Gemeente Landsmeer

GEMEENTEBLAD

Officiële uitgave van de gemeente Landsmeer

Nr. 285703

25 november 2019

Privacybeleidskader gemeente Landsmeer 2019

1 Inleiding

In onze digitale samenleving is de afhankelijkheid van (digitale) informatie groot. Veel informatie wordt gedeeld met elkaar, met inwoners en bedrijven en andere instanties. Hierdoor ontstaan ook risico's. De vraag hoe we onze informatievoorziening willen en kunnen beschermen beschrijven we in het Informatiebeveiligingsbeleid en in dit Privacy Beleidskader. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen).

Privacy is in de afgelopen jaren, mede door de digitalisering, brede uitwisseling van informatie en de Algemene Verordening Gegevensbescherming (AVG) veel actueler geworden. Het raakt de persoonlijke levenssfeer van inwoners en ondernemers, en vereist een andere houding en invulling van de overheid. De gemeente Landsmeer is niet alleen verantwoordelijk voor het borgen van de privacy van hun inwoners, maar ook voor het zorgvuldig omgaan met persoonsgegevens in de ketens die zij regisseren en de netwerken waarin ze samenwerken. Vanuit dit oogpunt is het noodzakelijk een visie op privacy en beleid te formuleren, zodat deze gebruikt kan worden als kapstok om de diverse uitvoeringszaken, zoals bijvoorbeeld de regie op eigen gegevens, vorm te geven, en bewoners en ondernemers te laten weten waar zij van gemeentewege op mogen rekenen.
Daarbij is het kunnen voldoen aan de AVG leidend. Per 25 mei 2018 ging de Algemene Verordening Gegevensbescherming officieel in. De Autoriteit Persoonsgegevens is de toezicht houdende instantie en mag bij vaststelling van gebreken een boete opleggen van maximaal € 20.000.000,- of 4% van de wereldwijde omzet.

Dit document bevat de algemene beleidsuitgangspunten over privacy van de gemeente Landsmeer. Deze hebben een sterk normerend karakter en geven gemaakte keuzes weer. Verder beschrijft dit document welke personen in welke rollen betrokken zijn bij privacy en welke maatregelen genomen worden om deze te beschermen. Dit zijn maatregelen op het vlak van huisvesting, ICT, maar houden ook werkafspraken en proceduremaatregelen in. Het beleid geldt dan ook niet alleen voor beheerders van informatie of voor gebouwbeheerders, maar voor iedere medewerker en manager. Iedereen in de organisatie gaat met informatie om.

2 Privacy-gevoeligheid en bescherming van informatie

Privacy gaat over het beschermen van personen in relatie tot informatie die van of over hen bekend is en/of ten aanzien van hen wordt toegepast. Dit wordt ook wel bescherming van persoonsgegevens (of: gegevensbescherming) genoemd en is verankerd in de Grondwet en verder uitgewerkt in de AVG en de Uitvoeringswet AVG.

Binnen de gemeente Landsmeer wordt veel gewerkt met persoonsgegevens, zoals die van inwoners, ondernemers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de inwoners voor het goed uitvoeren van de gemeentelijke wettelijke taken. In onze hedendaagse samenleving kunnen persoonsgegevens voor allerlei doeleinden worden ingezet. Bewoners en ondernemers moeten er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat.
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, transparantie en gebruikerscontrole. De gemeente Landsmeer laat door middel van deze beleidsnotitie zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente.

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. Voorkomen moet worden dat er onnodige of te vergaande inbreuken worden gemaakt. De AVG biedt hiervoor het wettelijk kader en heeft als doel om de privacy van alle Europese inwoners te beschermen. Als algemene regel geldt dat persoonsgegevens op behoorlijke en zorgvuldige wijze moeten worden verwerkt. De AVG bepaalt verder dat persoonsgegevens alleen voor een specifiek doel mogen worden verzameld en gebruikt, en dat deze gegevens niet langer mogen worden bewaard dan noodzakelijk om het doel waarvoor ze zijn verzameld, te realiseren.

3 Beleidsuitgangspunten

De gemeente Landsmeer hanteert de volgende uitgangspunten in haar privacy beleid.

3.1 Doel en scope Privacy Beleidskader

In dit document worden de uitgangspunten op het terrein van privacy weergegeven, wat de verschillende verantwoordelijkheden zijn van betrokken functionarissen en welke maatregelen de gemeente Landsmeer neemt om informatie te beschermen.

Het Privacy Beleidskader (PBK) gemeente Landsmeer is van toepassing op de gehele bedrijfsvoering van de gemeente Landsmeer voor zover hierbij gewerkt wordt met persoonsgegevens.

Het Privacy Beleidskader van de gemeente Landsmeer is nauw verbonden met het Informatiebeveiligingsplan.

Het Privacy Beleidskader wordt 2-jaarlijks geëvalueerd, geactualiseerd, en herijkt.

3.2 Wetgeving/compliancy

De privacy dient te voldoen aan de relevante wet- en regelgeving:

Rechtmatigheid, behoorlijkheid, transparantie. Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding. De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

Dataminimalisatie. De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn. Persoonsgegevens worden niet langer bewaard dan wettelijk nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid. De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het Informatiebeveiligingsbeleid.

Delen met derden. In het geval van samenwerking met externe partijen, waarbij sprake is van verwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet.
De Privacy Officer controleert deze afspraken regelmatig.

Subsidiariteit. Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit. De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en het te dienen doel.

