Provinciale Staten Drenthe

Statenstuk 2023-135

Beleidskader privacy provincie Drenthe

Voorgestelde behandeling:
- Statencommissie op 24 januari 2024
- Provinciale Staten op 14 februari 2024
- Fatale beslisdatum: n.v.t.

Voorstel van het presidium van Provinciale Staten van Drenthe van 13 december 2023, kenmerk 50/SG/202302860

Behandeld door de mevrouw L. Schutte, telefoonnummer (0592) 36 56 84

Inleiding

In 2018 zijn de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) in werking getreden. Privacyregels zijn daarmee uniform verankerd in Europa en verder uitgewerkt in nationale wetgeving. De normen uit de AVG en UAVG zijn echter algemeen van aard en met veel beleidsruimte. Elke organisatie krijgt ruimte om eigen keuzes te maken, mits dit verantwoord is binnen de algemene normen. In het verleden zijn veel van deze keuzes (impliciet) ook gemaakt binnen de provincie Drenthe en/of wordt er, sinds de inwerkingtreding, zo veel mogelijk op een bepaalde manier mee gewerkt.

Om transparant te zijn als overheid en om willekeur te voorkomen bestaat de noodzaak te komen tot beleid ten aanzien van privacy. Het privacybeleid is algemeen beleid, geldend voor bestuurders en ambtenaren, waarin staat wie waarvoor verantwoordelijk is en welke keuzes de provincie heeft gemaakt ten aanzien van privacy. Hierbij is tevens de gelegenheid genomen om benodigde specifieke bepalingen voor het Drents Parlement en de Statengriffie vast te leggen. Als provincie Drenthe willen we graag uniform werken op het gebied van privacy. Provinciale Staten sluiten aan op dit beleidskader en stellen het beleid vast voor Provinciale Staten. Hoewel gedeputeerde niet voor de Staten kan spreken, kan hij wel een toelichting geven op dit stuk.

De ontwikkelingen en de druk op het privacy domein zijn op dit moment groot. In 2024 worden er enkele Europese richtlijnen omgezet naar nationaal recht die ook in 2024 nog geïmplementeerd moeten worden. Dit kan dus betekenen dat het voorliggende beleid in 2024 aangepast moet worden of dat er aanvullende kaders moeten worden gesteld.

In het beleidskader wordt de wetgeving over privacy zoveel mogelijk nader uitgewerkt voor de provincie. Dit zorgt ervoor dat de provincie zo zorgvuldig en veilig mogelijk omgaat met persoonsgegevens van betrokkenen.

Privacybeleid
De provincie Drenthe werkt met persoonsgegevens. Dit gaat om gegevens van zowel externe personen, zoals inwoners en contactpersonen van andere overheden, bedrijven en instellingen, als van interne personen, zoals bestuurders en werknemers. Zonder deze gegevens kan de provincie Drenthe het werk niet doen en de betrokkenen niet van dienst zijn. De provincie Drenthe wil zorgvuldig omgaan met deze persoonsgegevens en de privacy van betrokkenen beschermen.

In het beleidskader staan 13 privacyprincipes verwoordt die weergeven hoe de provincie Drenthe omgaat met privacy en de bescherming daarvan.
De provincie Drenthe verzamelt en/of verwerkt alleen persoonsgegevens als er een grondslag voor is (artikel 6 AVG). Dit wordt vervolgens vastgelegd in het verwerkingsregister. In beginsel zal de provincie gegevens verwerken op grond van een wettelijke bevoegdheid in verband met publieke taken. Daarnaast minimaliseert en bewaart de provincie Drenthe persoonsgegevens niet langer dan strikt noodzakelijk. Dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verzameling en/of verwerking.

Overheden hebben ook een informatieplicht richting betrokkenen. In de AVG is expliciet opgenomen dat persoonsgegevens verzameld en/of verwerkt moeten worden op een manier die transparant is voor de betrokkene. Voor een natuurlijke persoon moet transparant zijn of en in hoeverre de persoonsgegevens (zullen) worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt.

Communicatie met betrokkene dient bovendien plaats te vinden in begrijpelijke, beknopte en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal.

Paragrafen Provinciale Staten
In het beleidskader privacy provincie Drenthe is het privacybeleid voor de provincie Drenthe vastgelegd, om voor de provincie Drenthe zo goed mogelijk invulling te geven aan de Europese en landelijke wetgeving. Dit beleid geldt voor de gehele provincie, dus voor zowel GS als PS.
De volgende paragrafen gaan **specifiek** over Provinciale Staten dan wel de Statengriffie.

3.2.1. College van Gedeputeerde Staten (GS) en Provinciale Staten (PS)
GS en PS zijn samen verantwoordelijk voor het naleven van het privacybeleid van de provincie Drenthe, ieder voor het eigen deel. GS en PS hebben met dit kader het privacybeleid vastgesteld voor de uitvoering van de eigen werkzaamheden in lijn met de AVG.

3.2.2. Algemeen directeur en Statengriffier
Mensen hebben recht op inzage in de persoonsgegevens die organisaties van hen verwerken. Het recht op inzage wordt ook wel en AVG-verzoek bedoelt.
Op basis van artikel 3, sub f Besluit mandaat, volmacht en machtiging Provinciale Staten en Commissaris van de Koning van Drenthe 2022 heeft de Statengriffier het mandaat en machtiging om namens Provinciale Staten beslissingen te nemen met betrekking tot verzoeken tot uitoefening van privacy (AVG-verzoeken). In die hoedanigheid heeft de Statengriffier eenmaal per jaar contact met de functionarisgegevensbeschermer (FG).

3.2.4. Medewerkers
De medewerkers van de Statengriffie (PS) voeren, net zoals de medewerkers van ambtelijke organisatie (GS), de werkprocessen uit binnen de kaders van het privacybeleid.

Advies

PS en GS stellen het voorliggende kader beide vast. Het advies aan PS is daarmee om in te stemmen met het ‘beleidskader privacy provincie Drenthe’.

Beoogd effect

Door in te stemmen met het beleidskader privacy provincie Drenthe werken Gedeputeerde Staten en Provinciale Staten uniform op het gebied van privacy en zijn de normen, zoals gesteld door de AVG en UAVG, uitgewerkt en verankerd.

Uitvoering

Communicatie

- website

Bijlagen

1. Beleidskader privacy provincie Drenthe

Assen, 13 december 2023
Kenmerk: 50/SG/202302860

Provinciale Staten van Drenthe,

mevrouw drs. J. Klijnsma, voorzitter
mevrouw mr. drs. S. Buissink, griffier

*Ontwerp*besluit

2023-135-1

Provinciale Staten van Drenthe;

gelezen het voorstel van het presidium van Provinciale Staten van Drenthe van 13 december 2023, kenmerk 50/SG/202302860;

BESLUITEN:

In te stemmen met het Beleidskader privacy provincie Drenthe

Assen, 14 februari 2024

Provinciale Staten voornoemd,

, voorzitter , griffier

provincie Drenthe

Beleidskader privacy provincie Drenthe

Colofon

Datum
februari 2023

Adresgegevens
Provincie Drenthe
Westerbrink 1
Postbus 122
9400 AC ASSEN
Telefoon: (0592) 36 55 55
www.provincie.drenthe.nl

Documentgegevens

Titel	: Beleidskader privacy provincie Drenthe
Document	: Privacybeleid provincie Drenthe
Status	: Vastgesteld door Gedeputeerde Staten van Drenthe d.d. @@@@
Versie	: 0.4

Inhoud

0. Voorwoord

Sinds 25 mei 2018 is in de hele Europese Unie de Algemene verordening gegevensbescherming (AVG)[1] van toepassing. Op nationaal niveau is de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) vastgesteld. De AVG en de UAVG geven regels voor de bescherming van de privacy en de verwerking van persoonsgegevens.

Ook de provincie Drenthe werkt met persoonsgegevens. Waar nodig worden door de provincie Drenthe persoonsgegevens verwerkt voor het goed kunnen uitvoeren van wettelijke medebewindstaken, autonome taken of voor de provinciale bedrijfsvoering.
Hierbij gaat het om gegevens van zowel externe personen, zoals inwoners en contactpersonen van andere overheden, bedrijven en instellingen, als van interne personen, zoals bestuurders en werknemers. Zo kunnen bijvoorbeeld inwoners via de website van de provincie Drenthe allerlei formulieren invullen of informatie opvragen. Daarbij worden persoonsgegevens aan de provincie Drenthe verstrekt. Zonder deze gegevens kan de provincie Drenthe het werk niet doen en de betrokkenen niet van dienst zijn. Bestuurders en werknemers verstrekken persoonsgegevens aan de provincie Drenthe als contactgegevens of gegevens voor het salaris- en personeelssysteem.

Als provincie Drenthe gaan wij zorgvuldig om met persoonsgegevens en het beschermen van de privacy van betrokkenen.

De AVG en de UAVG geven niet voor elk privacyvraagstuk een pasklaar antwoord. De Europese en landelijke wetgeving bevatten normen, die samen een afwegingskader geven. Aan de hand van het wettelijk afwegingskader moet de provincie Drenthe beoordelen of een bepaalde verwerking van persoonsgegevens is toegestaan, en zo ja, onder welke voorwaarden. In dit document hebben wij het privacybeleid van de provincie Drenthe vastgelegd, om voor de provincie Drenthe zo goed mogelijk invulling te geven aan de Europese en landelijke wetgeving. Privacy-afwegingen kunnen daarnaast ook in andere processen en regelingen van de provincie Drenthe zitten.

Gedeputeerde Staten van Drenthe
Provinciale Staten van Drenthe

[1] De AVG staat ook wel bekend onder de Engelse naam General Data Protection Regulation (GDPR).

1. Algemeen

1.1 Inleiding

In dit hoofdstuk wordt achtereenvolgens ingegaan op de definities die van belang zijn voor het privacybeleid van de provincie Drenthe, het bereik van dit document en de opbouw van dit document.

1.2 Definities

In het privacybeleid van de provincie Drenthe wordt uitgegaan van de onderstaande definities. Deze definities zijn afkomstig uit dan wel zo veel mogelijk afgeleid van bestaande wet- en regelgeving (met name artikel 4 van de AVG), uit het Beleidskader informatiebeveiliging van de provincie Drenthe en uit gegevens van betrokken instanties, zoals de Autoriteit Persoonsgegevens (AP).

Autoriteit Persoonsgegevens (AP): de onafhankelijke Nederlandse toezichthouder op de naleving van de Europese en nationale regels voor de bescherming van persoonsgegevens. De AP draagt hiermee bij aan de bescherming van het grondrecht op bescherming van persoonsgegevens.

Betrokkene: degene over wie de gegevens gaan en die daarmee geïdentificeerd kan worden.
NB. De betrokkene is géén eigenaar van zijn/haar gegevens, maar heeft daarover wel zeggenschap, afhankelijk van welke wettelijke grondslag op de verwerking van toepassing is.

Coördinator Informatiebeveiliging (CIB): functionaris die binnen de organisatie zorgdraagt voor de informatiebeveiliging. NB. Het doel van de functie is het zorgdragen voor een samenhangend pakket van maatregelen voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen de organisatie. Risicoanalyse, oog voor de bedrijfsvoering en inachtneming van de wettelijke voorschriften zijn daarbij sleutelbegrippen.

Datalek: inbreuk in verband met persoonsgegevens, leidend tot ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Het kan ook gaan om het ongewenst vernietigen, verliezen, wijzigen en/of verstrekken van persoonsgegevens, waardoor betrokkenen schade kunnen leiden.

Derde[2]: een natuurlijke persoon of organisatie, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Functionaris Gegevensbescherming[3] **(FG)**: functionaris die binnen de organisatie toezicht houdt op en adviseert over de toepassing en naleving van de AVG (een interne privacytoezichthouder). NB. Organisaties zijn in bepaalde situaties verplicht een FG aan te stellen. Overheidsorganisaties en publieke organisaties zijn altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken.
Deze verplichting geldt dus ook voor de provincie Drenthe. De FG van provincie Drenthe verricht werkzaamheden voor (de organisaties van) PS en GS. De organisatie van PS betreft de Statengriffie. Overheidsorganisaties moeten hun FG aanmelden bij de AP. Behalve de FG kent de provincie Drenthe ook een privacy officer.

Gegevensbeschermingseffectbeoordeling, ook wel data protection impact assessment (DPIA[4]**)**: een beoordeling van de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen; hiermee worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van privacy.

Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

[2] De definitie van derde staat in de AVG (artikel 4, aanhef en onder 10). Deze definitie is daarvan afgeleid.
[3] Ook wel Data Protection Officer, afgekort DPO.
[4] Ook wel Privacy Impact Assessment (PIA).

Informatie: informatie is voor de organisatie een ‘bedrijfsmiddel’ en ook vaak een ‘product’. Informatie heeft waarde voor de organisatie en dient voortdurend op een passende manier beveiligd te zijn. Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn. Informatie valt ook binnen de archiefwetgeving gegeven definitie van archiefbescheiden. Daaruit volgt dat deze in goede, geordende en toegankelijke staat dient te zijn en dat de vastgestelde bewaartermijn moet worden nageleefd. De beveiliging is een uitwerking van wat onder ‘goede staat’ kan worden verstaan.

