GEMEENTE Lansingerland

GEMEENTEBLAD

Officiële uitgave van de gemeente Lansingerland

Nr. 74526

20 februari 2024

Privacybeleid Gemeente Lansingerland

1 Introductie

1.1 Inleiding

Dit beleid schetst het kader om de privacybelangen van burgers van de gemeente Lansingerland (hierna: de gemeente) goed te borgen. Het beschermen van de privacy van onze bewoners en medewerkers is voor de gemeente een wettelijke plicht. Het College van Burgemeester en Wethouders (hierna: College van B&W), de gemeenteraad en de burgemeester zijn eindverantwoordelijk voor de juiste uitvoering van de Algemene Verordening Gegevensbescherming. Met dit beleid worden er concrete handvatten geboden om invulling te geven aan deze wettelijke plicht en wordt duidelijk hoe de gemeente omgaat met de persoonsgegevens die de gemeente verwerkt.

De gemeente heeft als publieke organisatie een bijzondere verantwoordelijkheid om de privacy van bewoners te waarborgen. Binnen de maatschappij heeft de gemeente een voorbeeldfunctie en werkt het vaak met gevoelige gegevens van bewoners. Gemeentelijke dienstverlening omvat verschillende services en interacties tussen een gemeente en haar inwoners, zoals het verstrekken van vergunningen, het verwerken van belastingen, het handhaven van de openbare orde en meer. In deze dienstverlening wordt veel persoonlijke informatie verwerkt, wat kan leiden tot een spanningsveld tussen het leveren van efficiënte en effectieve diensten en het beschermen van de privacy van individuen. Het navigeren van het spanningsveld tussen gemeentelijke dienstverlening en privacy is van vitaal belang om het evenwicht te bewaren tussen het bieden van essentiële diensten en het beschermen van de privacy van individuen. Doordacht privacybeleid stelt de gemeente in staat om zowel de behoeften van bewoners te dienen als te voldoen aan de wettelijke en ethische verplichtingen met betrekking tot de bescherming van persoonsgegevens.

1.2 Doel

Het doel van dit privacybeleid is om te beschrijven hoe de gemeente invulling geeft aan privacy management zodat de medewerkers van de gemeente begrijpen waarom privacy management nodig is en hoe ze dit vorm moeten geven.

Het doel van privacy management is vervolgens om het controleerbaar en aantoonbaar te maken hoe de gemeente het bovengenoemde spanningsveld navigeert en hoe daarmee aan de privacywetgeving wordt voldaan. Met adequaat privacy management wordt beoogd dat het proces van gegevensverwerking binnen de gemeente duidelijk en controleerbaar is. De gemeente kan zo privacy risico's beheersen. Dit betekent concreet dat persoonsgegevens (in het geval van de Algemene Verordening Gegevensbescherming) en politiegegevens (in het geval van de Wet Politiegegevens) rechtmatig, behoorlijk en transparant worden verwerkt. Een rechtmatige, behoorlijke en transparante verwerking betekent onder andere dat er een grondslag moet zijn waarop de gemeente de gegevens verzamelt en verwerkt, de verwerking noodzakelijk is om de doelen van de gemeente omtrent goede dienstverlening te bereiken én dat dit duidelijk naar de betrokkene moet worden gecommuniceerd. Dit rechtmatig, behoorlijk en transparant werken is gestoeld op de uitgangspunten van de gemeente Lansingerland om een sterke digitale dienstverlening te bieden en een transparante en open overheid te zijn.[1]

1.3 Scope

1.3.1 Voor wie?

Dit beleid is van toepassing op alle bestuurders, de gemeenteraad, en medewerkers van de gemeente Lansingerland, zowel intern als externe medewerkers en zowel in vaste als tijdelijke dienst.

1.3.2 Voor wat?

Het privacybeleid is van toepassing op alle processen en verwerkingen die plaatsvinden onder verantwoordelijkheid van de gemeente binnen de geldende wet- en regelgeving op het gebied van gegevensbescherming.

Onder dit privacybeleid vallen in ieder geval:

- Alle dienstverlening die de gemeente in het kader van haar publieke taak uitvoert waarbij persoonsgegevens worden verwerkt.

1) Zie hiervoor het coalitieakkoord van de gemeente Lansingerland: Samen Verantwoord Verder 2022 - 2026

- Alle bedrijfsvoering van gemeente Lansingerland voor zover hierbij gewerkt wordt met persoonsgegevens.
- Processen die de gemeente uitbesteedt, inkoopt of op een andere manier organiseert. Voorbeeld van een proces is het aanvragen van leerlingenvervoer.
- Gegevensuitwisseling met derden zoals de Belastingdienst, de Raad voor de Kinderbescherming, de politie en zorgaanbieders waar de gemeente verwerkersverantwoordelijke voor is.
- De samenwerkingsverbanden die de gemeente aangaat met externe partijen waarbinnen persoonsgegevens worden uitgewisseld.
- Het opslaan en archiveren van gegevens. Hier valt zowel papier als digitale opslag van gegevens onder.
- De gehele 'data life cycle': van het genereren of verzamelen van persoonsgegevens en politiegegevens, het dagelijkse gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan.
- De verwerking van statistische en/of geanonimiseerde gegevens, voor zover niet kan worden uitgesloten dat personen kunnen worden geïdentificeerd of geprofileerd.