3.3 Persoonsgegevens

Omgang met persoonsgegevens

1. Persoonsgegevens worden alleen verwerkt voor het uitvoeren van bepaalde wettelijke taken en vastgestelde regelingen. Dit ter uitvoering van de AVG voorgeschreven doelbinding en proportionaliteit. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor het doel nodig is. De wet bepaalt verder dat er voor elke verwerking van persoonsgegevens een wettelijke grondslag moet zijn (Artikel 6.1 AVG). Dat betekent dat de verwerking alleen mag plaatsvinden in de volgende gevallen:
    a. de betrokkene heeft toestemming gegeven voor de specifieke verwerking;
    b. voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
    c. om een verplichting na te komen die in de wet staat;
    d. om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

e. voor de goede vervulling van een gemeentelijke taak.

2. De gemeente Landsmeer zorgt ervoor dat de persoonsgegevens juist zijn en zorgt dat ze zo nodig worden geactualiseerd. Alle wettelijke maatregelen worden genomen om de persoonsgegeven die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn onverwijld worden gewist of worden gerectificeerd.
3. Gegevens worden alleen bij een wettelijke grondslag of niet zonder toestemming van de betrokkene gedeeld of verzameld.
4. Om te zorgen voor passende technische en organisatorische beveiligingsmaatregelen zorgt de gemeente dat de Informatiesystemen voldoen aan onder andere de eisen van informatiebeveiliging via de Baseline Informatiebeveiliging Overheid (BIO).
5. Gegevens worden niet verwerkt, tenzij dit nodig is voor het uitvoeren van een wettelijke taak of regeling.
6. Persoonsgegevens worden niet langer bewaard dan strikt nodig is om de doelen te realiseren waarvoor de gegevens worden verzameld.
7. De rechten die betrokkenen hebben staan benoemd in de privacyverklaring op de site van de gemeente Landsmeer.
8. Wanneer een inbreuk in verband met persoonsgegevens (datalek) een risico inhoudt voor de rechten en/of vrijheden van natuurlijke personen worden de betrokkene en de Autoriteit Persoonsgegevens (AP) tijdig geïnformeerd. De melding wordt zonder vertraging aan de Autoriteit Persoonsgegevens gemeld. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, moet de melding onderbouwd worden met een motivering voor de vertraging.
9. Persoonsgegevens worden gedeeld met verschillende derden als dit noodzakelijk is voor het uitvoeren van de taken en om te voldoen aan een eventuele wettelijke verplichting. Met bedrijven die persoonsgegevens verwerken in onze opdracht, sluiten wij een verwerkersovereenkomst en/of privacy-convenant om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van persoonsgegevens. De gemeente Landsmeer blijft verantwoordelijk voor deze verwerkingen zolang dit conform de verwerkersovereenkomst is.
10. De gemeente Landsmeer gebruikt alleen cookies die geen inbreuk maken op de privacy.

4 Taken en verantwoordelijkheden

Het is belangrijk principes te hanteren, uitgangspunten te stellen en keuzes te maken, om privacy gestalte te geven binnen de organisatie.

4.1 Principes, uitgangspunten, verantwoordelijkheden

De wet wijst het college aan als de probleemeigenaar van privacy beleidsvoering (de ‘verwerkingsverantwoordelijke’), maar het college zal op zijn beurt de uitvoering aan anderen opdragen. Op alle niveaus dienen rollen en verantwoordelijkheden duidelijk te zijn, en zijn er afspraken nodig over het afleggen van interne verantwoording. Uiteindelijk is iedereen op zijn/haar eigen manier verantwoordelijk voor geslaagde privacy beleidsvoering. Het college blijft in alle gevallen eindverantwoordelijk.

1. Privacy is ieders verantwoordelijkheid. Er wordt van alle medewerkers (ook ingehuurde) verwacht dat ze zich „fatsoenlijk" gedragen en geheimhouding betrachten.
2. De gemeentesecretaris draagt de algemene eindverantwoordelijkheid voor informatieveiligheid en deelaspecten ervan, zoals privacybescherming en de bedrijfscontinuïteit. De burgemeester draagt de bestuurlijke verantwoordelijkheid voor deze onderwerpen.
3. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Landsmeer hebben een interne eigenaar die de waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid binnen de gemeente Landsmeer voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie. Deze eigenaar is altijd een Proceseigenaar. Bij extern beheerde informatiebronnen en –systemen heeft de eigenaar de rol van opdrachtgever.
4. Er is een Functionaris Gegevensbescherming (FG) aangesteld door het college van B&W. Deze functionaris heeft een controlerende functie en komt op voor de belangen van de betrokkenen waarvan de gemeente persoonsgegevens verwerkt. De Functionaris Gegevensbescherming rapporteert eenmaal per jaar rechtstreeks aan het College (nadat de rapportage is besproken met de betrokkenen).
5. Er is een Chief Information Security Officer (CISO)/Privacy Officer (PO) per 1 juli 2019 door het college van B&W aangesteld. Deze functionaris ziet er op toe dat het privacy beleid wordt opgesteld en geïmplementeerd.
6. Bij privacy incident hanteert de proceseigenaar de procedure Melden datalekken.
7. Bij risicovolle procesvoering, zoals bij het Sociaal Domein en Burgerzaken, worden via protocollen op maat gesneden processen toegepast en laat de proceseigenaar zich periodiek auditen op grond van dit Privacy Beleidskader en het betreffende procesplan.

8. Het college evalueert tweejaarlijks de doeltreffendheid en de doelmatigheid van dit Privacy Beleidskader.
9. Het college informeert de raad over privacy beleidsvoering in de P&C cyclus en de uitvoering ervan jaarlijks in de jaarrekening.

4.2 Toezicht
De FG is de toezichthouder van de gemeente Landsmeer op de naleving van privacywetgeving conform artikel 37-39 AVG.

Het college informeert interne en externe doelgroepen over de FG en communiceert de contactgegevens aan de Autoriteit Persoonsgegevens.