Informatieveiligheid: informatieveiligheid op orde is een randvoorwaarde voor een efficiënt en effectief primair proces. Als de informatieveiligheid niet voldoende is geborgd, loopt het vertrouwen in de provincie gevaar. Informatieveiligheid is geen doel op zich, maar een integraal onderdeel van de kwaliteitszorg voor bedrijfsprocessen en informatievoorziening van de provinciale organisatie. De kwaliteitsaspecten waarnaar gekeken wordt zijn: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

- Beschikbaarheid: het waarborgen dat geautoriseerde gebruikers toegang hebben tot informatie en dat benodigde bedrijfsmiddelen, zoals onder andere werkplekken en pc’s, voorhanden zijn.
- Integriteit: het waarborgen van de juistheid, de volledigheid en tijdigheid van informatie en verwerking.
- Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.
- Controleerbaarheid: het waarborgen dat achteraf onweerlegbaar de toegang en transacties gecontroleerd kunnen worden.

Ontvanger[5]: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

Persoonsgegevens: alle gegevens zoals bedoeld in artikel 4, aanhef en onder 1 van de AVG. Hierbij gaat het samengevat over gegevens die gaan over natuurlijke personen en waaraan je een persoon als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaalde persoon (bijvoorbeeld: naam, (e-mail)adres, geboortedatum, telefoonnummer, foto’s). Naast ‘gewone’ persoonsgegevens kent de AVG ook ‘bijzondere’ persoonsgegevens[6]. Dit zijn gegevens die door hun aard bijzonder gevoelig zijn, zoals etnische achtergrond, gezondheid, politieke voorkeuren of genetische en biometrische gegevens. NB. Gegevens over organisaties, zoals bedrijven, zijn in de regel geen persoonsgegevens.

Privacy: is een grondrecht en een voorwaarde om vrij te zijn in wie je bent en wat je doet. Privacy gaat erover dat mensen regie houden over hun gegevens. Het gaat erom dat mensen niet continu gevolgd worden, dat de gegevens van mensen veilig zijn, het gaat over de zeggenschap over de eigen persoonsgegevens.

Privacy ambassadeur (pramba): een medewerker per domein of van de Statengriffie die fungeert als privacy-aanspreekpunt voor de collega’s uit het domein, de privacy officer en de FG.

---

[5] Deze definitie van ontvanger staat in de AVG (artikel 4, onder 9).

[6] De AVG (artikel 9) spreekt van 'bijzondere categorieën persoonsgegevens'. Dit zijn gegevens over:

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuigingen;
- Lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon;
- Gezondheid;
- Seksueel gedrag of seksuele gerichtheid.

Bijzondere categorieën persoonsgegevens betreffen gegevens die naar hun aard vertrouwelijker zijn dan 'gewone' persoonsgegevens. Het vertrekpunt is dat verwerking van deze categorieën van gegevens verboden is tenzij aan een aantal voorwaarden is voldaan. Andere bijzondere gegevens zoals strafrechtelijke informatie en Burgerservicenummer (BSN) vallen onder specifieke wettelijke regimes.

Privacy officer (PO): een daartoe aangewezen jurist bij de provincie Drenthe met privacytaken; deze jurist draagt zorg voor de dagelijkse gang van zaken rondom privacy en is eerste vervanger van de FG.

Privacyverklaring: een verklaring waarin de betrokken overheid ingaat op de bescherming van de privacy van degene die contact opneemt of heeft met de betrokken overheid en daarbij persoonsgegevens deelt met deze overheid.

Profilering[7]: het indelen van personen in categorieën (profielen) op basis van hun persoonsgegevens. Op basis van deze profielen kunnen vervolgens (geautomatiseerde) individuele besluiten worden genomen.

Pseudonimisering[8]**:** het verwerken van persoonsgegevens op een zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Toestemming van de betrokkene[9]: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de betrokkene betreffende verwerking van persoonsgegevens aanvaardt.

Verwerker[10]: de persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie. NB. Er is alleen sprake van verwerkerschap als de verwerker niet aan het rechtstreekse gezag van de verwerkingsverantwoordelijke is onderworpen. Als er sprake is van een hiërarchische verhouding, dan is er geen sprake van verwerkerschap; in dat geval wordt er gesproken van ‘intern beheer’.

Verwerking[11]: alles wat je met een persoonsgegeven doet, zoals 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 gegevens.

Verwerkingsregister[12]: administratie van verwerkingsactiviteiten; betreft een overzicht van de verschillende verwerkingsactiviteiten die onder de verantwoordelijkheid van de organisatie vallen.

Verwerkingsverantwoordelijke[13]: de persoon of organisatie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

---

[7] De definitie van profilering in de AVG (artikel 4, onder 4) luidt: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
[8] Deze definitie van pseudonimisering staat in de AVG (artikel 4, onder 5).
[9] Deze definitie van toestemming van de betrokkene staat in de AVG (artikel 4, onder 11).
[10] De rollen van verwerker en verwerkingsverantwoordelijke kunnen samenvallen in één organisatie, wanneer de verwerkingsverantwoordelijke tevens zelf de verwerkingen uitvoert. De definitie van verwerker in de AVG (artikel 4, aanhef en onder 8) luidt: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
[11] De definitie van verwerking in de AVG (artikel 4, aanhef en onder 2) luidt: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
[12] Het verwerkingsregister wordt ook wel register van verwerkingsactiviteiten genoemd.
[13] De definitie van verwerkingsverantwoordelijke in de AVG (artikel 4, aanhef en onder 7) luidt: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

1.3 Bereik

Overkoepelende, richtinggevende visie
Dit beleidskader is een overkoepelende, richtinggevende visie op het privacybeleid van de provincie Drenthe en biedt kaders voor alle onderliggende (beleids)documenten en/of (beheers)maatregelen die de provincie Drenthe opstelt dan wel neemt op het terrein van de bescherming van privacy van zowel externe als interne betrokkenen die in contact staan met en persoonsgegevens delen met de provincie Drenthe. Het privacybeleid is van toepassing op alle taken en processen waar Provinciale Staten (PS) en Gedeputeerde Staten (GS) van de provincie Drenthe verantwoordelijk voor zijn en heeft betrekking op de persoonsgegevens van personen van wie de provincie Drenthe gegevens verwerkt (of laat verwerken), voor zover dit onder het gezag van PS of GS valt. Het privacybeleid wordt waar nodig verder uitgewerkt in specifieke (beleids)documenten (zoals de privacyverklaring voor externe betrokkenen op de website van de provincie Drenthe en voor interne betrokkenen op Huisnet en het protocol meldplicht datalekken) en (beheers- en beveiligings)maatregelen rondom privacy. Zowel organisatiebreed als indien nodig per domein of voor de Statengriffie.

Het privacybeleid raakt zowel de ambtelijke als de bestuurlijke organisatie van de provincie Drenthe.

Ideale situatie
In dit document wordt de ideale situatie rondom privacybeleid geschetst. De provincie Drenthe streeft een zo hoog mogelijk niveau van privacy(bescherming) na. Binnen de wet- en regelgeving worden afwegingen gemaakt om de juiste balans te vinden tussen het reduceren van de risico's, de taakstelling van de organisatie, een praktische manier van werken en de persoonlijke levenssfeer van betrokkenen.

Relatie met andere (beleids)kaders van de provincie Drenthe
Het privacybeleid van de provincie Drenthe staat in nauwe relatie met het Beleidskader informatiebeveiliging van de provincie Drenthe. Hierin is het informatiebeveiligingsbeleid van de provincie Drenthe vastgelegd. Het informatiebeveiligingsbeleid heeft betrekking op de beveiliging van informatie(verwerking) en geeft een kader voor maatregelen op het gebied van informatiebeveiliging. Dit kader wordt gevormd door de vastlegging van de uitgangspunten van beleid, de inrichting van de beveiligingsorganisatie en de beschrijving van de processtappen die cyclisch in de tijd worden doorlopen. Een goede informatiebeveiliging geeft meer bescherming van de privacy.

Doorontwikkeling
Dit document over privacybeleid is bedoeld als duurzaam kader, maar waar nodig vinden in de toekomst aanpassingen plaats en wordt dit document verder doorontwikkeld en zonodig aangepast aan veranderde wet- en regelgeving. Ook de steeds verdergaande digitalisering, met nieuwe technologieën, kan in de toekomst andere eisen stellen aan de bescherming van gegevens en privacy. Dit beleidskader wordt minimaal elke vijf jaar tegen het licht gehouden op actualiteit en waar nodig aangepast. Indien nodig gebeurt dit eerder op een daartoe geëigend moment.

Voor wie is dit?
Dit document is bedoeld voor de verwerkingsverantwoordelijke, de verwerker en zowel externe als interne betrokkenen waarvan persoonsgegevens bij de provincie Drenthe worden verwerkt en/of bewaard. Het geeft inzicht in hoe de provincie Drenthe het beleid rondom privacy voert.

1.4 Context

Het privacybeleid van de provincie Drenthe dient in samenhang te worden gezien met de Nederlandse Overheid en Referentie Architectuur (NORA) en de Provinciale EnTerprise Referentie Architectuur (PETRA). De NORA richt zich op de publieke sector en geldt voor alle domeinen en bestuurslagen in Nederland. Vanuit de NORA wordt samengewerkt met het Centrum Informatiebeveiliging en Privacybescherming (CIP). Als uitvloeisel daarvan zijn in de NORA privacyprincipes geformuleerd. Deze hangen nauw samen met de AVG. Zie bijlage 1 voor de privacyprincipes uit de NORA. De PETRA (Interprovinciaal Overleg (IPO)) maakt onderdeel uit van de 'NORA-familie'.

1.5 Opbouw document

Na dit eerste algemene hoofdstuk gaat hoofdstuk 2 in op de doelstellingen en beleidsuitgangspunten van het privacybeleid van de provincie Drenthe. In hoofdstuk 3 worden het proces van het privacybeleid, de borging ervan en de verdeling van verantwoordelijkheden beschreven. In hoofdstuk 4 komt de inhoudelijke kern van het privacybeleid aan bod, met daarin principes en maatregelen. Hoofdstuk 5 is een kort afsluitend hoofdstuk. In de bijlagen zijn de privacyprincipes uit de NORA opgenomen. Ook wordt ingegaan op het proces, de borging en een samenvatting van de verdeling van de verantwoordelijkheden. In de bijlagen wordt ook ingegaan op de bronnen die geraadpleegd zijn bij het opstellen van dit privacybeleid. Waar nodig zijn in dit document voetnoten opgenomen.

2. Doelstelling en beleidsuitgangspunten privacybeleid

2.1 Inleiding

In dit hoofdstuk wordt achtereenvolgens ingegaan op de doelstelling en de beleidsuitgangspunten van het privacybeleid van de provincie Drenthe.

2.2 Doelstelling

De doelstelling van het privacybeleid van de provincie Drenthe luidt:
“Het bieden van een kader met beleidsuitgangspunten dat beoogt te bewerkstelligen dat de privacy van zowel externe als interne betrokkenen bij de provincie Drenthe wordt gewaarborgd.”

Met dit Beleidskader privacybeleid provincie Drenthe worden Europese en landelijke wetgeving over privacy en bescherming van persoonsgegevens zoveel mogelijk nader ingevuld voor de provincie Drenthe, ertoe leidend dat de provincie Drenthe zo zorgvuldig en veilig mogelijk omgaat met persoonsgegevens en privacy van betrokkenen.

2.3 Beleidsuitgangspunten

1. Ga uit van wet- en regelgeving rondom privacy
De provincie Drenthe gaat bij het privacybeleid in ieder geval uit van de Europese en landelijke wettelijke wet- en regelgeving rondom privacy.

Ten tijde van het opstellen van dit privacybeleid gaat het hierbij in ieder geval om:
- Algemene verordening gegevensbescherming (AVG).
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

Ook de ten tijde van het opstellen van dit privacybeleid de Wet open overheid en de in ontwikkeling zijnde Wet digitale overheid (Wdo) spelen hierbij een rol.

2. Ga uit van basiskaders
In ieder geval wordt uitgegaan van de volgende basiskaders voor het privacybeleid.
1. Nederlandse Overheids Referentie Architectuur (NORA).
2. Provinciale EnTerprise Referentie Architectuur (PETRA).
3. BurgerServiceCode (een gedragscode met tien kwaliteitseisen voor de relatie tussen burger en overheid in de moderne (digitale) samenleving).
4. Kwaliteitscirkel van Deming (met *Plan-Do-Check-Act*-cyclus).