1.3.3 Wettelijke context

Voor dit privacybeleid is de Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet Politiegegevens (Wpg) de voornaamste relevante wetgeving. Er is daarnaast andere relevante privacy- en materiewetgeving die de gemeente dient na te leven. Denk bijvoorbeeld aan de Wet basisregistratie personen, de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) en de Archiefwet. In deze wettelijke context wordt de meest bepalende wetgeving toegelicht: de AVG en de Wpg.

De AVG is een Europese verordening die het Europese grondrecht op de bescherming van persoonsgegevens uitwerkt. Regels voor de verzameling, verwerking en opslag van persoonsgegevens zijn hierin vastgelegd. Evenals de rechten van individuen met betrekking tot hun gegevens. De gemeente moet ervoor zorgen dat uitvoering wordt gedaan aan deze regelgeving.

De Wet Politiegegevens (hierna: Wpg) is een Nederlandse wet die specifiek van toepassing is op de verwerking van politiegegevens door politie, bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren (boa's). Politiegegevens zijn persoonsgegevens die verwerkt worden in het kader van een opsporingstaak. De Wpg stelt regels vast voor de verzameling, verwerking en uitwisseling van politiegegevens.

2 Privacymanagement model

2.1 Uitgangspunten

Om de balans te vinden tussen de doelstelling van de gemeente om de burger optimaal te ondersteunen én conform de geldende wet- en regelgeving op het gebied van privacy te werken, hanteert de gemeente een aantal uitgangspunten. Deze uitgangspunten helpen het bestuur, de directie, het management en de medewerkers om de balans te vinden in het spanningsveld tussen het leveren van efficiënte en effectieve diensten en het beschermen van de privacy van individuen.

Risico gebaseerd. De gemeente Lansingerland baseert de activiteiten en besluitvorming op een systematische en strategische beoordeling van risico's. Het doel is om de beschikbare middelen en inspanningen zo effectief mogelijk in te zetten op de gebieden met de grootste risico's, om zo effectiever en efficiënter te zijn in het bereiken van de gemeentelijke doelstellingen. De gemeente Lansingerland acteert niet op elk risico, maar maakt na een risicoanalyse een afweging welke risico's prioriteit hebben om op te pakken.

Continu verbeteren. De gemeente Lansingerland werkt volgens de PDCA-cyclus. PDCA staat voor plan, do, check, act. Dit houdt in dat de gemeente Lansingerland continu bezig is met verbeteren en het sturen op kwaliteitsmanagement. De PDCA-cyclus biedt een gestructureerde methode om processen te plannen, uit te voeren, te controleren en indien nodig aan te passen. Het werken met de PDCA-cyclus vereist betrokkenheid van alle relevante belanghebbenden en een cultuur van leren en verbeteren binnen alle lagen van de gemeente. Door systematisch gebruik te maken van de PDCA-cyclus kan de gemeente haar dienstverlening verbeteren, processen optimaliseren en beter inspelen op veranderende behoeften en uitdagingen.

Verantwoordelijk. Eindverantwoordelijk zijn de bestuursorganen voor de verwerkingen. De medewerkers zijn medeverantwoordelijk voor het naleven van relevante wet- en regelgeving, in dit geval de AVG en de Wpg. Medewerkers zijn verantwoordelijk om op de hoogte te zijn van de wettelijke kaders van gegevensverwerking en om daarbinnen te werken. Teammanagers stellen medewerkers in staat om deze verantwoordelijkheid te nemen en zijn verantwoordelijk om te toetsen en te borgen dat dit gebeurt. Alle processen en verwerkingen hebben één proceseigenaar binnen de gemeente. De primaire verant-

woordelijkheid voor privacy en het in kaart brengen van risico's binnen verwerkingen ligt bij de proceseigenaar (zie hoofdstuk 2.3.2).

Transparantie. De gemeente hanteert een open cultuur waarin risico's transparant zijn en bespreekbaar worden gemaakt. Daarnaast communiceert de gemeente open en eerlijk met haar inwoners en belanghebbenden over hoe persoonsgegevens worden verzameld, verwerkt en gebruikt. Dit principe speelt een cruciale rol voor de gemeente bij het opbouwen van vertrouwen richting de bewoners van de gemeente en het waarborgen van de privacy van individuen.

2.2 Het Three Lines model

Deze uitgangspunten implementeert de gemeente in haar bedrijfsvoering aan de hand van het Three Lines Model (oftewel het drie linies model). Het Three Lines Model is een organisatorisch raamwerk dat verantwoordelijkheden verdeelt tussen de eerste lijn (operationele afdelingen), tweede lijn (privacy en compliance) en derde lijn (Functionaris Gegevensbescherming (FG) en onafhankelijke audit). Het doel is het bevorderen van effectief risicomanagement, naleving van regelgeving en interne controle, waarbij elke lijn een specifieke rol speelt in het identificeren, beheersen en bewaken van risico's.