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

De FG:
- Informeert en adviseert het college, proceseigenaren en het Privacy- en InformatiebeveiligingsTeam (PIT) over de werking van het privacy beleid van de gemeente Landsmeer en nakoming van achterliggende wettelijke verplichtingen (heeft de lead in interpretatie van privacywetgeving)[1].
- Houdt toezicht op de nakoming van het privacy beleid en achterliggende wettelijke verplichtingen[1].
- Controleert de naleving van afspraken door gemeente Landsmeer en ketenpartners, eventueel ook in samenwerking met auditors[1].
- Is het contactpunt voor landelijke privacy toezichthouders – met name de Autoriteit
- Persoonsgegevens*.
- Helpt privacy klachten tot een goed einde te brengen (ombudsfunctie)[2].
- Adviseert bij privacy incidenten over ernst en omvang[2].
- Helpt het privacy beleid en daarmee tevens de visie uit te dragen bij interne en externe doelgroepen.
- Oefent de taken in volledige onafhankelijkheid uit.

De FG krijgt de nodige ruimte voor professionele uitvoering van taken.
- Het college en proceseigenaren zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij de verwerking van persoonsgegevens.
- De FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen gemeente Landsmeer waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- Het college en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De FG werkt onafhankelijk en mag dus niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, gestraft of ontslagen bij normale omstandigheden.

De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van privacywetgeving door de gemeente, onverminderd de opvattingen van landelijke toezichthouders.

De FG doet jaarlijks verslag van de werkzaamheden aan het college van B&W. De raad wordt via de planning & control-cyclus geïnformeerd.

5 Maatregelen

5.1 Specifieke maatregelen
1. Om te waarborgen dat persoonsgegevens alleen voor welomschreven gerechtvaardigde (dat wil zeggen op grond van de juiste rechtsgrond) en uitdrukkelijke doeleinden worden verzameld, worden alle verwerkingen bij de gemeente Landsmeer vastgelegd in een register van verwerkingsactiviteiten. Dit register wordt periodiek gecontroleerd en waar nodig aangevuld. Om te waarborgen dat verwerkingen toereikend, ter zake dienend en beperkt zijn tot “minimale gegevensverwerking” (tot wat noodzakelijk is voor de doeleinden waarvoor gegevens worden verwerkt) worden alle in het register van verwerkingsactiviteiten opgenomen verwerkingen juridisch getoetst aan de beginselen genoemd in de AVG.

1) is wettelijk opgenomen.
2) volgt uit wettelijke beschrijvingen.

2. Om te waarborgen dat bij verwerkingen van persoonsgegevens passende, organisatorische en technische beveiligingsmaatregelen worden getroffen moet de organisatie zich conformeren aan de normen zoals deze zijn gesteld in onder meer de BIO. Middels het uitvoeren van de Eenduidige Normering Single Information Audit (ENSIA) controleert de organisatie jaarlijks of zij voldoet aan de normen uit de BIO.
3. Om te waarborgen dat betrokkenen de mogelijkheid hebben hun rechten ten aanzien van persoonsgegevens uit te kunnen oefenen, worden er protocollen en procedures inzake deze rechten vastgesteld. Daarnaast worden betrokkenen tijdig en juist geïnformeerd over hun rechten. Hiertoe wordt er te allen tijde een juiste, makkelijk bereikbare en leesbare privacyverklaring op de website van de gemeente Landsmeer geplaatst.
4. Om te waarborgen dat verwerkingen van persoonsgegevens voldoen aan de hierboven genoemde punten, dient er, bij het opzetten van elke bestaande, nieuwe of aangepaste verwerking een pre-Data-Privacy Impact Assessment en Data-Privacy Impact Assessment uitgevoerd worden. Daartoe dienen de nodige protocollen en procedures gemaakt en geïmplementeerd worden.
5. Om te waarborgen dat de medewerkers van de gemeente Landsmeer op een correcte wijze met persoonsgegevens omgaan en daarop aanspreekbaar zijn worden zij regelmatig getraind en wordt in de organisatie op verschillende wijzen, zoals via de inzet van communicatie, aandacht gevraagd en gevestigd.
   Ingehuurde medewerkers dienen bij aanvang van de werkzaamheden een Verklaring integriteit en geheimhouding te ondertekenen.
6. Om te waarborgen dat derde partijen (verwerkers en/of zelfstandige) op een correcte manier met persoonsgegevens omgaan, worden persoonsgegevens pas doorgegeven als formeel afdoende garanties zijn vastgelegd en aangetoond kan worden dat deze derde partijen aan de eisen uit de AVG wordt voldaan. Dit wordt vastgelegd en moet worden aangetoond door zogenoemde verwerkersovereenkomsten.

5.2 Proces
Gemeente Landsmeer werkt toe naar een gemanaged niveau van kwaliteit in bescherming van de privacygegevens.

Volwassenheid privacybeleidsvoering			
	Niveau		**Omschrijving**
●	Optimaliserend	5	Organisatiebreed privacybeleid gekenmerkt door vanzelfsprekendheid en natuurlijke samenwerking. Optimalisering van beheersmaatregelen is een continu proces en gebeurt op basis van meetbaarheid, rekenschap, permanente dialoog en anticipatie.
●	Gemanaged	4	Organisatiebreed privacybeleid gekenmerkt door hoge awareness en bijsturing van beheersmaatregelen op basis van meetbaarheid, rekenschap en periodieke evaluaties.
●	Afgebakend	3	Privacybeleid beperkt zich tot processen die als meest risicovol in het oog springen. Deze worden in kaart gebracht en voorzien van passende beheersmaatregelen maar missen borging en zijn daarmee niet bestendig genoeg.
●	Herhaalbaar	2	De organisatie beschikt over beheersmaatregelen die breder toepasbaar zijn. Ze zijn echter vaak nog te operationeel, missen consistentie en zijn niet noodzakelijk toereikend.
●	Ad hoc	1	Maatregelen staan op zichzelf en ontbreken bij andere aandachtsgebieden. Ze zijn vaak te operationeel, missen consistentie en zijn niet noodzakelijk toereikend.
●	Nalatig	0	Privacy leeft niet. De wet wordt genegeerd. Privacywaarborgen zijn afwezig.