3. Het privacybeleid is van toepassing op de persoonsgegevens van externe en interne betrokkenen bij de provincie Drenthe
Het privacybeleid is van toepassing op de persoonsgegevens van externe en interne betrokkenen bij de provincie Drenthe. Bij externe betrokkenen kan bijvoorbeeld gedacht worden aan inwoners en contactpersonen van andere overheden, bedrijven en instellingen. Bij interne betrokkenen wordt gedoeld op bestuurders en werknemers van de provincie Drenthe (zowel in vaste als in tijdelijke dienst als op inhuurbasis vanuit een derde partij).

4. Afwijking van het privacybeleid vereist advisering door de FG
Afwijking van het privacybeleid door GS, PS of organisaties vereist advisering door de FG. Dit gebeurt schriftelijk. De FG is toezichthouder op de consistente uitvoering van het privacybeleid en rapporteert hierover waar het GS en organisatie betreft aan de directie en specifiek de provinciesecretaris. Waar het PS en organisatie betreft vindt rapportage plaats aan de Statengriffier.

5. Bescherming van de privacy is een lijnverantwoordelijkheid
Het privacybeleid maakt onderdeel uit van het integraal management. De manager is verantwoordelijk voor de naleving van het privacybeleid en de te treffen maatregelen in het eigen domein. De

perdomein aanwezige privacy ambassadeurs kunnen daarbij ondersteunen. De Algemeen directeur is ambtelijk eindverantwoordelijk voor het privacybeleid. Daar waar het de statengriffie betreft, is de Statengriffier ambtelijk eindverantwoordelijk.

6. Bescherming van de privacy is een persoonlijke verantwoordelijkheid
De persoonlijke verantwoordelijkheid van bestuurders en medewerkers van de provincie Drenthe ten aanzien van het privacybeleid is vastgelegd in gedragscodes, reglementen en bruikleenovereenkomsten met betrekking tot ICT[14]-apparatuur en dienstauto's. Zo legt eenieder een (ambts)eed af en is er integriteitsbeleid (integer omgaan met persoonsgegevens). Ook worden bijvoorbeeld ICT-bedrijfsmiddelen (waarop persoonsgegevens kunnen staan) niet uitgeleend aan derden. Er is een privacy- en gebruiksreglement bedrijfsmiddelen provincie Drenthe en een regeling dienstauto's.

7. Maatregelen voor bescherming van de privacy moeten controleerbaar zijn en zoveel mogelijk technisch gehandhaafd worden
Als er maatregelen voor bescherming van de privacy worden ingevoerd, wordt vooraf nagegaan op welke wijze de naleving en het functioneren ervan kunnen worden gecontroleerd. Technische middelen voor handhaving van maatregelen voor bescherming van privacy voorkomen zoveel mogelijk afhankelijkheid van organisatorische en procedurele maatregelen. Nadrukkelijk wordt hieraan toegevoegd dat risico mitigerende maatregelen zich niet beperken tot technische, want juist het menselijk handelen zal altijd een rol spelen.

8. Het privacybewustzijn en de morele oordeelsvorming van alle bestuurders en medewerkers wordt actief en structureel gestimuleerd
Van belang is dat het privacybeleid bekend is bij de bestuurders en medewerkers bij de provincie Drenthe. Het resultaat van het privacybeleid hangt voor een groot deel af van het privacybewustzijn van bestuurders en medewerkers van de provincie Drenthe en van betrokkenen. Het is daarom van belang dit bewustzijn omtrent de bescherming van de privacy en de morele oordeelsvorming op dat gebied actief en structureel te bevorderen. Te denken valt bijvoorbeeld aan een privacyverklaring, zowel op de website van de provincie Drenthe als op Huisnet. Het privacybewustzijn wordt verder vooral gevormd door het iBewustzijn, gekoppeld aan het informatiebeveiligingsbeleid. In het FG-verslag kan de FG aandacht besteden aan de situatie op dat moment omtrent privacybewustzijn.

9. De beveiliging van privacy wordt standaard in overeenkomsten tussen de provincie Drenthe en externe partijen vastgelegd
De provincie Drenthe laat standaard in overeenkomsten vastleggen dat de partijen onderling de privacy van betrokkenen beschermen en dat de externe partij bij het verrichten van werkzaamheden voor de provincie Drenthe het privacybeleid van de provincie Drenthe hanteert. Waar nodig ziet de FG dan wel de Coördinator Informatiebeveiliging (CIB) hierop toe en/of adviseert hierover.

Als een verwerkingsverantwoordelijke andere partijen inschakelt om persoonsgegevens voor hem of haar te verwerken, dan moet hij of zij met deze organisaties 'verwerkersovereenkomsten' afsluiten. Het gaat daarbij strikt om gevallen waarin de verwerker opdracht krijgt van de organisatie die verantwoordelijk is voor de verwerking van de persoonsgegevens; de verantwoordelijke opdrachtgever bepaalt wat er moet gebeuren met de gegevens en hoe.

Bij gezamenlijke verwerkingsverantwoordelijkheid - gegevensuitwisseling tussen twee verwerkingsverantwoordelijken - is het eveneens aan te bevelen een overeenkomst te sluiten waarin de betrokken partijen afspraken over de gegevensdeling vastleggen.

10. Overtreding privacybeleid kan leiden tot overleg dan wel sancties
In geval van overtreding van het privacybeleid worden betrokkenen hierop persoonlijk aangesproken. Bij ernstige (zeker bewuste) overtreding wordt zonodig gehandeld overeenkomstig de cao provinciale sector en de Ambtenarenwet. De mogelijkheid tot het opleggen van sancties geeft aan dat naleving van het privacybeleid niet vrijblijvend is, maar bindend voor alle medewerkers van de provincie Drenthe.

[14] ICT: informatie- en communicatietechnologie.

11. Datalekken bij de provincie Drenthe worden indien nodig gemeld bij de AP
Er is een meldplicht datalekken. Deze houdt in dat de provincie Drenthe direct een melding moet doen bij de AP zodra de provincie Drenthe een ernstig datalek heeft. Soms moet het datalek ook worden gemeld aan de betrokkenen, namelijk de personen van wie de persoonsgegevens zijn gelekt. Datalekken die gemeld worden bij de AP, worden via het daartoe bedoelde meldloket datalekken van de AP gemeld.

De provincie Drenthe heeft een protocol meldplicht datalekken waarin staat hoe omgegaan wordt met het melden van datalekken.

12. Jaarlijkse lijnverantwoording
De betrokken domeinen, concernprogramma's of concernprojecten dienen zich jaarlijks richting de directie te verantwoorden over de voortgang van de activiteiten op het gebied van privacy, die opgenomen zijn in het beleid. De Statengriffie biedt jaarlijks een rapportage aan het presidium van PS aan. Dit gebeurt waar nodig in samenspraak met de FG.

13. Jaarlijks FG-verslag
De FG is verantwoordelijk voor een jaarlijks FG-verslag (zonodig in overleg met de CIB), te agenderen in het directieoverleg en te bespreken met de Algemeen directeur en waar aan de orde met de Statengriffier. Het FG-verslag gaat daarna ter informatie naar GS, het presidium van PS en de Ondernemingsraad (OR). In het FG-verslag staat de stand van zaken van het privacybeleid in het afgelopen jaar, met waar mogelijk en nodig een vooruitblik naar het komende jaar dan wel de verdere toekomst.
Datalekken krijgen specifieke aandacht binnen het jaarverslag. De FG moet namelijk rapporteren over datalekken richting directie en specifiek de Algemeen directeur of de Statengriffier.

3. Proces, borging en verdeling verantwoordelijkheden privacybeleid

3.1 Inleiding

In dit hoofdstuk wordt achtereenvolgens ingegaan op het proces, de borging en de verdeling van verantwoordelijkheden rondom het privacybeleid van de provincie Drenthe. Voor het proces, de borging en een samenvatting van de verdeling van de verantwoordelijkheden in een matrix wordt verwezen naar bijlage 2.

3.2 Verdeling verantwoordelijkheden

3.2.1 College van Gedeputeerde Staten (GS) en Provinciale Staten (PS)

Het college van GS en PS zijn samen verantwoordelijk voor de naleving van het privacybeleid van de provincie Drenthe, ieder voor het eigen deel.

Het college van GS stelt het beleidskader privacy en eventuele wijzigingen daarin bestuurlijk vast en is daarmee bestuurlijk eigenaar van dit document. PS sluiten daarbij aan en worden geïnformeerd over wijzigingen. PS stellen daarmee geen eigen privacybeleid op, maar hebben wel aantoonbaar uitgangspunten vastgesteld voor de uitvoering van de eigen werkzaamheden in lijn met de AVG.

Waar nodig legt het college van GS over de uitvoering van het privacy beleid verantwoording af aan PS.

3.2.2 Algemeen directeur en statengriffier

Op ambtelijk niveau is de Algemeen directeur verantwoordelijk voor de borging van integriteit, in samenhang daarmee is ook de ambtelijke eindverantwoordelijkheid van de Algemeen directeur voor het privacybeleid te zien. De Algemeen directeur is ambtelijk eindverantwoordelijk voor de strategiebepaling (kaderstelling), sturing op en uitvoering van het privacybeleid. De Algemeen directeur is verantwoordelijk voor de voorbereiding van het privacybeleid en de wijzigingen daarop, ten behoeve van de vaststelling daarvan door GS. Dit doet de Algemeen directeur na beraad in de directie en na advisering door de FG. Minimaal één keer per jaar bespreekt de Algemeen directeur samen met de FG de naleving van de privacyregelgeving en het privacybeleid aan de hand van het jaarlijkse FG-verslag. Daarnaast zorgt de Algemeen directeur ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De Algemeen directeur stelt de FG in staat om met voldoende autonomie en middelen de taken goed uit te kunnen oefenen. De Algemeen directeur is ambtelijk eigenaar van dit document. Voorgaande is van overeenkomstige toepassing op de statengriffier, voor zover de bevoegdheid reikt. De statengriffier handelt op overeenkomstige wijze richting de FG voor zover het PS en de Statengriffie betreft.

3.2.3 Management

Het management is op uitvoeringsniveau verantwoordelijk voor een privacybestendige bedrijfsvoering en gegevenswisseling met derden. Zij zorgen voor uitvoering van en controle op naleving van het privacybeleid binnen hun eigen domein. Uiteraard voor zover passend binnen hun mandaat en dit beleidskader. Zij leggen hierover verantwoording af aan de directie en specifiek de Algemeen directeur en waar nodig ook via de Algemeen directeur aan GS. Het management is verantwoordelijk voor het verzamelen en/of verwerken van persoonsgegevens die betrekking hebben op de werkprocessen van het eigen domein. Naleving van regels op het gebied van gegevensbescherming is de verantwoordelijkheid van de verwerkingsverantwoordelijke en/of de verwerker. De verantwoordelijke en de verwerker zien er volgens de AVG[15] op toe dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

[15] Artikel 38 AVG.

3.2.4 Medewerkers

De medewerkers voeren veelal de werkprocessen van het eigen domein of de Statengriffie daadwerkelijk uit, binnen de kaders van het privacybeleid. Veelal is het ook een medewerker die de persoonsgegevens daadwerkelijk verwerkt. De medewerkers zorgen ervoor dat zij volgens de regels uit dit beleidskader en de geldende wet- en regelgeving omgaan met persoonsgegevens. Naleving van regels op het gebied van gegevensbescherming is de verantwoordelijkheid van de verwerkingsverantwoordelijke en/of de verwerker. De verantwoordelijke en de verwerker zien er volgens de AVG[16] op toe dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Als sprake is van een nieuwe verwerking van persoonsgegevens meldt de betrokken medewerker dit bij de FG, ook voor opname in het verwerkingsregister. Als er sprake is van een datalek, meldt de betrokken medewerker dit via het daartoe bestemde kanaal volgens het protocol meldplicht datalekken.

3.2.5 Privacy ambassadeur

Per domein en voor de Statengriffie zijn er medewerkers die privacy ambassadeur (pramba) zijn. De privacy ambassadeur fungeert als privacy-aanspreekpunt voor de collega's uit het domein, de privacy officer en de FG. De privacy ambassadeurs krijgen een basisopleiding AVG en informatiebeveiliging en komen regelmatig bijeen om ervaringen uit te wisselen en kennis te delen. De privacy ambassadeur heeft de volgende taken:

- De privacy ambassadeur is op de hoogte van de AVG-basisprincipes en draagt deze uit.
- De privacy ambassadeur signaleert of er nieuwe verwerkingen van persoonsgegevens ontstaan en levert de nodige gegevens hiervoor aan voor het verwerkingsregister; de privacy ambassadeur krijgt ook periodiek een seintje om de bestaande registraties te controleren en eventuele wijzigingen door te geven.
- De privacy ambassadeur levert een bijdrage aan bewustwording rondom privacy.
- Bij AVG-verzoeken ondersteunt de privacy ambassadeur (bepaald op basis van het intakegesprek dat de FG met de verzoeker voert) de FG bij het inventariseren en verzamelen van de relevante persoonsgegevens.
- De privacy ambassadeur is het eerste aanspreekpunt bij inhoudelijke vragen over privacy en de AVG.
- De privacy ambassadeur is alert op het ontstaan van potentiële datalekken en wijst collega's op de juiste meldprocedure.
- De privacy ambassadeur wordt betrokken bij beleidsvorming en fungeert als sparringpartner voor de FG en de CIB bij het ontwikkelen van privacy- en beveiligingsbeleid.
- De privacy ambassadeur kan desgevraagd meedenken of een verwerkersovereenkomst gesloten moet worden met een externe partij en kan de verantwoordelijke contacteigenaar adviseren bij het afsluiten ervan volgens het model.
- De privacy ambassadeur wijst domeingenoten op het bestaan van een pre-DPIA-checklist (pre-data protection impact assessment-checklist) om te bepalen of voor een (nieuw) project of proces een DPIA gehouden moet worden. De privacy ambassadeur kan het initiatief nemen tot, of een rol spelen bij, het houden van een DPIA binnen het werkgebied van het domein. In ieder geval wordt de privacy ambassadeur op de hoogte gesteld door de FG en de CIB over de voortgang en uitkomsten van een DPIA die het domein van de privacy ambassadeur raakt.