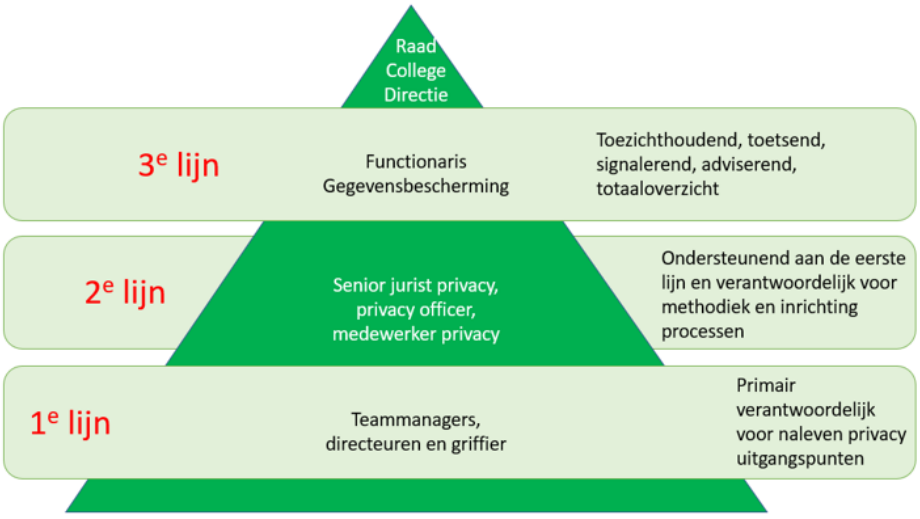
De eerste lijn, bestaande uit gemeentelijke diensten, identificeert en beheert dagelijkse privacy risico's bij gegevensverwerking. De tweede lijn, bestaande uit privacy medewerkers, bewaakt en ondersteunt de implementatie van privacybeleid en -normen. De derde lijn, de FG en onafhankelijke audit, evalueert onafhankelijk de doeltreffendheid van het privacymanagement:

1e Lijn: De teams zijn onder leiding van de teammanagers en directeuren Samenleving, Ruimte & Economie en Bedrijfsvoering integraal verantwoordelijk voor het naleven van de privacy uitgangspunten van de gemeente, zowel voor de AVG als de Wpg. De teams dienen zelf 'in control' (lees, beheersing van taken) te zijn door het treffen van adequate beheersmaatregelen en de monitoring van verwerkingen met persoonsgegevens. De teams zijn verantwoordelijk voor het identificeren en beheren van privacy risico's in hun dagelijkse werkzaamheden. Het initiëren van een risico analyse (in de vorm van een Data Protection Impact Assessment (DPIA) is bijvoorbeeld een manier om de risico's in kaart te brengen. De griffie verwerkt persoonsgegevens voor de gemeenteraad, bijvoorbeeld bij ingekomen brieven van inwoners. De griffier is in dit kader te beschouwen als proceseigenaar en dus onderdeel van de eerste lijn.

2e Lijn: De senior jurist privacy, de privacy officer en de medewerker privacy vormen de tweede lijn in de privacy governance van de gemeente. Zij ondersteunen de eerste lijn en houden toezicht op de implementatie en naleving van het privacybeleid en de bijbehorende procedures. De tweede lijn is verantwoordelijk voor het uitzetten van de beheersmaatregelen in de organisatie en om hier vervolgens risico gebaseerd op te sturen. De tweede lijn geeft gevraagd en ongevraagd advies aan de organisatie over privacy vraagstukken. Ten slotte is de tweede lijn verantwoordelijk voor het verzorgen van een overzicht en het leveren van een integrale verantwoording aan de derde lijn.

3e Lijn: De derde lijn is de onafhankelijke audit en de Functionaris Gegevensbescherming. In de derde lijn heeft de FG een toetsende, signalerende, initiërende en adviserende rol met betrekking tot de kwaliteit, de getrouwheid, rechtmatigheid en het functioneren van de eerste en tweede lijn. In de praktijk betekent dit het uitvoeren van periodieke controles en audits om de effectiviteit van het privacybeleid en de naleving ervan te beoordelen. Deze interne toezichthouder is tevens verantwoordelijk voor het opzetten van de externe Wpg audit.

Dit model zorgt voor een gestructureerde aanpak voor privacy management, waarbij de nadruk ligt op naleving van privacywetgeving en de bescherming van persoonsgegevens.



2.3 Rollen en verantwoordelijkheden

In dit hoofdstuk wordt de privacy governance met de bijbehorende rollen en verantwoordelijkheden beschreven. Met de beschrijving van deze rollen en verantwoordelijkheden wordt verder aangeduid hoe er binnen de gemeente Lansingerland wordt gestuurd op het borgen van privacy. In een onderliggend uitvoeringskader wordt invulling gegeven aan de taken die horen bij de rollen en verantwoordelijkheden binnen de privacy governance.

2.3.1 Rollen

Het College van B&W, de gemeenteraad en de burgemeester zijn ieder verwerkingsverantwoordelijke voor hun 'eigen' verwerkingen. Alle drie zijn wettelijk eindverantwoordelijk. In de dagelijkse werkzaamheden ligt deze verantwoordelijkheid bij de directie, met als hoogste uitvoeringsverantwoordelijke de gemeentesecretaris. Ten aanzien van de gemeenteraad is de griffier de uitvoeringsverantwoordelijke. De directie delegeert op hun beurt de verantwoordelijkheid aan de teammanagers, die de teams aansturen. Als privacy binnen de teams in de gemeente onvoldoende wordt geborgd, zal de betreffende directeur in actie moeten komen en de capaciteit inzetten op basis van het hoogste privacy risico. Elke medewerker van de gemeente is medeverantwoordelijk voor een geslaagde uitvoering van het privacybeleid. Medewerkers worden daartoe opgeleid en ook op managementniveau is hier structureel aandacht voor. Het College van B&W, de gemeenteraad en de burgemeester blijven eindverantwoordelijk voor de verwerkingen van gegevens van zowel burgers, medewerkers als derden, en voor de vereiste privacyborging op organisatieniveau. De rollen en verantwoordelijkheden worden hieronder weergegeven:

Verantwoordelijkheid	**Rol**
Feitelijk verantwoordelijk	**1e lijn** • Proceseigenaren (de teammanagers) • Directeuren • Griffier
Eindverantwoordelijk	**1e lijn** • College van B&W • Gemeenteraad • Burgemeester
Ondersteunen en vertalen privacy uitgangspunten en creëren van een integraal overzicht	**2e lijn** • Senior Jurist privacy • Privacy officer • Medewerker privacy
Toezicht	**3e lijn** • Functionaris Gegevensbescherming

2.3.2 Proceseigenaren

De proceseigenaar is degene die verantwoordelijk is voor een bedrijfsproces en vanuit deze rol regisseur is. De proceseigenaar zorgt ervoor dat een proces van begin tot einde optimaal uitgevoerd wordt. Dit geldt ook als een proces team- of domein overstijgend is. Op het vlak van privacy stelt de proceseigenaar eisen waar het proces en onderliggende systemen aan dienen te voldoen. De proceseigenaar is verantwoordelijk voor het toezicht op de naleving van dit privacybeleid. De griffie verwerkt persoonsgegevens. Het privacybeleid is daarom ook van toepassing op de griffie. De griffier is in dit kader te beschouwen als proceseigenaar.

De uitvoering van het privacybeleid, zowel voor de AVG als de Wpg, is een verantwoordelijkheid van het lijnmanagement. Alle verwerkingen binnen de gemeente hebben een eigenaar die het proces bewaakt en fungeert als aanspreekpunt, dit is de proceseigenaar. Het kan voorkomen dat een proceseigenaar het proceseigenaarschap mandateert aan een sub proceseigenaar binnen de gemeente. Bij mandatering blijft de mandaatgever verantwoordelijk voor de privacy bestendigheid van de verwerking.

Bij de privacy governance van de gemeente is de teammanager de proceseigenaar van de verwerkingen binnen een team. De teammanager is verantwoordelijk voor de verwerkingen die plaatsvinden binnen het team. Bij een nieuwe of veranderende verwerking van persoonsgegevens binnen het team is de teammanager verantwoordelijk voor het contact leggen met de tweede lijn. Op basis van de risico gebaseerde werkwijze van de gemeente wordt er samen met de tweede lijn een inschatting gemaakt van het potentiële risico dat de gemeente Lansingerland en de betrokkenen lopen. Hiervoor wordt een risico

analyse (in de vorm van een DPIA) uitgevoerd. De teammanager kan de rol van proceseigenaar onderverdelen binnen het team, maar blijft feitelijk verantwoordelijk en aanspreekpunt in relatie tot de tweede lijn. Als een verwerking wordt uitbesteed aan een externe leverancier, of er wordt samengewerkt met een externe leverancier, blijft de teammanager van het team waar de verwerking binnen valt verantwoordelijk.

De proceseigenaar heeft een actieve rol in het contact met externe partijen. In het geval van uitwisselingsverbanden, samenwerken in samenwerkingsverbanden of het uitbesteden van processen, maakt de proceseigenaar afspraken met de externe partij. De proceseigenaar is verantwoordelijk om de naleving van deze afspraken te controleren. Dit gebeurt in samenwerking met de tweede lijn.

2.3.3 College van B&W, gemeenteraad en burgemeester

Alle bestuursorganen van de gemeente Lansingerland zijn zelf 'verwerkingsverantwoordelijke' in de zin van de AVG. Het College van B&W, de gemeenteraad en de burgemeester zijn verwerkingsverantwoordelijke voor de gemeente. Het College van B&W stelt vanuit de rol als portefeuillehouder privacy, middels de vaststelling van het privacybeleid, uitgangspunten, richtlijnen en protocollen met betrekking tot privacy vast. Deze kaders worden gesteld aan de hand van landelijke en Europese wet- en regelgeving, jurisprudentie en normenkaders. Het College van B&W stimuleert het management van de organisatieonderdelen om voldoende technische en organisatorische maatregelen te nemen om persoons- en politiegegevens te beschermen.

De lijn tussen het College van B&W en de FG moet kort zijn. Het is hier van belang dat het College van B&W ervoor zorgt dat de FG naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens. Ook moet de FG volledig worden geïnformeerd over aspecten van de bedrijfsvoering binnen de gemeente waarbij persoons- en politiegegevens worden verwerkt of wanneer daartoe voornemens bestaan.

2.3.4 De tweedelijns privacy rollen

In de tweede lijn privacy is er een onderverdeling in drie rollen gemaakt. Zij stellen de kaders waarbinnen de eerste lijn werkt. Als tweede lijn hebben zij de verantwoordelijkheid om de eerste lijn te ondersteunen en adviseren in hun werkzaamheden. Hier hoort adviseren bij privacy incidenten bij, maar ook het ondersteunen van de klachten coördinator bij privacy gerelateerde klachten. Ook hebben de tweedelijns privacy rollen een controlerende en monitorende rol door te ondersteunen in het formuleren van de beheersmaatregelen. Ten slotte is de tweede lijn verantwoordelijk voor een overzicht waar privacy staat binnen de gemeente (bijvoorbeeld aan de hand van een privacy jaarverslag). Hoe de tweedelijns privacy rollen en verantwoordelijkheden worden uitgevoerd in taken, wordt toegelicht in het uitvoeringskader.