Privacy is nooit 'klaar'. Zolang gemeente Landsmeer persoonsgerelateerde informatie verwerkt, blijven privacy-waarborgen nodig. Oplossingen dienen geëvalueerd en aangepast te worden om te blijven sporen met maatschappelijke, wettelijke, technische en organisatorische ontwikkelingen. Privacy management vergt een permanent programma. In het PBK Gemeente Landsmeer worden de uitgangspunten van dat permanente privacy programma benoemd.

Stap 1: Uitvoeren bewustwording en transparantie
Opvoeren van de bewustwording en transparantie door het uitvoeren van Quick Wins zoals: geven van presentaties, maken van folders, verspreiden posters, aandacht op intranet enz.

Stap 2: Vaststelling PBK Gemeente Landsmeer
De motor voor het privacy programma is het overkoepelend privacy beleid zoals het college heeft vastgesteld en ten uitvoer legt in de vorm van het PBK Gemeente Landsmeer.

Stap 3: Voorzien in onafhankelijk toezicht
Gegeven het risicoprofiel (bijlage 3) dat van toepassing is bij de meest gevoelige processen die zich binnen de gemeentelijke organisatie afspelen, is onafhankelijk toezicht in de persoon van een FG een must en onder de AVG verplicht. Tijdsbeslag en positionering zal nu moeten volstaan met 8 uur per maand. Evaluatie na een jaar uitvoering zal moeten uitwijzen of deze uren voldoende zijn voor de FG.

Stap 4: Uitvoering gemeentelijk privacy beleid
Het PBK Gemeente Landsmeer zet aan tot verdere vormgeving van het gemeentelijke privacy beleid. Namens het college zal de portefeuillehouder hier zorg voor dragen, in samenwerking met alle 1e, 2e en 3e lijn betrokkenen (zie de RASCI-tabel in bijlage 2).

De CISO/PO is verantwoordelijk voor het vormgeven en bewaken van het privacy beleid binnen de gemeente, het in kaart brengen van de risico's (door bijvoorbeeld een DPIA uit te voeren), het maken van een implementatieplan, en tot slot heeft de CISO/PO een adviserende rol richting de teams.

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support door het PIT en de FG.

Bijlage 5 bevat een beschrijving van proces en verantwoordelijkheden van proceseigenaren. Proceseigenaren voorzien in passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen ('privacy waarborgen') en documenteren die maatregelen in procesplannen.

Bijlage 1. Definities

AVG (Algemene Verordening Gegevensbescherming) – Europese wet op de verwerking van persoonsgegevens, die rechtstreeks geldt in alle lidstaten.

Bedrijfsproces – gemeentelijke bedrijfsvoering waarbij persoonsgegevens worden verwerkt.

FG (Functionaris voor Gegevensbescherming) – wettelijk toezichthouder voor de naleving van privacywetgeving en bedrijfsvoorschriften.

(Gegevens)verwerking – zowel geheel of gedeeltelijk geautomatiseerde operationele informatieverwerking (bijvoorbeeld archiveren, analyseren, doorgeven, raadplegen) als ieder geheel daarvan (bijvoorbeeld de salarisadministratie, gemeentebelastingen of thuiszorg).

Persoonsgegevens – gegevens over personen en waarvan de gegevensverwerking door herleidbaarheid gevolgen heeft in de persoonlijke levenssfeer (privacy impact heeft).

DPIA (Data privacy impact assessment) – een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico's vanuit privacyoptiek, resulterend in een lijst van passende beheersmaatregelen (waarborgen).

DPIA-score – getalsmatige classificatie van noodzaak of risico van gegevensverwerking, als uitkomst van een DPIA.

PIT – het privacy- en informatiebeveiligingsteam dat de directie en proceseigenaren ondersteunt.

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

Privacy beleidskader – het bestuurlijk privacy beleid van een organisatie, die de kapstok vormt voor.

Privacy audit – controles op de naleving van privacy beleid en privacywetgeving.

Privacy beleid – het Privacy Beleidskader en alle nadere uitwerkingen hiervan.

Privacy beleidsvoering – sturing op privacy door het management ('governance').

Privacy incidenten – gebeurtenissen waartegen het privacy beleid en de privacywetgeving bescherming beoogt te bieden.

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

Procesdoel – een bedrijfsdoelstelling die noodzaakt tot verwerking van persoonsgegevens.

Proceseigenaren – teammanagers, die integraal verantwoordelijk zijn voor (overstijgende) proces- en ketenprocessen en uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen en veiligheid.

Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een DPIA).

Programmanager Privacy – degene die namens de portefeuillehouder privacy uitvoering geeft aan het privacy beleid.

Servicepunt – het contactpunt voor personen waar zij terecht kunnen voor het uitoefenen van hun privacy rechten.

Uitvoeringsorganisatie – een organisatie waaraan een of meerdere bedrijfsprocessen zijn uitbesteed.

Verwerkersovereenkomst – een overeenkomst tussen de gemeente en een derde partij, die een deel van de administratie voor de gemeente doet, waarin overeengekomen wordt dat deze derde partij zorgvuldig met de persoonsgegevens omgaat.