3.2.6 Functionaris Gegevensbescherming (FG) en privacy officer (PO)

Volgens de AVG[17] moet elke overheidsorganisatie verplicht een FG hebben, zo ook de provincie Drenthe. De FG heeft een wettelijke verantwoordelijkheid: "De FG houdt toezicht op en geeft advies over de verwerking van persoonsgegevens en heeft een geheimhoudingsplicht". De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wet- en regelgeving en het provinciale beleid op het gebied van privacy. Daarmee houdt de FG controle op de naleving van het privacybeleid en adviseert op het gebied van privacy. De privacy officer (PO) is de ambtelijk beheerder van dit document.

[16] Artikel 38 AVG.
[17] Artikel 37(1) AVG.

De AVG[18] stelt dat de FG wordt aangewezen op grond van zijn of haar professionele kwaliteiten en, in het bijzonder, zijn of haar deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn of haar vermogen de in de AVG[19] bedoelde taken te vervullen.

De FG heeft de volgende taken die mede voortvloeien uit de wettelijke verantwoordelijkheid:

- Informeren en adviseren van de verwerkingsverantwoordelijke en/of de verwerker en/of overige medewerkers over hun verplichtingen die voortvloeien uit de AVG en andere relevante privacywet- en regelgeving.
- Toezien op de naleving van de AVG, andere relevante privacywet- en regelgeving en het provinciale privacybeleid, waaronder het toewijzen van verantwoordelijkheden, het bewustmaken van en voorlichting geven aan betrokken medewerkers.
- (Het coördineren van) het uitvoeren van screenings dan wel audits rondom privacy, mogelijk in samenspraak met de CIB te koppelen aan het informatiebeveiligingsbeleid.
- Adviseren over gegevensbeschermingseffectbeoordelingen/data protection impact assessments (DPIA's) en toezien op de uitvoering daarvan.
- Samenwerken met en optreden als provinciaal contactpunt voor de AP.
- Rapporteren over de uitvoering van zijn of haar taken; de FG brengt rechtstreeks verslag uit aan de provinciesecretaris.
- Helpen privacyklachten tot een goed einde te brengen (ombudsfunctie).
- Bij privacy incidenten adviseren over de ernst en omvang.
- Beheer van en toezien op het verwerkingsregister.
- Lid van het platform integriteit

De FG houdt bij de uitvoering van zijn of haar taken rekening met het aan verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden.

Overigens is de FG niet persoonlijk verantwoordelijk wanneer de AVG niet nageleefd wordt. De AVG[20] maakt duidelijk dat het de verwerkingsverantwoordelijke of de verwerker is die erop toe dient te zien en moet kunnen aantonen dat de verwerking aan de voorwaarden van de wet- en regelgeving voldoet. Naleving van regels op het gebied van gegevensbescherming is de verantwoordelijkheid van de verwerkingsverantwoordelijke en/of de verwerker.

De FG moet volgens de AVG[21] de nodige ruimte krijgen voor professionele uitvoering van zijn of haar taken. Dit houdt onder andere het volgende in:

- PS, GS, de provinciesecretaris, de statengriffier, de managers en/of de betrokken medewerkers zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- De FG wordt bij de vervulling van zijn of haar taken ondersteund door hem of haar toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem of haar de nodige middelen ter beschikking te stellen voor het vervullen van deze taken.
- De FG wordt in beginsel niet geïnstrueerd over uitvoering van taken of gestraft of ontslagen voor de uitvoering van zijn of haar taken. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker.
- Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten.
- De FG is met betrekking tot de uitvoering van zijn of haar taken tot geheimhouding of vertrouwelijkheid gehouden.
- De FG kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.
- De zienswijze van de FG is zwaarwegend bij de naleving van de privacywetgeving door de provincie Drenthe.

Zoals al bij de Algemeen directeur aangegeven: minimaal één keer per jaar bespreekt de Algemeen directeur samen met de FG de naleving van de privacyregelgeving en het privacybeleid aan de hand van het jaarlijks FG-verslag. Dit geldt ook m.b.t. de Statengriffier.

[18] Artikel 37(5) AVG.
[19] Artikel 39 AVG.
[20] Artikel 24(1) AVG.
[21] Artikel 38 AVG.

Behalve de FG is er een privacy officer bij de provincie Drenthe. De privacy officer is een daartoe aangewezen jurist met privacytaken in het verlengde van de FG; deze jurist draagt zorg voor de dagelijkse gang van zaken rondom privacybeleid. De FG en de privacy officer werken nauw samen. De privacy officer is de eerste vervanger van de FG.

3.2.7 Coördinator Informatiebeveiliging (CIB)

De CIB heeft verantwoordelijkheden ten aanzien van het informatiebeveiligingsbeleid en heeft vanuit daar een nauwe relatie met het privacybeleid. De CIB is betrokken bij de beveiliging van persoonsgegevens.

4. Inhoud privacybeleid

4.1 Inleiding

In dit hoofdstuk wordt het privacybeleid van de provincie Drenthe beschreven. Als zoveel mogelijk nadere invulling van de Europese en landelijke wetgeving. In dit hoofdstuk staan de principes die de provincie Drenthe hanteert bij het omgaan met persoonsgegevens en de maatregelen die de provincie Drenthe treft. Bij het opstellen van dit hoofdstuk is als basis de Privacy Baseline[22] van het Centrum Informatiebeveiliging en Privacybescherming (CIP), in relatie tot de NORA, gebruikt. Waar nodig aangepast dan wel aangevuld voor de situatie in de provincie Drenthe. De in dit beleidskader opgenomen privacybeleid is te beschouwen als een gids voor de provincie Drenthe voor het omgaan met persoonsgegevens, maar is niet te beschouwen als een vervanger van de Europese en landelijke wetgeving.

4.2 Principes en maatregelen privacybeleid

In het algemeen geldt dat het privacybeleid[23] wordt ingepast in de reguliere bedrijfsvoering van de provincie Drenthe. Daarbij staan de volgende zogenoemde ACT-doelen centraal: Afscherming, Corrigeerbaarheid en Transparantie.

- Afscherming: persoonsgegevens worden afgeschermd voor het gebruik voor andere doelen dan de doelen waarvoor ze mogen gebruikt.
- Corrigeerbaarheid: voor elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens aan te passen of te vernietigen, indien de verwerking niet voldoet aan de eisen; bijvoorbeeld in geval van onjuiste informatie of als er geen noodzaak meer is om de informatie te bewaren.
- Transparantie: over elke verwerking van persoonsgegevens is de volgende informatie beschikbaar: de verantwoordelijken, categorieën persoonsgegevens, categorieën van betrokkenen, categorieën van ontvangers, doelbinding, wettelijke grondslag, bewaartermijnen, beveiligingsmaatregelen en organisatorische en technische inrichting van de verwerking van de persoonsgegevens.

Dit betekent dat als de provincie Drenthe een initiatief op welk beleidsterrein dan ook neemt, waar nodig de privacyaspecten die daarbij een rol spelen in beeld brengt volgens de principes van dit privacybeleid. Daarbij wordt ook rekening gehouden met de aard, omvang, context en het doel van de verwerking van persoonsgegevens en de risico's voor betrokkenen (hoe groot is de kans dat er zich daadwerkelijk een schending van de privacy voordoet en als dat onverhoopt mocht gebeuren, hoeveel hinder en schade geeft dit). Waar nodig is de FG betrokken bij het in beeld brengen hiervan.

In de volgende tekst staan per ACT-doel de principes van het privacybeleid beschreven. Per principe wordt aangegeven welke maatregelen nodig zijn. Soms is het bij het nemen van maatregelen nodig gegevens in te vullen in het zogenoemde verwerkingsregister.

[22] De Privacy Baseline geeft organisaties concrete handvatten om persoonsgegevens op een juiste manier te beschermen. In de Privacy Baseline zijn de eisen van de AVG en UAVG vertaald naar concrete, hanteerbare normen die duidelijk maken wat organisaties moeten doen om in overeenstemming met de wet de privacy van de betrokkenen te waarborgen.
[23] Referentie privacybeleid: AVG: artikel 5, 24, 40, UAVG: artikel. 2, 4, 78 en 157.

Samenvatting principes privacybeleid voor het verzamelen en/of (verder) verwerken van persoonsgegevens

1. Grondslag
2. Doelbinding
3. Minimalisatie van hoeveelheid en soort gegevens
4. Bewaartermijn
5. Beveiliging
6. Gegevens worden pas gedeeld met een verwerker wanneer een verwerkersovereenkomst is gesloten
7. Goede kwaliteit: juist en actueel
8. Transparant: informatieplicht en rechten van betrokkenen
9. Zorgvuldig omgaan met geautomatiseerde verwerkingen (profilering, big data, tracking en tracing, camera's)
10. Privacy by design en privacy by default
11. Gegevensbeschermingseffectbeoordeling/data protection impact assessment (DPIA)
12. Verwerkingsregister
13. Indien nodig datalek melden bij AP en betrokkenen informeren

Afscherming

Principe 1: De provincie Drenthe verzamelt en/of verwerkt alleen persoonsgegevens als er een grondslag[24] voor is, welke wordt vastgelegd in het verwerkingsregister

Voor verwerking van persoonsgegevens is een grondslag noodzakelijk. Verwerking van persoonsgegevens mag alleen als dit gebaseerd is op een van de zes grondslagen uit de AVG (artikel 6), namelijk:

- Wanneer de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden[25] [26].
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel van is.
- Om een verplichting na te komen die in de wet staat.
- Om een ernstige bedreiging van de gezondheid van de betrokkene te bestrijden[27].
- Voor de goede vervulling van de provinciale/publieke taak.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. NB. Vanwege het feit dat de wetgever de rechtsgrond bepaalt voor de verwerking van persoonsgegevens door overheidsinstanties, geldt de rechtsgrond 'gevaardigd belang' niet voor verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken.

De grondslag dient te worden vastgelegd in het verwerkingsregister. In beginsel zal de provincie gegevens verwerken op grond van een wettelijke bevoegdheid in verband met publieke taken.

Maatregel:

[24] Referentie doelbinding: AVG: artikel 5, 6, 9, 10, 22, 23 en UAVG: artikel 22, 23, 24,25, 26, 27, 28, 29, 30, 31, 32, 33, 40, 46.
[25] De verwerkingsverantwoordelijke stelt bij elke verzameling van persoonsgegevens tijdig informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, in voorkomende gevallen toestemming kan geven voor de verzameling en/of (verdere) verwerking. Voor de provincie Drenthe is het verkrijgen van toestemming door betrokkene overigens zelden nodig omdat de provincie Drenthe veelal handelt op basis van een wettelijke grondslag of omdat de provincie Drenthe een publiek belang heeft.
[26] Voor een geldige toestemming van de betrokkene gelden de volgende voorwaarden:
- Vrij: de toestemming moet vrij zijn gegeven.
- Specifiek en geïnformeerd.
- Ondubbelzinnig: er mag geen twijfel bestaan over het feit dat de betrokkene toestemming geeft.

[27] De AVG geeft aan: de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen. Vaak gaat het hier om de gezondheid.

- Stel per cluster van te verzamelen en/of verwerken persoonsgegevens de grondslag ervan vast en leg deze vast in het verwerkingsregister.

Principe 2: Voor elke verzameling en/of verwerking van persoonsgegevens door de provincie Drenthe is doelbinding[28] nodig, welke wordt vastgelegd in het verwerkingsregister

Volgens de AVG mogen persoonsgegevens alleen verzameld en/of verwerkt worden als daarvoor een gerechtvaardigd doel is vastgesteld; er is zogenoemde doelbinding. Dit wordt per cluster van te verwerken persoonsgegevens voorafgaand aan het verzamelen van persoonsgegevens vastgelegd in het verwerkingsregister. De gegevens mogen niet voor andere doelen verwerkt worden, tenzij er sprake is van een verenigbaar doel. Voor de uitvoering van diverse provinciale taken zijn de doelen voor het verwerken in een wet vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Maatregelen:

- Stel per cluster van te verzamelen en/of verwerken persoonsgegevens het doel ervan vast, voorafgaand aan het verzamelen van de persoonsgegevens, en leg dit vast in het verwerkingsregister.