2.3.4.1 Senior jurist privacy

De senior jurist privacy is op juridisch gebied verantwoordelijk voor de privacy compliance van de gemeente. De senior privacy jurist houdt hierbij vooral de grote lijnen in zicht: het opstellen en implementeren van het privacybeleid en het opstellen van het jaarverslag en de uitvoering hiervan.

2.3.4.2 Privacy officer

De privacy officer is verantwoordelijk voor de uitvoering van de privacy taken. Dit zijn taken als het adviseren bij verwerkersovereenkomsten, begeleiden van DPIA's, behandelen van verzoeken tot uitvoering van rechten van betrokkenen en het behandelen van datalekken. Samen met de chief information security officer (CISO), information security officer (ISO) en de FG neemt de privacy officer en de senior jurist privacy plaats in het periodieke Privacy en Informatiebeveiliging Team (PIT).

2.3.4.3 Medewerker privacy

De medewerker privacy heeft een ondersteunende rol: het helpen bij de uitvoering van de taken die bij de senior jurist privacy en de privacy officer horen. Daarnaast is deze medewerker verantwoordelijk voor het bijhouden van de actielijst en voor de overige administratieve taken.

2.3.5 Functionaris Gegevensbescherming

De Functionaris voor Gegevensbescherming is de interne toezichthouder van gemeente Lansingerland op de naleving van de AVG en de Wpg binnen de gemeente. De FG is geregistreerd bij de Autoriteit Persoonsgegevens en is het contactpunt voor betrokkenen, toezichthoudende autoriteiten en andere belanghebbenden met betrekking tot gegevensbescherming.

Binnen de gemeente Lansingerland is de FG het advies en informatiepunt in relatie tot de naleving van de AVG. De FG heeft een directe lijn met het College en informeert en adviseert het College, de eerste en tweede lijn gevraagd en ongevraagd met betrekking tot gegevensbescherming. De zienswijze van de FG is zwaarwegend en geldt als de manier waarop de gemeente Lansingerland de AVG naleeft.

In het uitvoeringskader worden de taken van de FG verder uitgelicht, hieronder is een overzicht van de taken van de FG opgenomen. De FG:

- informeert en adviseert het college, proceseigenaren en het Privacy en Informatiebeveiliging Team (PIT) over de werking van het privacybeleid van gemeente en nakoming van achterliggende wettelijke verplichtingen (heeft de lead in interpretatie van privacywetgeving);
- houdt toezicht op het beleid van de gemeente met betrekking tot de bescherming van persoonsgegevens;
- helpt met privacy klachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacy incidenten over ernst en omvang;
- ziet toe op 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;
- doet jaarlijks verslag van de werkzaamheden aan het College van B&W;
- houdt in het kader van de Wpg toezicht op:
    - het naleven van de Wpg;
    - het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens;
    - de toewijzing van de autorisaties;
    - de bewustmaking en opleiding van de boa's en andere functionarissen die betrokken zijn bij de verwerking van politiegegevens;
    - de audits;
    - de uitvoering van DPIA's;
    - jaarlijkse rapportage aan de verwerkingsverantwoordelijke over de bevindingen m.b.t. de Wpg. Bijvoorbeeld in het FG jaarverslag.

3 Privacymanagement proces

3.1 Invulling van privacymanagement

3.1.1 Privacy framework en de beheersmaatregelen

De gemeente geeft invulling aan privacy management door het implementeren van een gestructureerd privacy framework dat richtlijnen en procedures biedt voor de omgang met persoonsgegevens. Dit framework omvat duidelijke normen en richtlijnen die van toepassing zijn op alle aspecten van gegevensverwerking binnen de gemeente. Binnen dit framework worden beheersmaatregelen vastgesteld om risico's te minimaliseren en de bescherming van persoonsgegevens te waarborgen. Deze beheersmaatregelen omvatten technische, organisatorische en procedurele aspecten, zoals het versleutelen van gevoelige gegevens, het instellen van toegangsbeperkingen en het regelmatig evalueren, en indien nodig, bijwerken van privacybeleid.

Gemeente Lansingerland hanteert een privacy framework dat is gebaseerd op relevante normen op het gebied van privacy en informatiebeveiliging: het Privacy en Informatieveiligheid (PIV) framework. Dit framework is een verzameling van alle relevante wet- en regelgeving op het gebied van privacy en informatiebeveiliging zoals de privacy baseline van het Centrum Informatiebeveiliging en Privacy (CIP), de Wpg, de VNG Criteria borging AVG 2.0 én de ISO27701. De privacy baseline van het CIP is een vertaling van de AVG voor overheidsorganisaties. De beheersmaatregelen die zijn opgenomen zijn vertalingen van normen als de privacy baseline, de Wpg, de VNG criteria borging AVG 2.0 én de ISO27701.