Bijlage 2. Rollen en verantwoordelijkheden

Een 'RASCI-tabel' met daaraan toegevoegd de indeling naar 1e, 2e, 3e, 4e- lijns-risicomanagement helpt om rollen en verantwoordelijk inzichtelijk te maken:

RASCI	Vertaald naar privacy	Concreet
R Responsible	Feitelijk verantwoordelijk	**1e lijn** • Afdelingshoofden • Medewerkers • Ketenpartners bij inkoop/outsourcing (zoals gemeenschappelijke regelingen)
A Accountable	Eindverantwoordelijk	**1e lijn** • College van B&W (portefeuillehouder) • Eventueel verschillende colleges gezamenlijk bij gecombineerd opdrachtgeverschap ('joint controllers')
S Supportive	Ondersteunend	**2e lijn** • Informatieadviseurs • Beveiligingsbeheerders • Juristen • Kwaliteitsmanagers • PrivacyOfficer
C Consulted (hier: Controlerend)	Toezicht	**3e lijn/ 4e lijn (intern/ extern)** • Functionaris voor Gegevensbescherming • Auditor • Accountant • Controller
I Informed	Geïnformeerd	**5e lijn** • Inwoners/ondernemers • Medewerkers • Gemeenteraad • Autoriteit Persoonsgegevens

Gelaagde aanpak en documentatie
Privacy beleid kent een gelaagdheid die het beste ook in de beleidsdocumentatie tot uitdrukking wordt gebracht en waarbij documenten op een logische manier met elkaar samenhangen.

- **Bestuurlijk privacy beleid**: een beleidsnota waarin het college de algemene aspecten van de privacy beleidsvoering regelt (overkoepelend privacy beleid): missie, wijze van sturing, middelen, toezicht en handhaving.
- **Procesplannen**: het bovenliggende beleidskader wordt nader uitgewerkt voor de afzonderlijke werkprocessen, door op basis van risicoanalyses (indien nodig in de vorm van DPIA's) concrete organisatorische en technische oplossingen te benoemen waardoor de bescherming van persoonsgegevens en rechten van personen op een passende manier gewaarborgd wordt.
- **Bewijs van uitvoering**: documentatie van planning, uitvoeringsacties, evaluaties en controles.

Rekenschap / accountability
Door bestuurlijk privacy beleid, eventueel voor bepaalde thema's nader uitgewerkt, komen de beleidsmatige privacy principes 'op groen' te staan. Door procesplannen en bewijs van uitvoering komen de privacy principes m.b.t. de uitvoering 'op groen' te staan. Op deze manier is er een sluitend en aantoonbaar stelsel van privacy waarborgen (bewijs van adequaat privacy management).

Functionaris voor de Gegevensbescherming
Voor de controle op de naleving van beleid en wetgeving beveelt de AVG aan dat organisaties zich laten bijstaan door een 'Functionaris voor de Gegevensbescherming'
(FG – vaak ook aangeduid als data protection officer of DPO). Deze rol wordt beschreven in artikelen 35-37 AVG. Een FG is voor gemeenten bovendien verplicht.

De FG is wettelijk toezichthouder náást de Autoriteit Persoonsgegevens.[3] Tevens fungeert de FG als privacy ombudsman voor personen die door gebrekkige gegevensverwerking in de knel zijn gekomen. De contactgegevens van de FG dienen namens het college van B&W te worden gecommuniceerd aan de Autoriteit Persoonsgegevens.

3) Niet te verwarren met toezichthouder *voor* de AP

De AP beoordeelt niet de geschiktheid van de FG. Bij de aanwijzing van een FG moet Gemeente Landsmeer zich er zelf van vergewissen van dat de persoon voldoet aan de wettelijke eisen. Grofweg is iemand geschikt als FG wanneer hij/zij over de volgende kwaliteiten beschikt:[4]

- expert op het gebied van privacywetgeving;
- praktijkdeskundig (kennis van organisaties, processen, ICT en informatiebeveiliging);
- onafhankelijk en betrouwbaar;
- beroepservaring die past bij zijn verantwoordelijkheden;
- vaardigheden op het gebied van communicatie, PR en regulatory affairs.

Een FG moet dus multidisciplinair zijn, en kunnen fungeren als sparringpartner voor zowel het college als voor onderdelen van de gemeentelijke organisatie, hij moet daarom stevig in de schoenen staan. Let er bij de selectie ook op dat de FG in staat is pragmatisch te denken. Tegelijkertijd moet de FG ook in staat zijn om duidelijk maar met tact te signaleren waarin de gemeente buiten de kaders van de privacywetgeving opereert (eerder grensrechter/coach dan politieagent).

Vanwege zijn/haar wettelijke status is het oordeel van de FG juridisch zwaarwegend. De FG is de aangewezen persoon om de knopen door te hakken in juridische discussies. Voor zover de FG en de AP afwijkende standpunten innemen, is het in principe aan de rechter om een beslissende uitspraak doen.

4) Vgl. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_fg.pdf

Bijlage 3. Risicoklassering persoonsgegevens

Niet alle verwerking van persoonsgegevens is risicovol. Er wordt onderscheid gemaakt in twee risiconiveaus, laag en hoog.

Laag Risico
Openbare persoonsgegevens vallen in ieder geval onder deze categorie. Hiervan is algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internet sites etc. Daarnaast bestaat een categorie persoonsgegevens waarvan de risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zodanig laag zijn dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens gaat dan het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie. Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel - gast, vereniging - lid, organisatie - deelnemer. Opgemerkt wordt dat het lidmaatschap van een instelling op zich al informatie kan bevatten betreffende een persoon. Indien dit gegevens zijn die vallen onder de categorie bijzondere gegevens, bijvoorbeeld over politieke voorkeur, seksuele leven, kerkelijk genootschappen etc., dan moet het risico als hoog worden opgevat.