Principe 3: De provincie Drenthe minimaliseert bij het verzamelen en/of verwerken van persoonsgegevens de hoeveelheid en het soort gegevens zoveel mogelijk

Bij het verzamelen en/of verwerken van persoonsgegevens worden de hoeveelheid en het soort gegevens beperkt (artikel 5 onder c AVG). Er worden zo minimaal mogelijk persoonsgegevens verzameld en/of verwerkt. Dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verzameling en/of verwerking.

Maatregel:

- Verzamel en/of verwerk een zo minimaal mogelijke hoeveelheid en soort persoonsgegevens die voor het doel noodzakelijk zijn; controleer hierop bij aanvang en tijdens het verzamelen en/of verwerken van persoonsgegevens.

Principe 4: De provincie Drenthe bewaart persoonsgegevens niet langer dan strikt noodzakelijk[29] voor de dienstverlening of wettelijke verplichting; de bewaartermijn[30] wordt vastgelegd in het verwerkingsregister

Persoonsgegevens mogen niet langer bewaard worden dan strikt noodzakelijk voor de dienstverlening of wettelijke verplichting. Als in sectorspecifieke wetgeving een bewaartermijn is vastgelegd, dan geldt die bewaartermijn.

Er is op grond van de AVG geen concrete bewaartermijn voor persoonsgegevens. Persoonsgegevens mogen echter alleen bewaard worden als identificeerbare gegevens voor zolang het nodig is voor de doeleinden waarvoor ze verzameld en/of verwerkt worden[31].

[28] Referentie doelbinding: AVG: artikel 5, 6, 9, 10, 22, 23 en UAVG: artikel 22, 23, 24,25, 26, 27, 28, 29, 30, 31, 32, 33, 40, 46.
[29] Referentie bewaren van persoonsgegevens: AVG: artikel 5, lid 1e UAVG: artikel 43.
[30] De bewaartermijn is de maximale periode waarin de persoonsgegevens noodzakelijk worden bewaard om het doel van de verwerking te bereiken of niet langer dan de termijn die verankerd is in sectorspecifieke wetgeving.
[31] De AVG is niet van toepassing op de persoonsgegevens van overleden personen (artikel 27 AVG). Lidstaten kunnen regels vaststellen over de verwerking van persoonsgegevens van overleden personen.

Maatregelen:

- Bepaal per cluster van te verzamelen en/of verwerken persoonsgegevens de (wettelijke) bewaartermijn; ga daarvoor na hoe lang de gegevens nodig zijn voor het doel waarvoor deze worden verzameld of gebruikt. Kijk of er concrete bewaartermijnen in wetten zijn aangegeven waar de provincie Drenthe zich aan moet houden. Bijvoorbeeld in de archiefwetgeving of de belastingwetgeving; meer specifiek in de krachtens de archiefwetgeving vastgestelde provinciale selectielijst voor archiefbescheiden waarin alle relevante wetgeving (waaronder ook belastingwetgeving) al is verwerkt. Leg de bewaartermijn vast in het verwerkingsregister.
- Tref maatregelen waardoor de bewaartermijn niet wordt overschreden. De verantwoordelijke bepaalt na elke verwerking van persoonsgegevens of er nog redenen zijn om de betreffende persoonsgegevens te bewaren.
- Als de bewaartermijn verloopt verwijdert, vernietigt of anonimiseert de verantwoordelijke de persoonsgegevens.
- Er is controle op de verwijdering, vernietiging of anonimisering. Archiefwetgeving bepaalt de wijze en termijnen van bewaren van informatie. De provinciearchivaris ziet toe op tijdige en correcte vernietiging van daartoe in aanmerking komende archiefbescheiden. Let wel: het gaat digitaal dan om *erasure* en niet om *deletion*, dus geen verwijdering maar vernietiging. Verder autoriseert de provinciearchivaris, na controle, ook de vernietiging namens GS.
- Softwarematige verwijdering of anonimisering en vernietiging van gegevensdragende hardware wordt bij voorkeur door een specialist of een gespecialiseerde organisatie gedaan. Als persoonsgegevens zijn vastgelegd op een ‘read only’ gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, maar waarvan gegevens wel kunnen worden gekopieerd, tref dan maatregelen zodat de gegevens op geen enkele wijze meer kunnen worden ingezien, gebuikt of anderszins verwerkt. Stel de betrokkene op de hoogte bij onmogelijkheid van verwijdering of anonimisering. Het bewaren van persoonsgegevens op een ‘read only’ gegevensdrager is overigens niet de enige manier waarop persoonsgegevens tóch bewaard kunnen worden. Ook de provinciearchivaris is gerechtigd om vanwege het belang, zoals omschreven in het archiefbesluit, het vernietigen van (onderdelen van) informatie tegen te houden. Uiteraard kan er dan wel krachtens de archiefwetgeving een beperking aan de openbaarheid van maximaal 75 jaar worden gesteld.

Principe 5: De provincie Drenthe zorgt voor een passende beveiliging[32] van persoonsgegevens conform het vigerende informatiebeveiligingsbeleid; leg de beveiligingsmaatregelen en categorieën ontvangers van persoonsgegevens vast in het verwerkingsregister

Om verantwoord om te kunnen gaan met persoonsgegevens is een adequate beveiliging van de gegevens nodig.

Op grond van de AVG moet de provincie Drenthe dan ook passende technische en organisatorische maatregelen nemen om de persoonsgegevens te beveiligen.

Voor de beveiliging van de persoonsgegevens geldt het vigerende informatiebeveiligingsbeleid van de provincie Drenthe.

[32] Referentie beveiliging: AVG: artikel 32, UAVG: Mvt §5.2.4.

Maatregelen:

- Voer een actueel informatiebeveiligingsbeleid; hiervoor is of wordt een actueel Beleidskader informatiebeveiligingsbeleid vastgesteld.
- De verwerkingsverantwoordelijke en de verwerker zorgen ervoor dat de toegang tot de persoonsgegevens beperkt is tot diegenen die toegang moeten hebben voor het uitvoeren van hun functie of taken of tot diegenen die daartoe wettelijk zijn gehouden.
- Geef de persoonsgegevens alleen aan de ontvangers (degenen waaraan de gegevens worden verstrekt) die de persoonsgegevens nodig hebben. Leg de categorieën ontvangers vast in het verwerkingsregister.
- Beveilig persoonsgegevens fysiek dan wel organisatorisch tegen diefstal en ongewenste toegang conform het informatiebeveiligingsbeleid. Betrek hierbij zonodig de CIB. Leg de beveiligingsmaatregelen vast in het verwerkingsregister.

Principe 6: De provincie Drenthe deelt gegevens pas met een verwerker wanneer een verwerkersovereenkomst is gesloten

Doorgifte van persoonsgegevens kan bijvoorbeeld gebeuren aan verwerker(s) en aan andere verwerkingsverantwoordelijke(n). De provincie Drenthe geeft geen gegevens door aan organisaties buiten de Europese Unie.

Bij doorgifte aan een derde partij als verwerker moeten er afdoende garanties zijn dat er verwerkt wordt volgens de AVG. De verwerker moet passende technische en organisatorische maatregelen treffen zodat deze voldoet aan de AVG en de bescherming van de rechten van de betrokkene gewaarborgd is.

De verwerking door een derde partij (als verwerker) namens de provincie Drenthe moet in een overeenkomst, ook wel een verwerkersovereenkomst genoemd, worden vastgelegd.

Binnen de provincie Drenthe wordt gewerkt met een model verwerkersovereenkomst; dit model is conform de AVG en is afgestemd op het inkoopbeleid. Het is aan degene die de inkoop doet om ervoor te zorgen dat de verwerkersovereenkomst wordt afgesloten. Voor de inkoopopdracht, die via het domein rondom inkoop gaat, is het via het proces geborgd dat er een check op wordt gedaan. Daar waar mogelijk wordt gebruik gemaakt van dit model. Indien verwerkers zelf met een overeenkomst komen, zal die moeten worden getoetst aan interne normen.

Maatregelen:

- Werk met een model verwerkersovereenkomst, welke standaard wordt meegestuurd bij bijvoorbeeld aanbestedingen[33].
- Als persoonsgegevens worden overgedragen aan een verwerker, dan wordt een verwerkersovereenkomst gesloten die in een register worden opgeslagen. Leg hierin garanties vast, zodanig dat aangetoond kan worden dat ook bij en na de overdracht aan de AVG wordt voldaan. Leg ook onderlinge verantwoordelijkheden vast en stel de betrokkene hiervan op de hoogte. De verwerkersovereenkomst wordt in schriftelijke vorm (dit kan ook elektronisch zijn) vastgelegd.
- Wanneer verwerking niet had mogen plaatsvinden, dan wordt door de verwerkingsverantwoordelijke de doorgifte van persoonsgegevens beëindigd en worden de AP en de betrokkenen hierover geïnformeerd.
- Laat de vraag of een verwerkersovereenkomst noodzakelijk is onderdeel uitmaken van de inkoop- en aanbestedingsprocedure van de provincie Drenthe.

Corrigeerbaarheid

Principe 7: De provincie Drenthe verzamelt en/of verwerkt alleen persoonsgegevens die van een goede kwaliteit[34] ofwel juist en actueel zijn

[33] Met verbonden partijen worden aparte afspraken gemaakt. Bij kleinere dienstverleners/inkopen moeten de teams er zelf aan denken om een verwerkersovereenkomst af te sluiten.
[34] Referentie kwaliteitsmanagement: AVG: artikel 7 lid 3, 11 lid 2, 12, 16, 17, 18, 19, 20, 21, 22, 23, UAVG: -.

Volgens de AVG moeten maatregelen worden getroffen om te waarborgen dat de te verzamelen en/of verwerken persoonsgegevens van een goede kwaliteit ofwel juist en actueel zijn. Indien nodig worden persoonsgegevens gecorrigeerd of geactualiseerd. De provincie Drenthe neemt redelijke maatregelen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist of niet actueel zijn te wissen of te rectificeren. De provincie Drenthe zorgt ervoor dat gegevensverwerking correct en in overeenstemming met de wens van de betrokkene is.

De provincie Drenthe wist op verzoek van de betrokkene de hem of haar betreffende persoonsgegevens wanneer er sprake is van een van de volgende gevallen[35]:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld en/of verwerkt.
- De betrokkene trekt de toestemming waarop de verwerking berust in[36] en er is geen andere rechtsgrond voor.
- De betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking.
- De persoonsgegevens zijn onrechtmatig verwerkt.
- De persoonsgegevens moeten worden gewist om te voldoen aan een in het wettelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
- De persoonsgegevens van kinderen jonger dan 16 jaar zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

Het recht op het corrigeren of wissen (‘recht op vergetelheid’) van persoonsgegevens kan worden beperkt door wettelijke bepalingen.

Maatregelen:

- Tref de nodige maatregelen[37] om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen; controleer op gezette tijden.
- Rectificeer op verzoek van betrokkene onjuiste persoonsgegevens.
- Vervolledig op verzoek van betrokkene onvolledige persoonsgegevens, met inachtneming van de doeleinden van de verzameling en/of verwerking.
- Wis op verzoek van betrokkene persoonsgegevens wanneer er sprake is van een van de in voorgaande tekst genoemde gevallen.
- Bouw in het systeem dan wel proces van dataverzameling en/of verwerking de mogelijkheid tot verwijdering, correctie dan wel actualisatie van persoonsgegevens in. Als dit gebeurt op verzoek van betrokkene, licht deze dan over de status van de afhandeling in.

[35] Bij bezwaar van betrokkene wordt de verwerking gestaakt, tenzij er dwingende gerechtvaardigde gronden voor de verwerking kunnen worden aangevoerd die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.
[36] De betrokkene mag te allen tijde zijn of haar toestemming intrekken. Deze intrekking heeft geen invloed op de legitimiteit van de verwerkingen vóór intrekking, maar vanaf het moment dat iemand zijn of haar toestemming intrekt, mogen de persoonsgegevens niet meer worden verwerkt.
[37] De 'nodige maatregelen' zijn die maatregelen die in redelijkheid van de verwerkingsverantwoordelijke kunnen worden verwacht. Wat in redelijkheid kan worden verwacht hangt af van de soort gegevens, de stand van de techniek en de kosten die met de maatregelen gepaard gaan. Het zorg dragen voor juistheid en nauwkeurigheid van de persoonsgegevens is daarmee een inspanningsverplichting voor de verwerkingsverantwoordelijke en geen resultaatverplichting.

Transparantie

Principe 8: De provincie Drenthe verzamelt en/of verwerkt persoonsgegevens op een zodanige manier dat die transparant is voor betrokkene; de provincie Drenthe heeft hiertoe een informatieplicht[38] richting betrokkenen en betrokkenen hebben de nodige rechten

De wijze waarop de persoonsgegevens worden verzameld en/of verwerkt is voor de betrokkene transparant en maakt het de betrokkene mogelijk zijn/haar rechten uit te oefenen.