De beheersmaatregelen (genaamd SMART-controls in Recourse) worden continu gemonitord door periodiek in de organisatie op te halen of de gemeente voldoet aan de beheersmaatregelen. Als blijkt dat de organisatie of organisatieonderdelen de beheersmaatregelen niet uitvoeren, dan moet actie worden ondernomen. Niet compliant zijn met beheersmaatregelen betekent niet compliant met relevante wet- en regelgeving en dit vormt een risico voor de gemeente Lansingerland. De eerste en tweede lijn moeten in actie komen om het risico te mitigeren. In onderstaand kader het volgende voorbeeld:

De beheersmaatregel voor de aanwezigheid van privacybeleid: het PIV framework schrijft voor dat de gemeente privacybeleid moet hebben. Achterliggende normen zijn hierbij VNG Criteria borging AVG 2.0 en de Wpg voor boa's. Om te achterhalen of de gemeente voldoet aan deze beheersmaatregel, wordt uitgevraagd of er vastgesteld privacybeleid is. Als terugkomt dat dit niet zo is, voldoet de gemeente niet aan de achterliggende normen en dus niet aan de wet. Hierop kan vervolgens gestuurd worden.

Als echter terugkomt dat privacybeleid aanwezig is én vastgesteld is, dan voldoet de gemeente aan deze beheersmaatregel.

Een belangrijk onderdeel van dit privacy managementproces is het inventariseren van de risico's en beheersmaatregelen die specifiek zijn voor de verwerkingen van de gemeente. Binnen de privacy organisatie wordt op privacy risico's gestuurd door middel van het uitvoeren van Data Protection Impact Assessments (DPIA) en pre-DPIA's door de eerste en tweede lijn. Deze assessments worden ingezet bij nieuwe en bestaande projecten, systemen of diensten die mogelijk een impact hebben op de privacy van inwoners. Door DPIA's uit te voeren, kan de gemeente proactief privacy risico's identificeren en beoordelen voordat een initiatief wordt geïmplementeerd. Dit stelt de gemeente in staat om passende beheersmaatregelen te plannen en uit te voeren om potentiële risico's te minimaliseren.

De risico's worden vervolgens vergeleken met de beheersmaatregelen die al aanwezig zijn. Als de beheersmaatregelen het risico niet benoemen, wordt er een beheersmaatregel toegevoegd of uitgebreid door de eerste en tweede lijn. Deze werkwijze is in lijn met de PDCA-cyclus en het 'continue verbeteren' uitgangspunt van de gemeente Lansingerland.

De combinatie van een robuust privacy framework, continue monitoring van beheersmaatregelen en de uitvoering van DPIA's vormt een integrale benadering van privacy management die de gemeente in staat stelt om zowel effectieve dienstverlening als privacybescherming te waarborgen.

3.1.2 Het privacy management proces

Het privacy management proces omvat verschillende stappen om privacy risico's te identificeren, beoordelen, beheersen en op lange termijn te monitoren en evalueren. De kernstappen van dit proces zijn:

1. **Identificatie van privacy risico's**: In deze fase worden door het uitvoeren van DPIA's potentiële privacy risico's geïdentificeerd die kunnen ontstaan bij de verwerking van persoonsgegevens. Dit omvat het in kaart brengen van de verschillende activiteiten, processen en systemen waarbij persoonlijke informatie wordt betrokken. Als aan beheersmaatregelen niet of deels wordt voldaan, bevinden zich hier mogelijke privacy risico's.
2. **Beoordeling van privacy risico's**: Bij deze stap worden de geïdentificeerde privacy risico's beoordeeld. Dit gebeurt op basis van criteria zoals impact op individuen, gevoeligheid van gegevens en de kans op een incident middels het uitvoeren van DPIA's. Dit helpt bij het prioriteren van risico's en het bepalen van de benodigde beheersmaatregelen.
3. **Ontwikkeling van beheersmaatregelen**: Na het beoordelen van de risico's worden passende beheersmaatregelen ontwikkeld om deze risico's te verminderen of te elimineren. Dit omvat technische, organisatorische en procedurele maatregelen die gericht zijn op het waarborgen van de privacy en beveiliging van persoonsgegevens. De DPIA geeft aanbevelingen hoe de risico's gemitigeerd kunnen worden. De eerste lijn is verantwoordelijk om deze op te pakken en (zie ook volgende stap) deze te implementeren.
4. **Implementatie van beheersmaatregelen**: De vastgestelde beheersmaatregelen worden geïmplementeerd in de organisatie. Dit omvat het integreren van de maatregelen in de dagelijkse werkwijzen, systemen en processen om ervoor te zorgen dat privacy risico's effectief worden aangepakt. De eerste lijn is verantwoordelijk voor de implementatie van de beheersmaatregelen. De tweede lijn ondersteunt hierbij.
5. **Monitoring en evaluatie**: Na de implementatie wordt het privacy management proces voortgezet met monitoring. Hierbij wordt gecontroleerd of de genomen beheersmaatregelen daadwerkelijk de gewenste effecten hebben en of nieuwe risico's zich voordoen. De monitoring door beheersmaatregelen vindt plaats door een check op de effectiviteit van de beheersmaatregelen door de tweede lijn.
6. **Rapportage en communicatie**: De bevindingen van de monitoring worden gerapporteerd aan het management en andere relevante belanghebbenden. Dit zorgt voor transparantie en zorgt ervoor dat passende beslissingen kunnen worden genomen op basis van de risico-evaluatie. De derde lijn, in dit geval de FG, informeert de organisatie middels het FG jaarverslag. De tweede lijn informeert de organisatie eveneens middels het privacy jaarverslag.
7. **Evaluatie en bijsturing**: Periodiek wordt het gehele proces geëvalueerd om te beoordelen of het privacy management effectief is en of er verbeteringen mogelijk zijn. Indien nodig worden beheersmaatregelen aangepast om de evoluerende risico's aan te pakken. Middels de jaarverslagen van de FG en het privacy jaarverslag, geeft de directie aan waar de prioriteit ligt en waarop gestuurd moet worden.