Hoog risico
De stand van de techniek, ontwikkelingen in de maatschappij en andere factoren kunnen van invloed zijn op de gevolgen die verlies of onrechtmatige verwerking van persoonsgegevens met zich mee kunnen brengen voor de betrokkenen. Onderstaande opsomming van categorieën van persoonsgegevens waar deze gevolgen ernstig kunnen zijn, is daarom niet uitputtend:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG. Het gaat daarbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele voorkeur, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;
- Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden;
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen;
- Gegevens die betrekking hebben op mensen uit kwetsbare groepen. Het gaat hier bijvoorbeeld om mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijf huis verblijven, om klokkenluiders of om informanten van de politie of het Openbaar Ministerie;
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven;
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (BSN).

Behalve de aard van de verwerkte gegevens, kan ook de verwerking zelf risico's met zich meebrengen voor de betrokkenen. Factoren die een rol spelen zijn onder meer:

- Hoeveelheid verwerkte persoonsgegevens per persoon. Naarmate er per persoon meer persoonsgegevens worden verwerkt, kan verlies of onrechtmatige verwerking leiden tot een grotere inbreuk op de persoonlijke levenssfeer;
- Doel of doelen waarvoor de persoonsgegevens worden verwerkt. Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter.

Bijlage 4. De AVG en andere wetten

In deze paragraaf wordt de relatie tussen de AVG en andere wetten kort behandeld. Over het algemeen geldt dat de AVG geldt als algemene wet, waarvan de bepalingen niet van toepassing kunnen zijn wanneer er bijzondere wetgeving van toepassing is. Dat neemt niet weg dat ook indien de bijzondere wet leidend is, de AVG aanvullend van toepassing kan zijn. Zo zullen bijvoorbeeld ook dan de algemene basisprincipes van artikel 5 lid 1 AVG van toepassing zijn. Zo zal het college in alle gevallen slechts persoonsgegevens mogen verwerken voor welbepaalde en uitdrukkelijk omschreven doelen en moeten zorgen dat de gegevens juist zijn.

AVG versus BRP
De AVG is niet van toepassing op de Wet Basisregistratie personen (Wet BRP). De wet BRP heeft een eigen, gesloten, privacy regime. Dat wil zeggen dat de wet limitatief bepaalt aan welke overheden de in de registratie opgenomen gegevens mogen worden verstrekt, voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taak. Verder is krachtens deze wet bepaald aan welke derden deze informatie kan worden verstrekt.

AVG versus Wob
Onder de Wet bescherming persoonsgegevens (Wbp) gold dat de Wet openbaarheid van bestuur (Wob) een bijzondere wet is ten opzichte van de (algemene) Wbp. In zo'n geval gaat de bijzondere wet voor. Aannemelijk is dat de jurisprudentie waarin dit is uitgemaakt onder de AVG zijn geldigheid zal behouden. Indien de Wob van toepassing is, is de AVG dat niet. Dat betekent niet dat de bescherming van persoonsgegevens geen rol speelt bij de uitvoering van de Wob. Binnen de Wob zijn er namelijk twee weigeringsgronden waarbij de persoonlijke levenssfeer een rol speelt.

AVG versus Archiefwet
De AVG kent een aantal specifieke uitzonderingen voor verwerking van persoonsgegevens met het oog op archivering in het algemeen belang. Een aantal uitzonderingen werkt rechtstreeks, zie artikel 89 AVG: Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Bij verwerkingen onder de noemer van onderzoek en archivering dienen de rechten en vrijheden van betrokkenen (oftewel: de privacy) te worden gewaarborgd. Het accent hierbij ligt bij het beginsel van gegevensminimalisering (dataminimalisatie). Dit betekent dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk voor het doel. Zodra het mogelijk is om het archiveringsdoel te halen met ontkoppelde gegevens (ofwel geanonimiseerde gegevens, niet langer herleidbaar tot een natuurlijke persoon en dus niet langer persoonsgegevens) moet deze ontkoppeling worden uitgevoerd. Als dat nog niet mogelijk is kan wellicht een (tijdelijke) oplossing worden gevonden in de vorm van pseudonimisering waarbij koppeling nog wel mogelijk is, maar de daarvoor benodigde informatie niet direct beschikbaar is.

Artikel 89 lid 3 AVG bevat een specifieke bepaling op grond waarvan de lidstaten kunnen afwijken van enkele voorschriften van de AVG. Het gaat hier om de mogelijkheid om af te wijken van de artikelen 15 (het recht op inzage), 16 (het recht op rectificatie), 18 (het recht op beperking van de verwerking), 19 (kennisgevingsplicht), 20 (het recht op overdraagbaarheid van de gegevens) en 21 (het recht op bezwaar). De gemeente dient kritisch te blijven kijken binnen de eigen werkprocessen voorafgaand aan archivering en deze te toetsen op dataminimalisatie, zodat kan worden aangetoond dat ook voor wat betreft het gemeentelijke archief voldaan is aan de vereiste passende waarborgen die voortkomen uit de AVG en de UAVG.

AVG versus Wet politiegegevens
Voor de politie geldt als het gaat om de omgang met persoonsgegevens de Wet politiegegevens, uitgewerkt in het Besluit Politiegegevens. Deze wet bevat een eigen privacy regime. De AVG is hierop niet van toepassing.

AVG versus identiteitsbewijs
In veel gevallen is een inwoner verplicht zich te identificeren met een geldig identiteitsbewijs (de Wet Identificatieplicht en andere wetten). Dat betekent niet per se dat dan ook een kopie daarvan bewaard mag worden. Een identiteitsbewijs bevat een burger servicenummer en kan bijzondere persoonsgegevens bevatten. Verwerken is dus verboden tenzij. Een voorbeeld: de Wet op de loonbelasting verplicht de gemeente als werkgever een kopie van een identiteitsbewijs van een ambtenaar/werknemer te bewaren tot 5 jaar na het jaar waarin deze persoon uit dienst is getreden. Dit is een voorbeeld van een wettelijke grondslag voor het bewaren van een kopie van een identiteitsbewijs.

