar het management stuurt niet op dit vlak. Er zijn specifieke maatregelen/plannen op gebieden met hoge risico's.
1	Ad hoc	Beleid, regels of procedures ontbreken. Maatregelen staan op zichzelf, worden vaak ingegeven door operationele vraagstukken en zijn niet noodzakelijk toereikend. Consistentie en coördinatie ontbreekt, waardoor er soms dubbel werk wordt gedaan. Vereiste maatregelen ontbreken vaak door gebrek aan awareness en kennis.
0	Nalatig	Privacy leeft niet. De wet wordt genegeerd. Privacywaarborgen zijn afwezig.

7.2 Werkprogramma

Het college stelt jaarlijks het werkprogramma privacybeleidsvoering vast, mede op basis van de jaarrapportage van de FG en de aanbevelingen die hij hierin doet. Het werkprogramma bevordert opzet, bestaan en werking van passende waarborgen voor de bescherming van persoonsgegevens binnen de kaders van het privacybeleid Gemeente Lansingerland, ter uitvoering van de wet. Het werkprogramma is met name gericht op het realiseren en in stand houden van een privacybestendige bedrijfscultuur binnen Gemeente Lansingerland, met gebruikmaking van overige instrumenten zoals:

- Besluitvorming;

- Training en bewustwording;
- Ontwikkelen generieke procedures;
- Waarborgen actualiteit procesplannen;
- Privacymanagement procedures.

8 Bijlage – Tabel privacyrelevantie

De verplichting tot privacybeleidsvoering van de proceseigenaar ontstaat bij privacyrelevantie van zijn proces. Van privacyrelevantie is sprake wanneer informatie wordt verwerkt volgens de typen 1 tot en met 9 in de onderstaande tabel – met uitzondering van anonieme gegevens (type 8).

Type gegevens	Beschrijving	Voorbeeld
Identificerende gegevens	Zoomen direct in op een individu.	Naam, portret-/pasfoto
Gepseudonimiseerde gegevens	Alle gegevens die niet identificerend zijn zonder aanvullende gegevens.	Zie hierna: attribuerende gegevens, bijzondere gegevens, procesgegevens, conditionele gegevens, geprofileerde gegevens, anonieme gegevens of desnoods cookies – zolang ze niet zonder onevenredige inspanningen gecombineerd kunnen worden tot identificerende gegevens. Dit is met name het geval bij een deugdelijke 'privacy by design'-aanpak.
Attribuerende gegevens	Beschrijven eigenschappen van een persoon.	Leeftijd, geslacht, beroep, adresinformatie, dossierinformatie, locatiegegevens – zie ook bijzondere gegevens en geprofileerde gegevens
Bijzondere gegevens	Attribuerende gegevens die bij wet zijn aangemerkt als verhoogd privacygevoelig.	Gegevens over etniciteit, politieke opvattingen, levensbeschouwing, lidmaatschap van een vakbond, genetische of biometrische gegevens, gezondheidsgegevens, gegevens over seksueel gedrag of geaardheid, strafrechtelijke gegevens.
Procesgegevens	Helpen om nauwkeurige gegevensverwerking te waarborgen conform het juistheidsbeginsel in artikel 5 AVG.	Met name servicenummers zoals rekeningnummer, dossiernummer, klantnummer, personeelsnummer, BSN etc. Attribuerende gegevens zijn onder omstandigheden tevens procesgegevens. Denk bijvoorbeeld aan locatiegegevens en time stamps voor correcte berekening van parkeertarieven.
Conditionele gegevens	Zoomen niet in op een persoon tenzij daar een goede reden voor is (personalisering onder bijzondere condities).	Telefoonkostenbewaking, emailmonitoring, surfgedrag, beelden van bewakingscamera's – zie gepseudonimiseerde gegevens. Een conditie om te personaliseren is bijvoorbeeld fraudedetectie of detectie van veiligheid bedreigend gedrag in openbare ruimten ('crowd control').
Geprofileerde gegevens	Gegevens die door geautomatiseerde analyse inzicht bieden in persoonlijke kenmerken.	Profilering op iemands beroepsprestaties, economische situatie, gezondheidskenmerken, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen - zie attribuerende gegevens.
Anonieme gegevens	Gegevens die niet herleidbaar zijn tot individuen en daarom niet meer onder de privacywetgeving vallen.	Gegevens over groepen personen – bijvoorbeeld het aantal mensen dat van een dienst gebruik maakt of het aantal personeelsleden dat tevreden is over de werksituatie. Let op: bij kleine groepen (vuistregel: 8 personen of minder) is anonimiteit niet langer gewaarborgd en zijn de gegevens hooguit nog gepseudonimiseerd of zelfs direct al identificeerbaar.
Cookies	Gegevens over ICT-gebruik die de gebruiker bewust of onbewust op online randapparatuur opslaat, zoals op een smartphone, computer, tv of een met internet verbonden	Cookies voor vergroting van gebruiksgemak, verbetering van dienstverlening, profilering etc. Spelregels voor cookies zijn gebaseerd op bijzondere wetgeving (telecomrecht). Er is vrijwel altijd overlap met typen 1 t/m 8.

	navigatieapparaat.	