Het privacy risicomanagement proces is een cyclisch proces dat continu wordt herhaald om ervoor te zorgen dat privacy risico's adequaat worden aangepakt en dat de bescherming van persoonsgegevens wordt gehandhaafd in overeenstemming met de geldende privacywetgeving en -normen.

3.2 Operationeel beleid

3.2.1 Introductie

De belangrijkste beheersmaatregelen uit het privacymanagement framework worden verder uitgewerkt in operationeel beleid om ervoor te zorgen dat abstracte richtlijnen en principes worden vertaald naar concrete en praktisch toepasbare stappen die binnen de dagelijkse activiteiten van de gemeente kunnen worden geïntegreerd. Implementatie van beheersmaatregelen in operationeel beleid is van essentieel belang om de bescherming van persoonsgegevens te waarborgen en te voldoen aan privacyregelgeving. Om de beheersmaatregelen een herkenbare structuur te geven zijn ze ingedeeld in een aantal thema's. Per thema is er een uitvoeringskader beschikbaar. Het uitvoeringskader is een verdere uitwerking van de privacy thema's op operationeel niveau. De thema's worden hieronder geïntroduceerd en kort uitgelegd.

3.2.2 Privacy management

Privacy management	***Beheersdoelstelling***	**Uitwerking**	**Rol 1e. 2de en 3de lijn**
De gemeente Lansingerland neemt de verantwoordelijkheid voor het zorgvuldig omgaan met persoonsgegevens en stuurt hierop 	*De gemeente maakt beslissingen over de omgang met persoonsgegevens op basis van beleid en procedures waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt.*	De gemeente geeft invulling hieraan middels dit privacybeleid en het onderliggende uitvoeringskader	Het privacybeleid en uitvoeringskader wordt opgesteld en bijgehouden door de tweede lijn.

3.2.3 Privacy risico beheersing

Privacy risico beheersing	***Beheersdoelstelling***	**Uitwerking**	**Rol 1e, 2de en 3de lijn**
De gemeente Lansingerland werkt risico gebaseerd en stuurt op de grootste risico's 	*De gemeente werkt risico gebaseerd om privacy risico's en de impact daarvan op de betrokkenen te identificeren en actief terug te dringen*	Het uitzetten van beheersmaatregelen in Recourse en het uitvoeren van DPIA's. Hoe de gemeente DPIA's uitvoert is uitgewerkt in het uitvoeringskader	De tweede lijn zet de beheersmaatregelen uit in de organisatie. De eerste lijn initieert de DPIA, de tweede lijn ondersteunt hierbij.

3.2.4 Privacy by design

Privacy by design	***Beheersdoelstelling***	**Uitwerking**	**Rol 1e, 2de en 3de lijn**
 De gemeente Lansingerland werkt volgens de principes van privacy-by-design	*De gemeente heeft als doel om privacybescherming en -overweging te integreren in het ontwerp en ontwikkeling van nieuwe systemen en processen*	De aanpak bevordert om proactieve privacy maatregelen in het ontwerp te verankeren en niet in de nasleep toe te passen. In de praktijk betekent dit dat bij de configuratie van systemen de gemeente altijd kiest voor de privacy-vriendelijke variant	Zowel de eerste, tweede als derde lijn dient te werken volgens de principes van privacy by design. De FG heeft in de rol als toezichthouder het mandaat om hier toezicht op te houden

3.2.5 Rechten van betrokkenen

Rechten van betrokkenen	***Beheersdoelstelling***	**Uitwerking**	**Rol 1e, 2de en 3de lijn**

 De gemeente Lansingerland is transparant richting betrokkenen over de verwerking van persoonsgegevens	*De gemeente informeert betrokkenen tijdig en begrijpelijk over de verwerking waarvoor de gemeente verwerkingsverantwoordelijke is. Daarnaast maakt de gemeente het mogelijk dat individuen wiens persoonsgegevens worden verwerkt door de gemeente, hun rechten kunnen uitoefenen*	De gemeente informeert betrokkenen middels de privacyverklaring en dit privacybeleid over hun rechten en hoe deze uit te oefenen	De tweede lijn is verantwoordelijk voor het opstellen en onderhouden van de privacyverklaring en het privacybeleid. De eerste lijn dient te werken volgens deze documenten. De tweede lijn pakt de verzoeken van rechten van betrokkenen op en handelt deze af

3.2.6 Uitwisselingsrelaties

Uitwisselingsrelaties	***Beheersdoelstelling***	**Uitwerking**	**Rol 1e, 2de en 3de lijn**
 De gemeente Lansingerland heeft inzicht in de relaties met externen en beschermt de persoonsgegevens binnen deze relaties	*De gemeente wisselt gegevens uit met externe partijen. Als verwerkingsverantwoordelijke en in samenwerkingsverbanden vindt de gemeente het belangrijk dat deze externe partijen zorgvuldig met de gegevens van de gemeente omgaan*	Door het maken van afspraken, het tekenen van overeenkomsten met de externe partijen en het toezien op de naleving van gemaakte afspraken moeten de gegevens van gemeente ook bij de externe partij gewaarborgd zijn	De eerste lijn initieert en maakt afspraken met de externe partij. De tweede lijn ondersteunt hierbij. In het uitvoeringskader is contract en leveranciersmanagement verder uitgewerkt