Informatieplicht

In de AVG is expliciet opgenomen dat persoonsgegevens verzameld en/of verwerkt moeten worden op een manier die transparant is voor de betrokkene. Voor een natuurlijke persoon moet transparant zijn of en in hoeverre de persoonsgegevens (zullen) worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt. Communicatie met betrokkene dient bovendien plaats te vinden in begrijpelijke, beknopte en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal.

Maatregelen:

- Informeer betrokkene actief over het verzamelen en/of verwerken van zijn/haar persoonsgegevens; behoudens een aantal wettelijke uitzonderingen.
    - Wanneer betrokkenen gegevens aan de provincie Drenthe verstrekken, worden zij op dat moment op de hoogte gesteld van de manier waarop de provincie Drenthe met hun persoonsgegevens om zal gaan. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de provincie Drenthe persoonsgegevens van hem/haar verzamelt en/of verwerkt en weet waarom en voor welk doel dat gebeurt.
    - Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene binnen een redelijke termijn geïnformeerd. Altijd direct de eerste keer dat met hem/haar wordt gecommuniceerd en uiterlijk binnen een maand. Deze plicht is niet van toepassing als betrokkene de informatie al heeft, het onmogelijk of ondoenlijk is om de informatie te verstrekken, de verwerking wettelijk verplicht is of daarmee de doeleinden van de verwerking ernstig in het gedrang komen.

Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van de provincie Drenthe bij het verzamelen en/of verwerken van persoonsgegevens, maar bepaalt ook de rechten van de personen[39] van wie de gegevens worden verzameld en/of verwerkt. Deze rechten bestaan uit:

- Recht op informatie: betrokkenen hebben het recht om aan de provincie Drenthe te vragen of zijn/haar persoonsgegevens worden verwerkt.
- Recht op inzage[40]: betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt; op verzoek van betrokkenen vertelt de provincie Drenthe welke persoonsgegevens van betrokkenen worden verwerkt, met welke specifieke grondslag en op welke manier de provincie Drenthe dat doet.
- Recht op correctie: als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de provincie Drenthe om dit te corrigeren.
- Recht op dataportabiliteit: dit is het recht om gegevens van betrokkene mee te nemen naar een andere organisatie of daar naartoe over te laten dragen.
- Recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- Recht van verzet: betrokkenen hebben het recht aan de provincie Drenthe te vragen om hun persoonsgegevens niet meer te gebruiken.

[38] Referentie informatieverstrekking aan betrokkene: AVG: artikel 13, 14 en 15 en UAVG: Art. 5, 22, 24, 27, 28, 32, 41.
[39] Referentie toegang gegevensverwerking voor betrokkenen: AVG: artikel 11, 12, 15, 86, UAVG: -.
[40] Als de betrokkene bijvoorbeeld om een kopie verzoekt van de eigen persoonsgegevens, moet een kopie van die gegevens worden verstrekt dan wel toegang tot de gegevens in een beveiligde omgeving worden gegeven. Er mogen voor de kopie geen kosten in rekening worden gebracht. Als de betrokkene meerdere kopieën wil ontvangen, mag daarvoor op basis van administratieve kosten wel een redelijke vergoeding worden gevraagd. Bij een inzageverzoek moet de identiteit van de betrokkene worden vastgesteld.

- Recht om vergeten te worden (ook wel: recht op vergetelheid): in gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op een menselijke blik bij besluiten: dit betreft een recht met betrekking tot geautomatiseerde besluitvorming en/of profilering; er worden door de provincie Drenthe geen beslissingen over betrokkene genomen door volledig geautomatiseerde besluitvorming.
- Recht op bezwaar (ook wel: klachtrecht): betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens. De betrokkene kan bij de provincie Drenthe een klacht indienen over het gebruik van de persoonsgegevens van betrokkene; als de betrokkene en de provincie Drenthe er onderling niet uitkomen, kan betrokkene een klacht indienen bij de AP.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan schriftelijk ingediend worden. Als het verzoek niet wordt opgevolgd, kan betrokkene bezwaar (ex artikel 7.1. Algemene wet bestuursrecht (Awb)) maken bij de provincie Drenthe of een klacht indienen bij de AP.

Maatregel:

- Houd het proces rondom rechten van betrokkenen actueel.
- Informeer betrokkenen over hun rechten en draag er zorg voor dat betrokkenen op een laagdrempelige wijze hiervan gebruik kunnen maken.

    - De provincie Drenthe heeft een maand de tijd, vanaf de ontvangst van het verzoek van betrokkene om gebruik te maken van de ‘rechten van betrokkenen’, om te beoordelen of het verzoek gerechtvaardigd is. Binnen een maand zal de provincie Drenthe (de verwerkingsverantwoordelijke) laten weten wat er met het verzoek gaat gebeuren.
    - Afhankelijk van de complexiteit van het verzoek en van het aantal verzoeken van betrokkene kan die termijn indien nodig nog eens met twee maanden worden verlengd. De provincie Drenthe (de verwerkingsverantwoordelijke) stelt de betrokkene binnen een maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.
    - NB. Aan de hand van het verzoek van de betrokkene kan de provincie Drenthe aanvullende informatie opvragen om zeker te zijn van de identiteit van betrokkene.

Principe 9: De provincie Drenthe gaat zorgvuldig om met geautomatiseerde verwerkingen van persoonsgegevens, zoals in het geval van profilering[41], het verzamelen van big data, tracking en tracing en het inzetten van camera’s

Profilering

Technisch is het mogelijk om geautomatiseerde persoonsgegevens met elkaar te verbinden. Wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te voorspellen, is er sprake van profilering. Voorbeelden van persoonlijke aspecten kunnen zijn: financiële situatie, interesses, gedrag of locatie. De provincie Drenthe doet niet aan louter geautomatiseerde besluitvorming of profilering welke herleidbaar is tot het individu. Mensen - en niet systemen - nemen beslissingen op basis van een zorgvuldige afweging van belangen.

Maatregel:

- Doe in principe niet aan louter geautomatiseerde besluitvorming of profilering welke herleidbaar is tot het individu.

[41] Ook wel profiling.

Verzamelen van big data, tracking en tracing

Bij big data worden een grote hoeveelheid en een grote verscheidenheid aan soorten gegevens verzameld. Met computertechnologie is het mogelijk om oneindig veel gegevens te verzamelen en/of te verwerken. Met statistiek is het vervolgens mogelijk om in een verzameling van losse gegevens een betekenis of overeenkomst te vinden. Door gebruik te maken van statistiek kan veel informatie over een persoon verkregen worden.

Bij tracking en tracing worden (online) personen, voertuigen, laadeenheden, zendingen of artikelen gevolgd, waarbij wordt gebruik gemaakt van een combinatie van identificatie-, communicatie- en registratiesystemen.

De provincie Drenthe verzamelt, verwerkt en deelt alleen persoonsgegevens verkregen door big data, tracking en tracing als ze niet herleidbaar zijn tot een persoon en de provincie Drenthe verzamelt deze gegevens alleen voor onderzoek dat door of namens de provincie wordt uitgevoerd.

Maatregelen:

- Verzamel, verwerk en deel alleen persoonsgegevens verkregen door big data, tracking en tracing als ze niet herleidbaar zijn tot een persoon; verzamel deze gegevens alleen voor onderzoek dat door of namens de provincie wordt uitgevoerd.
- Maak voor big data, tracking en tracing uitsluitend gebruik van brongegevens die door daartoe geautoriseerde personen zijn verzameld.
- Zet brongegevens die gebruikt worden voor big data-toepassingen om in een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is. Indien anonimiseren niet mogelijk is: vraag vooraf toestemming aan de FG die de aanvraag zal beoordelen in het kader van de wet en doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats geanonimiseerd worden.
- Laat onderzoek aan de hand van de dataset verkregen uit big data, tracking en tracing niet door dezelfde medewerkers uitvoeren die de gegevens hebben verzameld.

Inzetten van camera's

Voor vergroting van de veiligheid (zoals bescherming van de veiligheid en gezondheid van medewerkers en bezoekers, tegengaan van diefstal en beschadiging van eigendommen) wordt in en rondom het provinciehuis van de provincie Drenthe en overige eigendommen van de provincie Drenthe gebruik gemaakt van cameratoezicht. De camerabeelden worden alleen voor dat doeleinde gebruikt. Om de privacy zo goed mogelijk te waarborgen, dient de inzet van camera's kenbaar te zijn.

Maatregel:

- Wijs bezoekers van de provincie Drenthe in en rondom het provinciehuis of bij overige eigendommen van de provincie op het gebruik van cameratoezicht, bijvoorbeeld in het reglement voor bezoekers en/of via bebording.

Principe 10: De provincie Drenthe past privacy by design en privacy by default toe

Privacybescherming bestaat niet alleen uit toetsing en controle achteraf. Ook aan de voorkant, bij het ontwerpen en inrichten van processen en systemen van gegevensverzameling en/of -verwerking hoort privacybescherming een belangrijk uitgangspunt te zijn. De FG kan hierin desgewenst een adviserende rol hebben.

De provincie Drenthe hanteert privacy by design en privacy bij default. Privacy by design houdt in dat er al bij het ontwerpen van producten en diensten voor wordt gezorgd dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of de bouw van een systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische maatregelen om de persoonsgegevens te beschermen. Dataminimalisatie (zie principe 3) kan hierbij ook helpen; er worden zo min mogelijk persoonsgegevens verzameld en/of verwerkt; alleen datgene wat strikt noodzakelijk is voor het bereiken van het doel. Privacy by design voorkomt reparaties achteraf.

Privacy by default houdt in dat de standaardinstellingen van producten en diensten, zoals invulformulieren, altijd zoveel mogelijk de privacy moeten garanderen. Bijvoorbeeld door bij het gebruik van een app die de provincie Drenthe aanbiedt niet de locatie van gebruikers te laten registreren als dat niet nodig is of door iemand die zich op een nieuwsbrief wil abonneren alleen te vragen naar zijn/haar e-mailadres.

Maatregelen:

- Pas bij (het verlenen van opdrachten tot) het ontwikkelen van producten en diensten van of namens de provincie Drenthe zoveel mogelijk privacy by design en privacy by default (gebruik van standaardinstellingen die zoveel mogelijk de privacy garanderen) toe.

Principe 11: De provincie Drenthe voert bij een risicovolle verzameling en/of verwerking van persoonsgegevens een gegevenbeschermingseffectbeoordeling uit, ook wel data protection impact assessment (DPIA) genoemd

Een gegevensbeschermingseffectbeoordeling ofwel DPIA is een instrument om vooraf aan het verzamelen en/of verwerken van persoonsgegevens de privacyrisico's ervan in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

De provincie Drenthe moet zelf bepalen of er sprake is van een risicovolle verzameling en/of verwerking[42]. Bij de volgende categorieën verzamelingen en/of verwerkingen moet de provincie Drenthe in ieder geval op grond van de AVG een DPIA uitvoeren:

- Systematische, uitgebreide en geautomatiseerde beoordeling van persoonlijke aspecten van betrokkenen (bijvoorbeeld profilering).
- Grootschalige verwerking van bijzondere of strafrechtelijke gegevens.
- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Verder zal de provincie Drenthe een DPIA uitvoeren als er sprake is van hoge risico's voor de rechten en vrijheden van betrokkenen.

Een DPIA bevat ten minste:

- Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de publieke belangen die door de verwerkingsverantwoordelijke worden behartigd.
- Een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden.
- Een beoordeling van de risico's.
- De beoogde maatregelen om de risico's aan te pakken.

Het besluit om een DPIA uit te voeren wordt genomen door de verwerkingsverantwoordelijke, na advies van de FG in overleg met de CIB dan wel privacy officer. Hiertoe is er een pre-DPIA-checklist. Deze bestaat uit een vragenlijst die moet worden ingevuld door degenen die technisch en organisatorisch verantwoordelijk zijn voor de verwerking. De privacy officer kan het initiatief nemen tot, of een rol spelen bij, het houden van een DPIA. In ieder geval wordt de privacy officer op de hoogte gesteld door de FG en de CIB over de voortgang en uitkomsten van een DPIA.

[42] Om privacyrisico's tijdig te signaleren zijn risicomanagement en intern toezicht van belang. Referentie risicomanagement: AVG: artikel 24, 25, 35, 36, 42, UAVG: -. Referentie intern toezicht: AVG: artikel 5, UAVG: -.

Maatregelen:

- Stel een pre-DPIA-checklist op, aan de hand waarvan bepaald kan worden of er wel of niet een DPIA gehouden zou moeten worden, en stel een DPIA-checklist op, aan de hand waarvan een DPIA zelf kan worden gehouden. Houd deze checklisten actueel.
- Voer een DPIA uit voorafgaand aan een risicovolle verzameling en/of verwerking van persoonsgegevens. Vraag de FG[43] en de CIB om advies.
- Raadpleeg als verwerkingsverantwoordelijke voorafgaand aan de verwerking de AP wanneer uit een DPIA blijkt dat de verwerking een hoog risico kan opleveren (als de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken).