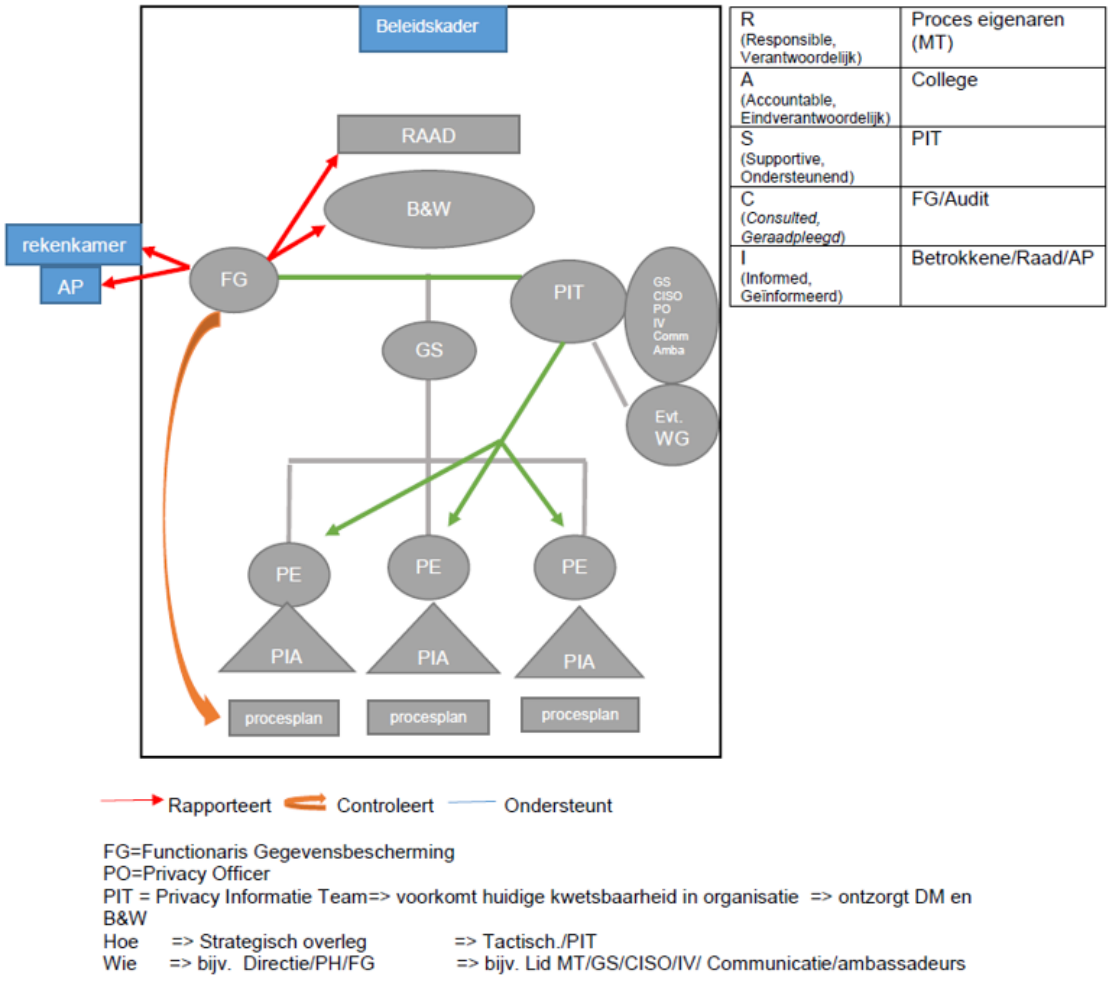
AVG versus Wet inzake de geneeskundige behandelingsovereenkomst en de Jeugdwet
De Wet inzake de geneeskundige behandelingsovereenkomst (WGBO) en de Jeugdwet bevatten regels over de omgang met persoonsgegevens voor medisch hulpverleners en voor jeugdzorgwerkers. De WGBO en de Jeugdwet kunnen in zoverre worden opgevat als privacywetten, ook al regelen ze veel meer onderwerpen dan de omgang met persoonsgegevens. De specifieke bepalingen in deze bijzondere wetten gaan voor de algemene bepalingen van de AVG.

Bijlage 5. Gedragsnormen voor proceseigenaren

Het college verwacht van proceseigenaren rechtmatige en zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support door het PIT en de FG. Het college voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen de gemeente een privacy bestendige cultuur te realiseren.

Proceseigenaren voorzien in passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen ('privacy waarborgen') en documenteren die maatregelen in procesplannen. De portefeuillehouder privacy houdt een 'artikel 30-register' (Verwerkingsregister zie 4.1) bij van de gegevensverwerkingen die onder de eindverantwoordelijkheid van het college valt. Proceseigenaren helpen om het register volledig en actueel te laten zijn door middel van 'artikel 30-formulieren'.

Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacy beleidsvoering en faciliteren de uitoefening van rechten door personen over wie de gemeenten gegevens verwerken. Proceseigenaren verlenen hieraan hun medewerking.
Het college en proceseigenaren dragen het belang uit van privacy beleidsvoering en geven zelf het goede voorbeeld. Zij maken privacy bespreekbaar. Bij dilemma's gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt.