3.2.7 Inzicht in verwerkingen

Inzicht in verwerkingen	***Beheersdoelstelling***	**Uitwerking**	**Rol 1e, 2de en 3de lijn**
 De gemeente Lansingerland verwerkt persoonsgegevens rechtmatig en heeft inzicht en grip op alle verwerkingen door de gemeente en de rechtmatigheid daarvan	*De gemeente verwerkt persoonsgegevens alleen rechtmatig, behoorlijk en met een wettelijke grondslag. De gemeente heeft een compleet beeld van de verwerkingen van persoonsgegevens*	De gemeente heeft een register van verwerkingsactiviteiten. Hierin is vastgelegd wat de verwerking is, met welk doel en welke wettelijke grondslag hieraan ten grondslag ligt	De tweede lijn onderhoudt het register van verwerkingen. De eerste lijn is verantwoordelijk voor het melden van een nieuwe of aangepaste verwerking. De derde lijn houdt toezicht op het register middels steekproeven

3.2.8 Informatiebeveiliging

informatiebeveiliging	***Beheersdoelstelling***	**Uitwerking**
 Informatiebeveiliging is een belangrijk onderdeel om persoonsgegevens bij de gemeente Lansingerland te beschermen	*De gemeente verwerkt persoonsgegevens alleen met adequate en passende informatiebeveiliging. Dit thema is belegd bij concerncontrol*	De gemeente heeft informatiebeveiligingsbeleid

4 Monitoring en evaluatie

4.1 Cyclus van het privacybeleid

Dit beleid is opgesteld aan de hand van de geldende wet- en regelgeving op het gebied van de bescherming van persoonsgegevens en de verwerking van politiegegevens. Het privacybeleid treedt in werking na vaststelling door de verantwoordelijke, de gemeenteraad, de burgemeester en het College van B&W. Dit beleid wordt elke drie jaar ambtelijk geëvalueerd en wordt tussentijds herzien wanneer dat nodig

is. De evaluatie van dit beleid is gestoeld op de PDCA-cyclus (Plan-Do-Check-Act). Dit is een model voor continue verbetering van de werkprocessen, een belangrijk uitgangspunt voor de gemeente.

4.2 Audit Wpg
In de Wet Politiegegevens is vastgelegd dat de verwerkingsverantwoordelijke de naleving van de Wpg moet controleren middels audits. Werkgevers van boa's die voor de uitvoer van hun opsporingstaak persoonsgegevens verwerken zijn verplicht om eens per vier jaar een externe privacy audit uit te voeren. De gemeente is een werkgever van boa's en is dus verplicht tot het uitvoeren van externe privacy audits op de Wpg. De rapportage van deze externe audit moet worden verstrekt aan de externe toezichthouder, de Autoriteit Persoonsgegevens (AP). Bij het constateren van tekortkomingen moet drie maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit. De verantwoordelijkheid voor het initiëren van deze audits ligt binnen de gemeente bij de derde lijn, de interne toezichthouder (zie 2.3.5).

Daarnaast moet in de jaren dat géén externe audit wordt uitgevoerd een interne audit Wpg worden uitgevoerd die specifiek gericht is op de werkzaamheden die binnen de lijnorganisatie plaatsvindt op grond van de Wpg.

5 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 Gegevensbescherming) – wettelijk toezichthouder voor de naleving van privacywetgeving en bedrijfsvoorschriften

Governance – sturing op privacy door het management

(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)

DPIA (Data Protection Impact Assessment) – een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico's vanuit privacy-optiek, resulterend in een lijst van passende beheersmaatregelen (waarborgen)

PIT – het privacy- en informatiebeveiligingsteam dat het college, directie, proceseigenaren en teammanagers ondersteunt

Politiegegevens – elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak: het handhaven van de rechtsorde en het verlenen van hulp aan hen die deze behoeven

Portefeuillehouder privacy – het lid van het college van B&W dat verantwoordelijk is voor de uitvoering en naleving van privacywetgeving met behulp van het privacybeleid

Privacy audit – controles op de naleving van privacybeleid en privacywetgeving

Privacybeleid – het algemeen privacybeleid van een organisatie

Privacy incidenten – incidenten waarbij een onrechtmatige gegevensverwerking plaatsvindt

Privacymanagement – verwijst naar het proces van beheren, beschermen en waarborgen van persoonlijke gegevens binnen de gemeente Lansingerland

Privacywetgeving – wetgeving die verwerking van persoonsgegevens regelt, in het bijzonder de AVG

Proces - is een serie van activiteiten (uitgevoerd door een menselijk handelen of door een systeem) waar verschillende middelen voor nodig zijn. Binnen de context van de gemeente Lansingerland is een proces een keten van activiteiten waar een product of dienst uit komt

Proceseigenaren – teammanager i.c. de afdelingshoofden die verantwoordelijk zijn voor uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen en veiligheid

Uitvoeringskader – in het uitvoeringskader wordt invulling gegeven aan de privacy governance rollen en verantwoordelijkheden. Bijvoorbeeld een uitwerking van het DPIA proces en het melden en afhandelen van datalekken

Verwerking - een handeling waar persoonsgegevens voor worden gebruikt. Dit kan zijn het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van persoonsgegevens

Wpg (Wet Politiegegevens) – Nederlandse wet die specifiek van toepassing is op de verwerking van politiegegevens door de politie, bijzondere opsporingsdiensten en boa's.