Privacyprincipe 12: De provincie Drenthe houdt een verwerkingsregister bij

De provincie Drenthe is verantwoordelijk voor het aanleggen en bijhouden van een register met daarin alle verwerkingen waarvan de provincie Drenthe de verwerkingsverantwoordelijke of verwerker is. Dit heet het verwerkingsregister.

Het verwerkingsregister van de provincie Drenthe is opgebouwd vanuit verwerkingen per domein of Statengriffie en verwerkingen die in de gehele organisatie plaatsvinden. Daarnaast is er een proces om het register actueel te houden. De privacy ambassadeurs hebben daar een grote rol in.

Dit verwerkingsregister[44] bevat in ieder geval[45]:

- Naam en contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, de verwerker en de FG.
- De grondslag voor het verzamelen en/of verwerken van persoonsgegevens.
- Het doel van het verzamelen en/of verwerken van persoonsgegevens.
- Een beschrijving van de categorieën betrokkene(n) waarvan de persoonsgegevens worden verzameld en/of verwerkt.
- Een beschrijving van de categorieën persoonsgegevens die worden verzameld en/of verwerkt.
- De categorieën ontvangers (aan wie de persoonsgegevens worden verstrekt).
- Eventuele overdracht van persoonsgegevens aan derden buiten de Europese Unie.
- De bewaartermijn van de te verzamelen en/of verwerken persoonsgegevens.
- Een algemene beschrijving van de beveiligingsmaatregelen en risicoanalyse.

Maatregel:

- Houd een verwerkingsregister van de provincie Drenthe bij. De FG en/of privacy officer beheert het verwerkingsregister; de privacy ambassadeurs hebben hier ook een grote rol in. De betrokken medewerkers uit domeinen, concernprogramma's of concernprojecten leveren via de privacy ambassadeur tijdig nieuwe of geactualiseerde gegevens voor opname in het verwerkingsregister aan bij de FG en/of privacy officer.
- Actualiseer het verwerkingsregister periodiek. De FG schrijft minimaal één keer per jaar via de privacy ambassadeurs alle domeinen aan met het verzoek het verwerkingsregister te controleren op actualiteit.

Privacyprincipe 13: De provincie Drenthe meldt een datalek[46] bij de AP en informeert de betrokkene, tenzij hiervoor een uitzondering geldt

[43] De verplichting om een DPIA uit te voeren is opgelegd aan de verwerkingsverantwoordelijke, niet aan de FG. Wel kan de FG betrokken worden bij het uitvoeren van de DPIA.
[44] Het verwerkingsregister dient in schriftelijke vorm te zijn, dit mag ook in elektronische vorm. De AVG stelt verder geen andere vormvereisten.
[45] In artikel 30 AVG staat welke onderdelen in het verwerkingsregister moeten staan.
[46] Referentie meldplicht datalekken: AVG: artikel 33 en 34, UAVG: artikel 41 en 42.

Er is sprake van een datalek wanneer persoonsgegevens (mogelijk) in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Enkele voorbeelden van datalekken zijn een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Bij een (potentieel) ernstig[47] datalek geldt een meldplicht. Het gaat in de AVG om twee verschillende meldplichten: er is een meldplicht aan de AP en er is een meldplicht aan de betrokkene, op wiens persoonsgegevens een inbreuk is gemaakt.

De provincie Drenthe meldt een datalek binnen de daarvoor gestelde termijn aan de AP, documenteert de inbreuk, en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.

De provincie Drenthe heeft een protocol meldplicht datalekken voor Gedeputeerde Staten.

Maatregelen:

- Meld als medewerker een (potentieel) ernstig datalek zo snel mogelijk na ontdekking bij de Servicedesk. Daarna start het proces uit het protocol meldplicht datalekken.
- Meld indien nodig als provincie Drenthe een datalek aan de AP zonder onredelijke vertraging en, indien mogelijk, uiterlijk binnen 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen. Als de melding aan de AP niet binnen 72 uur plaatsvindt, vermeld dan de motivering voor de vertraging.
- Als een datalek een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkene: meld het datalek onverwijld[48] aan de betrokkene in duidelijke en eenvoudige taal.
- De verwerkingsverantwoordelijke documenteert een datalek, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. De documentatie bevat de noodzakelijke gegevens van alle datalekken, ook die welke niet gemeld zijn. Datalekken worden aan de directie en specifiek de Algemeen directeur gemeld via het FG-verslag.

[47] Ernstig betekent in dit verband dat er kans is op verlies of onrechtmatige verwerking van persoonsgegevens. De provincie Drenthe maakt zelf een afweging of het datalek ernstig is en dus gemeld moet worden, uiteraard binnen de werking van de AVG.

[48] Wat in een concreet geval als ‘onverwijld’ moet worden aangemerkt, zal afhangen van de omstandigheden van het geval. Daarbij wordt rekening gehouden met het feit dat de betrokkene naar aanleiding van de melding tijdig in staat moet zijn gesteld mogelijke maatregelen te nemen om de nadelige gevolgen van het datalek zo veel mogelijk te beperken of te voorkomen.

5. Tot slot

Met dit document zijn de kaders gegeven voor het privacybeleid van de provincie Drenthe. Daarbij is voor de provincie Drenthe zoveel mogelijk nadere invulling geven aan de Europese en landelijke wetgeving rondom privacy. Uiteindelijk ligt er een verantwoordelijkheid bij alle personen van de provincie Drenthe om bij het verwerken van persoonsgegevens de privacy van betrokkenen te waarborgen.

Bijlagen

Bijlage 1 Privacyprincipes NORA

Deze bijlage hoort bij hoofdstuk 1, Algemeen.

De privacyprincipes uit de Nederlandse Overheid Referentie Architectuur (NORA) zijn:

1. Privacybeleid geeft duidelijkheid en sturing: de organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen.

2. Organieke inbedding: de verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld.

3. Risicomanagement: de verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de privacyrisico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen.

4. Intern toezicht: door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.

5. Toegang gegevensverwerking voor betrokkenen: de verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.

6. Meldplicht datalekken: de verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de AP, documenteert de inbreuk, en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.

7. Doelbinding gegevensverwerking: de verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk omschreven:
   - de doeleinden; en
   - de rechtvaardigingsgronden voor:
     1. de verdere verwerking op grond van de verenigbaarheid met de oorspronkelijke gerechtvaardigde doeleinden;
     2. de geautomatiseerde besluitvorming;
     3. bijzondere persoonsgegevens;
     4. de persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten;
     5. het nationaal identificerend nummer;
     6. de persoonsgegevens ten behoeve van wetenschappelijk of historisch onderzoek met een statistisch oogmerk en archivering in het algemeen belang.

8. Register van verwerkingsactiviteiten: de verwerkingsverantwoordelijke en de verwerker hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.

9. Kwaliteitsmanagement: de verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Indien dit op verzoek van betrokkene gebeurt, wordt deze over de status van de afhandeling geïnformeerd.

10. Beveiliging van de verwerking van persoonsgegevens: de verwerkingsverantwoordelijke en de verwerker treffen technische en organisatorische maatregelen om een verwerking van persoonsgegevens op een passend niveau te beveiligen.

11. Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens: de

verwerkingsverantwoordelijke stelt bij elke verzameling van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor de verwerking.

12. Bewaren van persoonsgegevens: door het hanteren van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.

13. Doorgifte persoonsgegevens: bij doorgifte aan een andere verwerkingsverantwoordelijke zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn er afdoende garanties.

Bijlage 2 Proces, borging en verdeling verantwoordelijkheden

Deze bijlage hoort bij hoofdstuk 3, Proces, borging en verdeling verantwoordelijkheden privacybeleid.

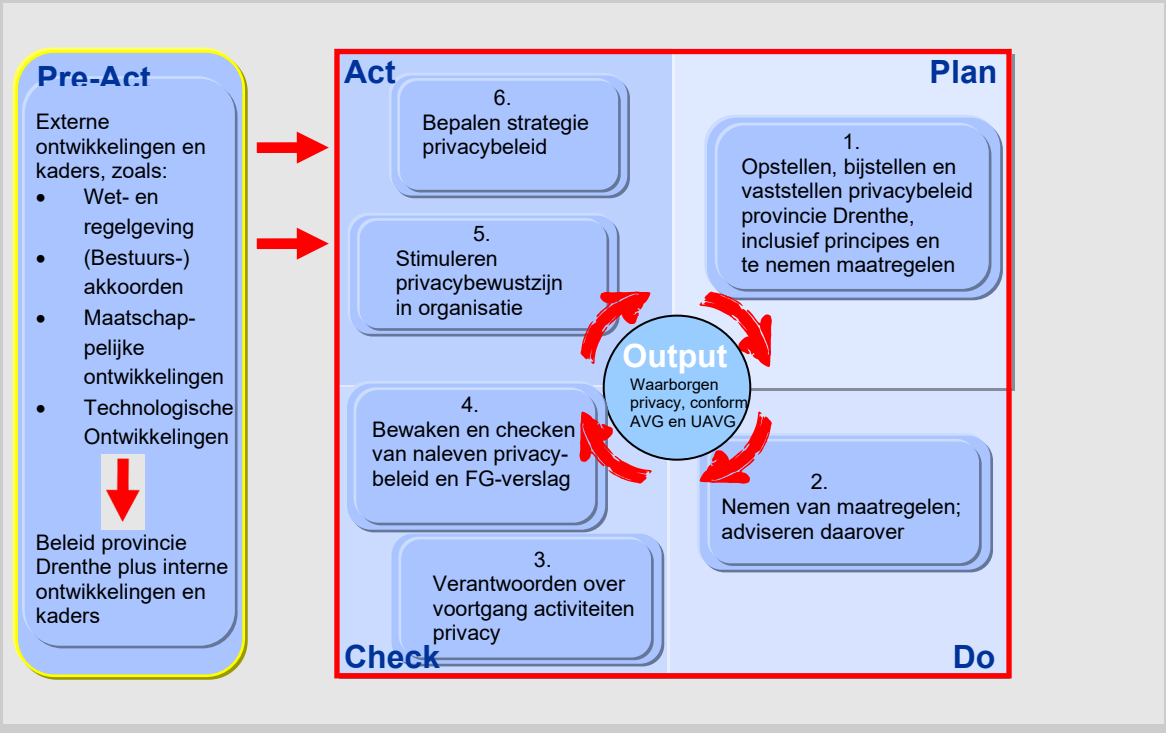
Inleiding

Het proces, de borging en de verdeling van verantwoordelijkheden rondom het privacybeleid van de provincie Drenthe zijn opgehangen aan de kwaliteitscirkel van Deming. Deze kwaliteitscirkel is opgedeeld in een viertal processtappen *Plan-Do-Check-Act*[49]. Deze processtappen vormen een sluitend proces met een begin en een einde gericht op een constante kwaliteitsverbetering. Dit alles leidt tot de gewenste *Output*, ofwel het gewenste resultaat. De fasen staan niet op zichzelf, maar worden beïnvloed door de '*Pre-Act*-fase'. Uit de omgeving komen allerlei invloeden op de provincie Drenthe af. Deze beïnvloeden het beleid en het handelen van de provincie Drenthe. Bij de provincie Drenthe geldt de Demingcirkel als algemeen geaccepteerd proces metamodel.

Proces en borging in beeld

Het proces rondom het privacybeleid bij de provincie Drenthe ziet er als volgt uit.