FG=Functionaris Gegevensbescherming
PO=Privacy Officer
PIT = Privacy Informatie Team=> voorkomt huidige kwetsbaarheid in organisatie => ontzorgt DM en B&W
Hoe => Strategisch overleg => Tactisch./PIT
Wie => bijv. Directie/PH/FG => bijv. Lid MT/GS/CISO/IV/ Communicatie/ambassadeurs

Procesplan aanpak
Aan procesplannen liggen privacy impact assessments (PIA's) ten grondslag. PIA's zijn instrumenteel voor het kunnen bepalen van passende beheersmaatregelen. Te vergelijken met een risicoanalyse. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de PIA, zoals verwoord in het PIA-rapport.
Voor nieuwe verwerkingen met persoonsgegevens en/of andere ontwikkelingen waarbij persoonsgegevens zijn betrokken, moet altijd een PIA worden uitgevoerd.

Ook voor bestaande verwerkingen moet een PIA worden uitgevoerd. Eerst moet worden vastgesteld of een PIA uitgevoerd moet worden over een bestaande verwerking. Dit gebeurt met behulp van een baselinetoets. Deze tool wordt ook gebruikt voor de uitvoer van de Baseline Informatiebeveiliging Overheid (BIO).
Tevens moet rekening gehouden worden met de criteria genoemd in de AVG zijn genoemd en die de Autoriteit Persoonsgegevens heeft beschreven. Als hiervan sprake is moet er ook een PIA worden uitgevoerd.

Een PIA kan op twee manieren worden uitgevoerd.
1. Door de impact, kwetsbaarheid en maatregelen van de verwerking met de proceseigenaar, belanghebbenden en het PIT te bespreken. Van de verwerking wordt een systematische beschrijving gemaakt. De noodzaak en evenredigheid wordt beschreven en wat de risico's zijn als de gegevens niet correct worden verwerkt. Tenslotte wordt beschreven welke maatregelen genomen moet worden om de risico's weg te nemen.
2. Het beantwoorden van vragen over de verwerking op:
    - Juridisch-;
    - Geautomatiseerd- en;
    - organisatorisch niveau.

De bevindingen en/of tekortkomingen worden in een rapport opgenomen en de domeinmanager aangeboden. Hij/zij dient hierop te acteren. De FG controleert of de genomen acties voldoen. Tevens moet worden afgesproken wanneer de PIA opnieuw moet worden uitgevoerd. De PIA wordt in het DPMS opgenomen. PIA-rapporten worden opgesteld conform artikel 35 lid 7 AVG.

Proceseigenaren documenteren met behulp van hun procesplannen hoe zij op een praktische manier in passende organisatorische en technische privacybeschermende maatregelen voorzien – met name om de volgende fouten te voorkomen:
1. Illegale/onrechtmatige gegevensverwerking: gebruik, opslag of uitwisseling van informatie is bij wet verboden (middels een rechtstreeks verbod of een beperking van het toegestane gebruik).
2. Disproportionele gegevensverwerking: gebruik, opslag of uitwisseling van informatie is (a) ontoereikend of juist overmatig of (b) het organisatiebelang bij de gegevensverwerking is onevenredig klein terwijl de impact op personen onevenredig nadelig kan zijn.
3. Irrelevante gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie dient geen bedrijfsdoel, doet niet ter zake of is verouderd.
4. Onnauwkeurige gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie is geen juiste weergave van de werkelijkheid.
5. Onveilige gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie dreigt te gemakkelijk toegankelijk te zijn voor onbevoegden, gemanipuleerd te worden of niet beschikbaar te zijn.
6. Niet-inachtneming van bijzondere wettelijke voorschriften: bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.
7. Onbewaakte gegevensverwerking: de proceseigenaar verzuimt om te controleren of de privacy waarborgende maatregelen daadwerkelijk zijn geëffectueerd of te evalueren in hoeverre zijn procesplan bijstelling behoeft.

Volgende punten komen ook in het procesplan:
- Een lijst van kenmerkende beheersmaatregelen voor sturingsdoeleinden en controle (audit). Proceseigenaren doen dit in samenspraak met het PIT en zo nodig met de FG;
- Een behoorlijke en zorgvuldige aanpak. Dit in overeenstemming met de wet. De FG bevestigt dit aan de hand van een verklaring waarbij hij eventueel ook aanbevelingen doet voor verdere optimalisering van de bedrijfsvoering;
- De afspraak wanneer het procesplan herzien moet worden. De proceseigenaar is verantwoordelijk voor het beheer van zijn procesplan. Een procesplan wordt bijgesteld wanneer in de praktijk blijkt dat de maatregelen onvoldoende passend blijken naar aanleiding van terechte klachten of andere onacceptabele incidenten;
- Een 'artikel 30-formulier' waarvan zij een afschrift verstrekken aan de portefeuillehouder privacy voor opname in het artikel 30-register. Proceseigenaren melden veranderingen voor het artikel 30-register onmiddellijk aan de hand van wijzigingsformulieren.

Artikel 30-formulier bevatten de volgende informatie:
1. Een beschrijvende aanduiding (naam) van het proces en de bijbehorende gegevensverwerking;
2. De PIA-scoring van het proces;
3. De naam, contactgegevens en het mandaat van de proceseigenaar;
4. Indien van toepassing: de contactgegevens van degene die die proceseigenaar assisteert in privacy aangelegenheden;

5. De bedrijfsdoelen die met het proces zijn gediend;
6. Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
7. De categorieën van ontvangers van de persoonsgegevens en, indien van toepassing, informatie over internationaal gegevensverkeer;
8. Informatie op hoofdlijnen over genomen beheersmaatregelen (key controls) – met name termijnen voor gegevensvernietiging en de aanpak op het gebied van informatiebeveiliging;
9. De FG-verklaring, indien afgegeven.

Ook als er **geen** PIA uitgevoerd moet worden, wordt dit vastgelegd in een document. Hierin wordt de reden opgenomen waarom er geen PIA wordt uitgevoerd en wanneer dit opnieuw moet worden herzien.