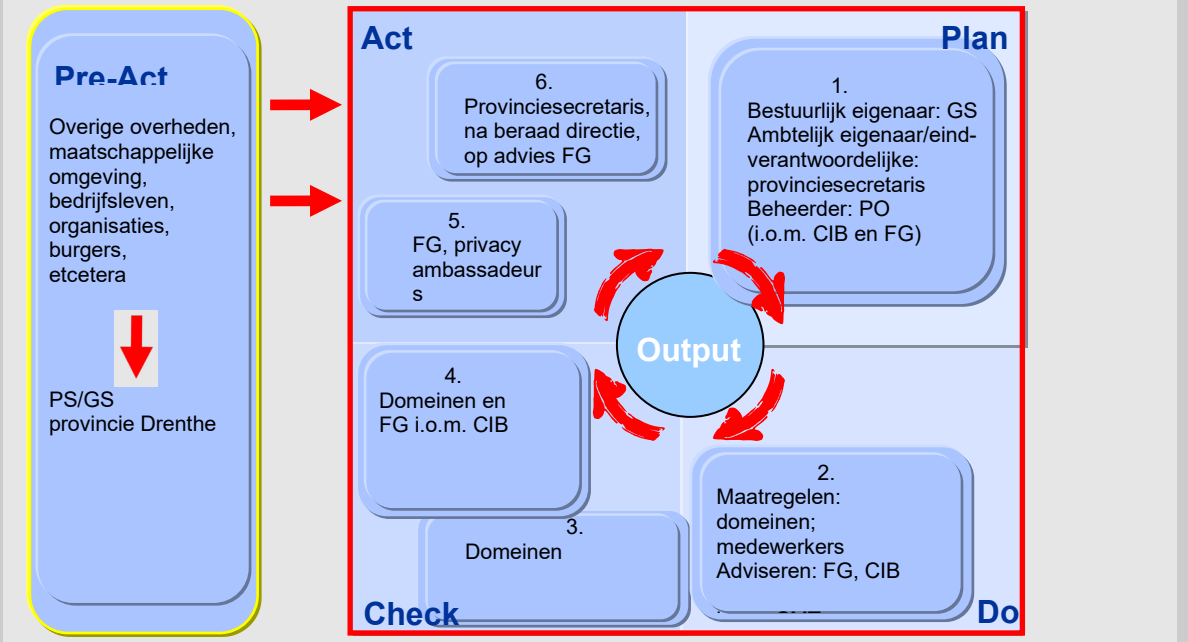
Proces privacybeleid provincie Drenthe



[49] Het is gebruikelijk de nadruk in eerste instantie te leggen op de '*Plan*-fase' in de Demingcirkel. Als die fase goed doorlopen is, kunnen de andere fasen daar ook goed gebruik van maken. Daarbij is overigens aan te tekenen dat de *'Plan*-fase' van een nieuwe ontwikkeling vaak ingegeven wordt door een '*Act*-fase', wellicht voortkomend uit een eerdere, andere ontwikkeling. Ook in relatie tot de *'Pre-Act*-fase'. Ofwel, de exacte startfase in de Deming-cirkel is niet altijd eenduidig te bepalen.

De borging van het privacybeleid bij de provincie Drenthe ziet er als volgt uit.

Borging privacybeleid provincie Drenthe



Daar waar het PS betreft, moeten de rollen worden vertaald naar de Statengriffie, Statengriffier en PS.

Toelichting proces en borging

Pre-Act
0. Bestuurlijke eindverantwoordelijkheid bij portefeuillehouder GS en GS; rol PS

Uit de omgeving komen allerlei invloeden op de provincie Drenthe af. Zo heeft de provincie Drenthe te maken met externe ontwikkelingen zoals nieuwe wet- en regelgeving, (bestuurs)akkoorden, maatschappelijke ontwikkelingen en technologische ontwikkelingen. Deze beïnvloeden het beleid van het provinciaal bestuur en de mogelijkheden van de organisatie van de provincie Drenthe. Er is vooral een relatie met de '*Act*-fase', maar feitelijk heeft de '*Pre-Act*-fase' invloed op de gehele *Plan-Do-*

Check-Act-cyclus.
Een portefeuillehouder in en uiteindelijk het gehele college van GS zijn bestuurlijk gezien eindverantwoordelijk voor het privacybeleid. PS hebben in voorkomende gevallen ook een bestuurlijke, vooral kaderstellende en controlerende, rol wat betreft het privacybeleid. Daarnaast dienen PS als bestuursorgaan te voldoen aan de AVG. Waar mogelijk sluiten PS daarom voor dat deel aan bij het privacybeleid.

Plan
1. Opstellen, bijstellen en vaststellen privacybeleid provincie Drenthe, inclusief principes en te nemen maatregelen: door bestuurlijk eigenaar (GS), ambtelijk eigenaar/eindverantwoordelijke (provinciesecretaris) en beheerder (PO) in overleg met CIB en FG
De PO stelt het Beleidskader privacy op en beheert deze; dit doet de PO waar nodig in overleg met de CIB en FG. Het Beleidskader privacy en bijstellingen daarvan worden voorgelegd aan de directie, waarbij de Algemeen directeur als ambtelijk eigenaar de ambtelijke eindverantwoordelijkheid heeft. Door het bespreken van het privacybeleid door het topmanagement worden het privacybeleid en de

verantwoordelijkheden op strategisch en uitvoeringsniveau geborgd. Het college van GS stelt vervolgens het Beleidskader privacy en eventuele wijzigingen daarin bestuurlijk vast en is daarmee bestuurlijk eigenaar van dit document.

Do

2. Nemen van maatregelen door domeinen en adviseren daarover door FG en/of CIB; persoonlijke verantwoordelijkheid medewerkers

Bescherming van de privacy is een lijnverantwoordelijkheid. De te nemen maatregelen uit dit beleidskader privacy worden dan ook opgepakt en uitgevoerd door alle domeinen. De managers zien hierop toe. Zij dienen ervoor zorg te dragen dat het privacybeleid integraal onderdeel van hun bedrijfsvoering is. Zonodig kunnen de FG en/of CIB daarbij adviseren. Daarnaast is de bescherming van de privacy een persoonlijke verantwoordelijkheid van alle medewerkers van de provincie Drenthe. Zij handelen in hun werkzaamheden naar de regels van het privacybeleid.

Check

3. Verantwoorden over voortgang activiteiten privacy door domeinen

De managers zijn op uitvoeringsniveau verantwoordelijk voor een privacybestendige bedrijfsvoering en gegevenswisseling met derden. Zij zorgen voor uitvoering van en controle op naleving van het privacybeleid binnen hun eigen domein. Uiteraard voor zover passend binnen hun mandaat en dit beleidskader. Zij leggen hierover verantwoording af aan de directie en specifiek de Algemeen directeur en waar nodig ook via de Algemeen directeur aan GS.

4. Bewaken en checken van naleven privacybeleid domeinen; jaarlijks FG-verslag door FG, zonodig in overleg met CIB

Zoals eerder gesteld: bescherming van de privacy is een lijnverantwoordelijkheid. Dit houdt in dat de bewaking van maatregelen in het kader van het privacybeleid bij de domeinen zelf ligt. De managers zien hierop toe.

Daarnaast is er jaarlijks een FG-verslag. De FG is hiervoor verantwoordelijk, zonodig in overleg met de CIB. Dit FG-verslag wordt geagendeerd in het directieoverleg en besproken met de provinciesecretaris. Het FG-verslag gaat daarna ter informatie naar GS en de OR. In het FG-verslag staat de stand van zaken van het privacybeleid in het afgelopen jaar, met waar mogelijk en nodig een vooruitblik naar het komende jaar dan wel de verdere toekomst. Datalekken krijgen specifieke aandacht binnen het jaarverslag. De FG moet namelijk rapporteren over datalekken richting directie en specifiek de provinciesecretaris.

Act

5. Stimuleren privacybewustzijn in organisatie door FG en in domein door privacy ambassadeurs

De FG stimuleert het privacybewustzijn in de organisatie. Te denken valt bijvoorbeeld aan een privacyverklaring, zowel op de website van de provincie Drenthe als op Huisnet. Het privacybewustzijn wordt verder vooral gevormd door het iBewustzijn, gekoppeld aan het informatiebeveiligingsbeleid. In het FG-verslag kan de FG aandacht besteden aan de situatie op dat moment omtrent privacybewustzijn. Binnen het domein levert de privacy ambassadeur een bijdrage aan bewustwording rondom privacy.

6. Bepalen strategie privacybeleid door provinciesecretaris, na beraad directie, op advies FG; rol GS/PS

Zonodig wordt op grond van voorgaande de strategie van de provincie Drenthe rondom het privacybeleid aangepast. Daarmee wordt geanticipeerd en/of gereageerd op externe en interne ontwikkelingen. Uiteraard binnen de kaders van de Europese en landelijke wet- en regelgeving. De ambtelijke eindverantwoordelijkheid voor de strategiebepaling van het privacybeleid ligt bij de provinciesecretaris, na beraadslaging in de directie. De FG adviseert hierbij. Het college van GS, met portefeuillehouder, is bestuurlijk gezien eindverantwoordelijk. In voorkomende gevallen hebben ook PS een bestuurlijke, vooral kaderstellende en controlerende, rol wat betreft het privacybeleid.

Herhaling
De (aangepaste) strategie wordt gebruikt voor de volgende *Plan-Do-Check-Act*-cyclus, beïnvloed door de '*Pre-Act*-fase'. Daarmee herhaalt de *Plan-Do-Check-Act*-cyclus zich voortdurend. En blijft de kwaliteit van het privacybeleid voortdurend in ontwikkeling en onder controle.

Output
Dit alles leidt tot de gewenste output, ofwel het gewenste resultaat. Namelijk een organisatie die de privacy van zowel externe als interne betrokkenen bij de provincie Drenthe waarborgt. Dit alles uiteraard conform de AVG en de UAVG.

Samenvatting verdeling verantwoordelijkheden

Samengevat in een matrix levert dit het volgende beeld op van de verdeling van verantwoordelijkheden naar spelers in de organisatie bij het privacybeleid. Hierbij wordt opgemerkt dat PS wordt bekeken als bestuursorgaan en niet in de kaderstellende rol ten aanzien van GS.

Verdeling verantwoordelijkheden privacybeleid

Verantwoordelijk-heden naar spelers	**PS**	**Griffier**	**GS**	**Provincie-secretaris, al dan niet na beraad directie en op advies FG**	**Domeinen**	**Individuele medewerker**	**Functionaris Gegevens-bescher-ming (FG)/ privacy officer (PO)**	**Coördi-nator Informatie-beveiliging (CIB)**
PRE-ACT								
Beleid provincie Drenthe in het algemeen	X		X					
PLAN								
1. Opstellen, bijstellen en vaststellen privacybeleid provincie Drenthe, inclusief principes en te nemen maatregelen	X	X	X	X			X	(x)
DO								
2. Nemen van maatregelen; adviseren daarover		X			X	X	X	
CHECK								
3. Verantwoorden over voortgang activiteiten privacy					X			
4. Bewaken en checken van naleven privacybeleid; jaarlijks FG-verslag (ter informatie naar GS en OR)					X		X	(x)
ACT								
5. Stimuleren privacybewustzijn in organisatie							X (in domein door privacy ambas-sadeur)	
6. Bepalen strategie privacybeleid; advies *(NB. GS bestuurlijk eindverantwoordelijk; in voorkomende gevallen hebben PS ook een bestuurlijke rol; vooral kaderstellend en controlerend)*	X	X	X	X			X	
OUTPUT								

Bijlage 3 Bronvermelding

Voor het opstellen van dit privacybeleid is gebruik gemaakt van de volgende bronnen.

Wet- en regelgeving

Algemene regels inzake elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid), Tweede Kamer der Staten-Generaal, 34 972, Nr. 2, Vergaderjaar 2017-2018

Algemene verordening gegevensbescherming (AVG), geldig vanaf 25 mei 2018

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

Documenten

Autoriteit Persoonsgegevens, Privacybeleid Autoriteit Persoonsgegevens, 8 oktober 2019, en website AP, april 2020, https://autoriteitpersoonsgegevens.nl/

Autoriteit Persoonsgegevens, Richtlijnen voor functionarissen voor de gegevensbescherming (FG's), vertaling van de Guidelines on Data Protection Officers (DPO's) van de artikel 29-werkgroep van Europese privacytoezichthouders

Centrum Informatiebeveiliging en Privacybescherming (CIP), Privacy Baseline; de AVG ontrafeld voor toepassing in organisaties, 6 mei 2019, https://www.cip-overheid.nl/media/1302/20190506-privacy-baseline-v3_2.pdf

Digitaleoverheid.nl, BurgerServiceCode, april 2020, https://www.digitaleoverheid.nl/document/burgerservicecode/

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Nieuwsbrief De gevolgen van de inwerkingtreding van de Aanpassingswet Algemene verordening gegevensbescherming voor het verkiezingsproces, augustus 2018

Ministerie van Justitie en Veiligheid, Handleiding AVG en UAVG, 22 januari 2018

Nederlandse Overheid Referentie Architectuur (NORA, Privacy Baseline, 25 maart 2020, https://www.noraonline.nl/wiki/De_Privacy_Baseline

Provinciale EnTerprise Referentie Architectuur (PETRA), Interprovinciaal Overleg (IPO), februari 2011, https://docplayer.nl/5279845-Provinciale-enterprise-referentie-architectuur-versie-1-2.html

Provincie Drenthe, Beleidskader basisarchitectuur provincie Drenthe, directie, 6 oktober 2014

Provincie Drenthe, Beleidskader informatiebeveiliging 2017-2020, Veilig, integer en vertrouwd; Hoe is onze informatie beveiligd?, directie, oktober 2017

Provincie Drenthe, Generiek procesmodel, directie, 6 oktober 2014, technisch gewijzigd 1 maart 2015

Provincie Drenthe, Privacyverklaring, website provincie Drenthe, maart 2020

Provincie Drenthe, Quickscan meldplicht datalekken, 25 maart 2019

Provincie Limburg, Privacybeleid provincie Limburg 2018, zoals besloten door Gedeputeerde Staten van Limburg, datum inwerkingtreding: 13 november 2018 (prb-2018-8377)

Rijksoverheid, informatie over AVG en privacy op website, maart 2020, https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens