Privacybeleidskader Gemeente Aa en Hunze

Algemeen deel (bestuurlijk privacybeleid)

Versie 02

12 december 2017

Privacybeleidskader Gemeente Aa en Hunze

Algemeen deel (bestuurlijk privacybeleid)

Inhoudsopgave

Definities

AVG (Algemene Verordening Gegevensbescherming) – Europese wet op de verwerking van persoonsgegevens, die rechtstreeks geldt in alle lidstaten.
Bedrijfsproces – gemeentelijke bedrijfsvoering waarbij persoonsgegevens worden verwerkt.
FG (Functionaris voor Gegevensbescherming) – wettelijk toezichthouder voor de naleving van privacywetgeving en bedrijfsvoorschriften
(Gegevens)verwerking – zowel geheel of gedeeltelijk geautomatiseerde operationele informatieverwerking (bijvoorbeeld archiveren, analyseren, doorgeven, raadplegen) als ieder geheel daarvan (bijvoorbeeld de salarisadministratie, gemeentebelastingen of thuiszorg).
Persoonsgegevens – gegevens over personen en waarvan de gegevensverwerking door herleidbaarheid gevolgen heeft in de persoonlijke levenssfeer (privacy impact heeft).
PIA (privacy impact assessment) – een beoordelingsrapport waarin een gegevensverwerking wordt geanalyseerd op noodzaak en risico's vanuit privacyoptiek, resulterend in een lijst van passende beheersmaatregelen (waarborgen)
PIA-score – getalsmatige classificatie van noodzaak of risico van gegevensverwerking, als uitkomst van een PIA
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
Privacybeleidskader – het bestuurlijk privacybeleid van een organisatie, die de kapstok vormt voor
Privacyaudit – controles op de naleving van privacybeleid en privacywetgeving
Privacybeleid – het privacybeleidskader en alle nadere uitwerkingen hiervan
Privacybeleidsvoering – sturing op privacy door het management ('governance')
Privacyincidenten – gebeurtenissen waartegen het privacybeleid 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 – lijnmanagers die verantwoordelijk zijn voor uitvoering van gemeentelijke taken zoals burgerzaken, uitvoering Jeugdwet, belastingen en veiligheid.
Procesplan – nadere, schriftelijk geformuleerde beheersmaatregelen voor de bescherming van persoonsgegevens (in de regel de gedocumenteerde follow-up van een PIA)
Programmanager Privacy – degene die namens de portefeuillehouder privacy uitvoering geeft aan het privacybeleid.
Servicepunt – het contactpunt voor personen waar zij terecht kunnen voor het uitoefenen van hun privacyrechten.
Uitvoeringsorganisatie - een organisatie waaraan een of meerdere bedrijfsprocessen zijn uitbesteed

1 Kernpunten

1.1 Voor wie?

Het Privacybeleidskader Gemeente Aa en Hunze bevat managementafspraken tussen het college en proceseigenaren. De afspraken moeten worden nagekomen in alle gevallen dat persoonsgegevens worden gebruikt, opgeslagen of uitgewisseld (‘verwerking van persoonsgegevens’).

1.2 Doel

Het doel van het Privacybeleidskader Gemeente Aa en Hunze is om te waarborgen dat personen gegarandeerd zijn van een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet.

1.3 Visie en missie

Gemeente Aa en Hunze ziet de bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. In de datamaatschappij moeten inwoners en medewerkers erop vertrouwen dat we persoonsgegevens op rechtmatig, zorgvuldig en veilig verwerken. Wie voor ons werkt, begrijpt dit en laat zich hierdoor leiden in zijn of haar dagelijks werk. Het college van B&W schept de voorwaarden voor een privacybewuste organisatiecultuur en voert in dat kader niet aflatend privacybeleid. We zijn transparant over onze gegevensverwerking en de manier waarop wij persoonsgegevens beschermen. Bij dilemma’s gaan wij de dialoog met betrokkenen aan en zoeken gezamenlijk naar oplossingen.

1.4 Kernpunten

1) Zorg voor privacy is een managementverantwoordelijkheid. Het college en proceseigenaren sturen op privacy volgens deze kernpunten van privacymanagement:
    1. Een proceseigenaar voert, als onderdeel van zijn verantwoordelijkheden, regie en houdt toezicht op zijn proces(sen) op basis van dit privacybeleidskader;
    2. Bij processen waaraan privacyrisico’s zijn verbonden, hanteert de proceseigenaar een procesplan;
    3. Een procesplan is duidelijk, actueel, stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd;
    4. Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel;
    5. Binnen een proces worden geen onrechtmatig verkregen gegevens verwerkt;
    6. Een procesplan benoemt de waarborgen voor een eerlijke, veilige en betrouwbare uitvoering van het proces;
    7. Een procesplan omvat eventuele opdrachten aan uitvoeringsorganisaties en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden;
    8. Een proceseigenaar handelt vragen of klachten van inwoners of medewerkers binnen vier weken af.;
    9. Bij privacyincidenten hanteert de proceseigenaar de Procedure meldplicht datalekken;
    10. Bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen op grond van dit privacybeleidskader en het betreffende procesplan.
2) Het college voorziet in een team van professionals dat het college en de proceseigenaren ondersteunt in de privacybeleidsvoering.

3) Het college voorziet in faciliteiten voor bewustwording en training.
4) Gemeente Aa en Hunze beschikt over maatregelen voor privacy-incidentmanagement.
5) Gemeente Aa en Hunze evalueert tweejaarlijks de doeltreffendheid en de doelmatigheid van dit privacybeleidskader.
6) Het college informeert de raad over de privacybeleidsvoering.
7) Het college handhaaft het privacybeleid. Gemeente Aa en Hunze heeft een Functionaris voor Gegevensbescherming aangesteld die toeziet op de naleving van privacywetgeving.

1.5 Scope

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

Het Privacybeleidskader Gemeente Aa en Hunze is het algemene deel van het privacybeleid binnen de gemeente. Het algemene beleidskader is de kapstok voor eventueel noodzakelijk privacybeleid binnen de verschillende programma's van Gemeente Aa en Hunze.

1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleidskader van Gemeente Aa en Hunze heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Informatiebeleid
De gemeente kent een door het college en raad vastgesteld informatiebeleidsplan (IBP). In het IBP is aandacht voor beveiliging en privacy van gegevens. Voor het verbeteren van de informatiebeveiliging en het waarborgen van de privacy is vanuit het IBP een aanzienlijk bedrag beschikbaar gesteld.

Integriteitsbeleid
Privacybeleidsuitvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid. Het integriteitsbeleid bestaat o.a. uit een door B&W vastgestelde gedragscode. In deze gedragscode worden het omgaan met gevoelige gegevens en het respect hebben voor 'privacy' nadrukkelijk benoemd.

Informatiebeveiligingsbeleid
In juni 2015 is door het college het informatiebeveiligingsbeleid goedgekeurd. De betrouwbaarheid, beschikbaarheid en vertrouwelijkheid van gegevens heeft vanzelfsprekend een nauwe relatie met het privacybeleidskader.

Personeel en organisatie
Het sturen op gekwalificeerd personeel, cultuur en een gekwalificeerde organisatie wordt uitgevoerd vanuit het P&O beleid. Hoewel er binnen Aa en Hunze geen algeheel vastgesteld personeelsbeleid is, zijn er diverse door het college vastgestelde regelingen zoals bijvoordbeeld een wervings- en selectieprotocol, een regeling voor opleiding en ontwikkeling en een klokkenluidersregeling.

Communicatie
De gemeente Aa en Hunze heeft in 2013 een integraal communicatiebeleid vastgesteld, dat ingaat op informatievoorziening, interactieve beleidsvorming en social media. Voor de jaarlijkse uitvoering wordt een jaarplan communicatie opgesteld, waarin o.a de ontwikkelingen in het sociaal domein en het organisatieontwikkelings-programma "Aa en Hunze stroomt" worden

ondersteund. Door privacy op te nemen als onderwerp in het volgende jaarplan kan communicatie de bewustwording ondersteunen.

Kwaliteitsbeleid

Het privacybeleidskader richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap. Binnen Aa en Hunze is geen formeel vastgesteld kwaliteitsbeleid. Wel zijn er vanuit “Aa en Hunze stroomt” diverse initiatieven ter verbetering van de processen en bijbehorende administratieve organisatie. Tevens toetsen we jaarlijks onze administratieve organisatie aan de hand van het interne controleplan;.

Continuïteit- en risicomanagement

Het privacybeleidskader schept waarborgen op het gebied van continuïteit en risicomanagement. Een goede privacybeleidsvoering gaat afbreuk –en aansprakelijkheisrisico’s tegen en voorkomt dat werkprocessen spaak lopen. Anders gezegd, wanneer de gegevensverwerking in een werkproces een schending bevat op de privacy vormt dit een gevaar voor de continuïteit van dit proces. De gemeente riskeert hiermee een boete.

2 Privacy management

Het college van Gemeente Aa en Hunze is verantwoordelijk voor de naleving van privacywetgeving en voert proactief privacybeleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat dit evenwichtig plaatsvindt. Dat wil zeggen; behoorlijk, zorgvuldig en in overeenstemming met de wet.

Privacy management is SMART-georganiseerd en heeft zelfstandige aandacht binnen de planning & control-cyclus van de gemeentelijke organisatie.

Het college legt over de privacybeleidsvoering verantwoording af aan de raad en betracht beleidstransparantie met behulp van publieksvoorlichting.

Het college draagt zorg voor de documentatie van beleid en maatregelen zodat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.

Het college houdt een register van de gegevensverwerkingen bij die onder hun verantwoordelijkheid plaatsvinden zoals bedoeld in artikel 30 Algemene Verordening Gegevensbescherming (AVG).

2.1 Managementstructuur

Het college is verantwoordelijk voor het voorzien in passende privacywaarborgen bij de uitvoering van gemeentelijke taken.

Privacy valt onder de verantwoordelijkheid van de portefeuillehouder privacy in het college, die voor dagelijkse aansturingstaken een programmamanager privacy kan benoemen.

Het college heeft een Functionaris voor Gegevensbescherming (FG) aangewezen – zie **Fout! V erwijzingsbron niet gevonden.**.

Het college voorziet in een team van professionals (hierna het P&I-team, kortweg: PIT) die onder de verantwoordelijkheid valt van de portefeuillehouder privacy. Het PIT ondersteunt proceseigenaren (zie hierna) bij de uitvoering van het gemeentelijk privacybeleidskader.

Teamleiders zijn operationeel eindverantwoordelijk voor de uitvoering van gemeentelijke taken (burgerzaken, openbare orde en veiligheid, gemeentebelastingen, sociaal domein, ruimtelijke ordening en milieu, e.a.).

2.2 Proceseigenaarschap

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

- Een teamleider is **proceseigenaar**.
- De proceseigenaar kan verantwoordelijkheden mandateren aan medewerkers ('subproceseigenaren')
- Het college blijft eindverantwoordelijk voor de privacybestendigheid van gemeentelijke processen als de **'verwerkingsverantwoordelijke'** in de zin van de AVG.

Proceseigenaren voeren regie over hun proces(sen) op basis van procesplannen (zie hierna in hoofdstuk 4.1) die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een

procesplan dient te passen binnen dit privacybeleidskader en is steeds in overeenstemming met de feitelijke situatie.

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

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

Een proceseigenaar kan proceseigenaarschap mandateren aan een partij buiten de gemeentelijke organisatie met toestemming van de hoofdproceseigenaar (samenwerking met externe ketenpartners). Het mandaat blijkt uit, bijvoorbeeld, een inkoopcontract, de deelname in een gemeenschappelijke regeling of gebruikmaking van een landelijke voorziening. Bij externe ketensamenwerking blijft de opdrachtgevende proceseigenaar namens het college verant-woordelijk voor de privacybestendigheid van de aanpak door hem ingeschakelde ketenpartner(s) en houdt hierop toezicht. De wet kan dwingende bepalingen bevatten over wederzijdse verantwoordelijkheden bij ketensamenwerking.

Wanneer gemeentelijke processen zodanig zijn georganiseerd dat de onderliggende gegevensverwerking onder de verantwoordelijkheid van meerdere teamleiders vallen, is het afdelingshoofd de proceseigenaar.

2.3 Toezicht

De Functionaris voor Gegevensbescherming (FG) is de toezichthouder van Gemeente Aa en Hunze op de naleving van privacywetgeving conform artikel 37-39 AVG.

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

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

De FG heeft als taken:
- Het opstellen en implementeren van strategisch privacybeleid (kapstokbeleid, dit beleidskader).
- toezien op de naleving van de AVG, de Wbp en het privacybeleidskader van de gemeente Aa en Hunze.
- informeren en adviseren over de AVG, de Wbp en het privacybeleidskader van de gemeente Aa en Hunze;
- toezien op het bijhouden van een register van de verwerkingsactiviteiten van de Verwerkingsverantwoordelijke conform art. 30 AVG;
- toezien op de uitvoering van PIA's conform art. 35 AVG en hierover desgevraagd advies uitbrengen;
- melden van Datalekken aan de AP conform art. 33 AVG;
- optreden als contactpunt voor de AP;
- beheren van en adviseren over verwerkersovereenkomsten.

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 Aa en Hunze waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.
- Het college en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.
- De FG mag niet geïnstrueerd worden over invulling van taken, onder druk worden gezet, gestraft of ontslagen.

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

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

3 Privacybeleid Gemeente Aa en Hunze

3.1 Algemeen

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

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

3.2 Noodzakelijke gegevensverwerking

Proceseigenaren verwerken persoonsgegevens uitsluitend voor de volgende doelen, voor zover dit valt binnen hun mandaat en noodzakelijk is voor:

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

3.3 Kapstokregeling

Het Privacybeleidskader van Gemeente Aa en Hunze heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten. Voor zover dit speelt, geven proceseigenaren via procesplannen nadere invulling aan het Privacybeleidskader Gemeente Aa en Hunze, in samenspraak met het PIT en de FG.

De volgende ’ programma’s worden binnen de gemeente onderscheiden:

- Bestuur en ondersteuning
  - Bestuur
  - Burgerzaken
  - Belastingen
  - Ondersteuning organisatie
- Veiligheid
  - Openbare orde en veiligheid
- Verkeer en vervoer
- Economie
  - Economische ontwikkeling en promotie
- Onderwijs
  - Onderwijshuisvesting
  - Onderwijsbeleid en leerlingenzaken
- Sport, cultuur en recreatie
- Sociaal domein
  - Maatschappelijke ondersteuning
  - Wijkteams
  - Inkomensregelingen
  - Maatschappelijke opvang

    - Jeugdzorg
- Volksgezondheid en milieu
    - Volksgezondheid
    - Milieubeheer
    - Afval
    - Begraafplaatsen
- Volkshuisvesting, Ruimtelijke Ordening en Stedelijke vernieuwing
    - Ruimtelijke ordening
    - Wonen en bouwen

Procesplannen beschrijven werkprocessen, de bijbehorende gegevensverwerking en de privacywaarborgen waarmee de werkprocessen omkleed zijn zodat een privacybestendige aanpak ontstaat.

Het Privacybeleidskader Gemeente Aa en Hunze bevat ook de aanzet voor het regelen van aspecten van privacybeleidsvoering die onder de directe verantwoordelijkheid van het college vallen.

Het Privacybeleidskader Gemeente Aa en Hunze, procesplannen en de daadwerkelijke uitvoering hiervan via organisatorische, technische en juridische oplossingen vormen samen het privacybeleid Gemeente Aa en Hunze. In geval van tegenstrijdigheid heeft het Privacybeleidskader Gemeente Aa en Hunze voorrang.

3.4 Inachtneming bijzondere wettelijke voorschriften

Op basis van het Privacybeleidskader Gemeente Aa en Hunze, geeft de gemeente uitvoering aan de Algemene Verordening Gegevensbescherming. Voor zover van toepassing, houden proceseigenaren tevens goed rekening met bijzondere wettelijke voorschriften – met name privacy-relevante bepalingen in de Wet basisregistratie personen, de Telecommunicatiewet, de Participatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning.

4 Privacyservices

4.1 Rechten

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

4.2 Vragen

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

4.3 Klachten

Bij klachten:
- hebben personen het recht om zich te wenden tot hiervoor aangewezen servicepunten;
- klachten worden zo snel mogelijk maar uiterlijk binnen twee weken afgehandeld;
- het servicepunt meldt de klacht onmiddellijk bij de incidentenregeling volgens paragraaf 5.6, die het PIT betrekt voor de feitelijke klachtafhandeling.
- Het PIT onderzoekt de gegrondheid van de klacht, waarbij zij name nagaat of de klacht betrekking heeft op de naleving van privacywetgeving en/of het privacybeleid van Gemeente Aa en Hunze.
- Het PIT kan de FG om advies vragen over de afhandeling van de klacht.

4.4 Beroep

Personen hebben het recht om na afhandeling van een klacht conform 4.3, hiertegen in beroep gaan bij de FG voor zover het beroep gericht is op de naleving van privacywetgeving en/of het privacybeleid van Gemeente Aa en Hunze.

5 Privacy programma

5.1 Werkprogramma

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

5.2 Bewustwording en training

Het college bevordert samen met hoofdproceseigenaren een privacybewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van medewerkers en leidinggevenden.

5.3 PR & communicatie

Het college is transparant over de privacybeleidsvoering en voert op dit thema evenwichtig communicatiebeleid waarbij proceseigenaren zo nodig voorzien in bijzondere voorlichting aan specifieke doelgroepen.

5.4 Verdere verwerking, archiefbeleid, gegevensvernietiging

Het college voorziet samen met proceseigenaren in met passende waarborgen omklede verdere verwerking van gegevens voor verenigbare doelen zoals het genereren van managementinformatie. Ook wordt voorzien in met passende waarborgen omklede oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.

5.5 Informatiebeveiliging

Het college ziet erop toe dat informatieveiligheid van Gemeente Aa en Hunze in lijn met de geldende norm wordt georganiseerd. Gemeente Aa en Hunze beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) die deelneemt in het PIT en samenwerkt met de portefeuillehouder privacy en de FG. Geheimhoudingsverklaringen zijn instrumenten binnen de gemeentelijke aanpak voor privacybescherming en informatieveiligheid. Bij processen in de klassen C2-3, B2-3, A2-3 worden aanvullende geheimhoudingsafspraken gehanteerd voor zover uit PIA's blijkt dat extra waarborgen op het gebied van vertrouwelijkheid/geheimhouding functioneel zijn.

5.6 Regeling privacyincidenten

Het college voorziet in een procedure voor privacyincidenten die onder de verantwoordelijkheid valt van de portefeuillehouder privacy[1]. Deze procedure voor privacyincidenten bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit en vertrouwelijkheid

[1] Zie het document 'Werkinstructie melden datalekken'

van informatievoorzieningen en gegevensopslag aantasten. Ook bevordert het college het oefenen op privacy-incidenten, incident management en crisiscommunicatie.

5.7 Handhaving

Het college handhaaft het gemeentelijk privacybeleid op basis van een regeling voor beloning van voorbeeldig gedrag volgens het Privacybeleidskader Gemeente Aa en Hunze.

5.8 Beleidsevaluatie

Hoofdproceseigenaren doen jaarlijks verslag aan de concerncontroller van hun oplossingen en incidenten die onder hun verantwoordelijkheid hebben voorgedaan met afschrift aan de FG. De FG doet jaarlijks verslag aan het college en geeft aanbevelingen die strekken tot verdere optimalisering de privacybeleidsvoering. Het college besluit over bijsturing van het gemeentelijk privacybeleid met inachtneming van de aanbevelingen van de FG.

6 Auditbeleid

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

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

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

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

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

7 Bijlagen

7.1 Gedragsnorm 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 Gemeente Aa en Hunze een privacybestendige cultuur te realiseren.

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

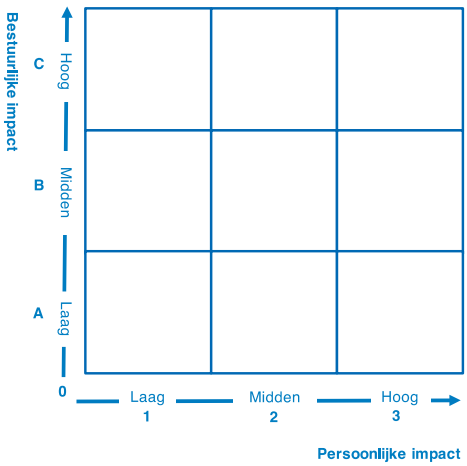
Het bijhouden van het art. 30 register valt onder de verantwoordelijkheid van de concerncontroller. Proceseigenaren helpen om het register volledig en actueel te laten zijn door middel van ‘artikel 30-formulieren’.

Het college is transparant over de bedrijfsvoering, gegevensverwerking en privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie de gemeente gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking.

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

7.1.1 Procesplan-aanpak

Aan procesplannen liggen privacy impact assessments (PIA’s) ten grondslag. PIA’s zijn instrumenteel voor het kunnen bepalen van passende beheersmaatregelen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van de PIA, zoals verwoord in het PIA-rapport.



Voor eenduidig begrip hanteert Gemeente Aa en Hunze een systeem van positieve en negatieve PIA-scores. Hoe hoger de PIA-score, hoe robuuster de beheersmaatregelen (privacywaarborgen). Proceseigenaren volgen het advies van het PIT bij de vaststelling van hun PIA-score. PIA-scores worden bepaald aan de hand van de hiernaast afgebeelde matrix.

Proceseigenaren zijn goed bekend met hun PIA-scores en hanteren onderstaande tabel om te bepalen in hoeverre PIA’s tevens deel uitmaken van het procesplan om op die manier de keuzes voor beheersmaatregelen te verantwoorden.

PIA-Score	PIA-rapport	Procesplan	Akkoord FG
A1	-	-	-
A2	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
A3	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
B1	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen

B2	Beknopt	PIA-rapport maakt deel uit van procesplan	Aanbevolen
B3	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C1	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C2	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht
C3	Volledig	PIA-rapport maakt deel uit van procesplan	Verplicht

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 onbeschikbaar te zijn.
6. **Niet-inachtneming van bijzondere wettelijke voorschriften:** bij gebruik, opslag of uitwisseling van informatie worden formele verplichtingen veronachtzaamd.[2]
7. **Onbewaakte gegevensverwerking:** de proceseigenaar verzuimt om te controleren of de privacywaarborgende maatregelen daadwerkelijk zijn geëffectueerd of te evalueren in hoeverre zijn procesplan bijstelling behoeft.

Voor A1-processen volstaan algemene oplossingen. Zolang een proces als A1 gekwalificeerd is, is daarvoor in mindere mate aandacht nodig.

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

7.1.2 Lijst van key controls

Proceseigenaren vatten, in samenspraak met het PIT en zo nodig de FG, hun procesplannen samen in een lijst van kenmerkende beheersmaatregelen (‘key controls’) voor sturingsdoeleinden en controle (zie paragraaf 6).

PIA-Score	Key controls	Samenspraak PIT	Samenspraak FG
A1	-	-	-
A2	Ja	Ja	Aanbevolen
A3	Ja	Ja	Verplicht
B1	Ja	Ja	Aanbevolen
B2	Ja	Ja	Aanbevolen
B3	Ja	Ja	Verplicht
C1	Ja	Ja	Verplicht
C2	Ja	Ja	Verplicht

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

C3	Ja	Ja	Verplicht

Proceseigenaren nemen de lijst van key controls op aan het einde van het procesplan.

7.1.3 FG-verklaring

Een evenwichtig procesplan beschrijft een behoorlijke en zorgvuldige aanpak, in overeenstemming met de wet. De FG bevestigt dit aan de hand van een verklaring waarbij hij eventueel ook aanbevelingen doet voor verdere optimalisering van de bedrijfsvoering.

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

Proceseigenaren nemen FG-verklaringen op aan het einde van het procesplan.

7.1.4 Artikel 30-formulieren

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

Een artikel 30-formulier bevat de volgende informatie:

- Naam en beschrijving verwerkingsproces
- De naam en contactgegevens van de proceseigenaar
- De PIA scoring van het proces (A1 tot C3)
- Het doel van de verwerking
- De grondslag voor de verwerking
- Een beschrijving van de categorieën van betrokkenen
- Een beschrijving van de categorieën van persoonsgegevens
- Een beschrijving van de gebruikers/ontvangers aan wie de gegevens worden verstrekt
- Doorgifte aan derde landen of internationale organisaties
- De bewaartermijn van de verzamelde persoonsgegevens
- Een algemene beschrijving van de geldende technische en organisatorische beveiligingsmaatregelen

7.1.5 Beheer procesplan

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.

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

PIA-Score	Evaluatie	Advies FG
A1	4 jaarlijks	-

A2	3 jaarlijks	Aanbevolen
A3	jaarlijks	Verplicht
B1	3 jaarlijks	Aanbevolen
B2	2 jaarlijks	Aanbevolen
B3	jaarlijks	Verplicht
C1	jaarlijks	Verplicht
C2	jaarlijks	Verplicht
C3	jaarlijks	Verplicht

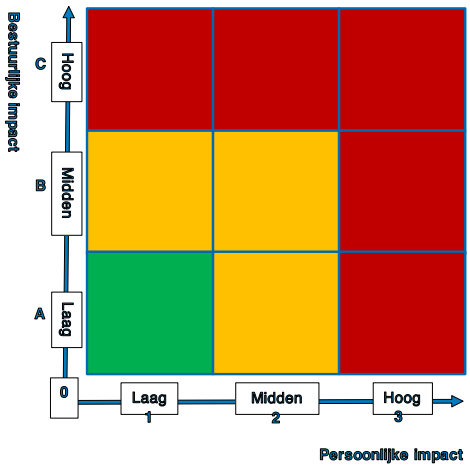
7.2 Het PIA-proces

7.2.1 Wanneer moet ik een PIA doen?

Wanneer een gegevensverwerking een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen moet er een PIA gedaan worden. Wat is de impact van een fout in het proces? Hoe hoger de impact hoe hoger het risico. Denk bijvoorbeeld aan het niet ontvangen van de juiste Jeugdhulp, de impact hiervan op iemands leven kan groot zijn.
Verzwarende omstandigheden bij de risico-overweging zijn:

- Het gebruik van nieuwe technologie (gps, gezichtsherkenning)
- Profileren of het voorspellen van gedrag (big data)
- Geautomatiseerde besluitvorming (zonder menselijke tussenkomst)
- Stelselmatig monitoren van openbare ruimten (cameratoezicht)
- Het gebruik van bijzondere persoonsgegevens (medisch, strafrechtelijk, religie, ras, etc.)
- Grootschaligheid van de verwerking (alle inwoners versus 100 inwoners).
- Combineren van bestaande datasets
- Verwerken van gegevens van kwetsbare betrokkenen (minderjarigen, cliënten, ouderen)
- Dataverkeer naar landen buiten de EU
- Wanneer de verwerking gericht is op een rechtsgevolg (toekennen/weigeren beschikking)

De eerste stap is de risicokwalificatie van het proces. De waardering loopt van A1 tot C3. Bij een A1 proces (linksonder) is zowel de bestuurlijke impact als de persoonlijke impact laag. Denk hierbij bijvoorbeeld aan het niet krijgen van een vergunning voor een buurtbarbecue door een fout in het proces.
Bij een C3 proces (rechtsboven) kan een fout zowel bestuurlijk als persoonlijk serieuze gevolgen hebben. Denk hierbij aan het van het balkon vallen van een minderjarig meisje in Hoogeveen door foutieve informatievoorziening in het sociale domein.
De waardering van het proces heeft gevolgen voor de frequentie van evaluatie en de benodigde maatregelen, zie daarvoor hoofdstuk 7.1 van het beleidskader. Een A1 proces is een proces met een dusdanig laag risico dat een PIA niet noodzakelijk is.



7.2.2 Hoe doe ik een PIA?

Een PIA begint met het invullen van de basisinformatie voor het verwerkingsregister, zie 7.1.4. Daarna worden er gesprekken gehouden met medewerkers, applicatiebeheerders en proceseigenaar. Het PIT ondersteunt de proceseigenaar met het doen van de PIA. Voor het doen van de PIA wordt het Rijksmodel gehanteerd.

7.2.3 Wat moet er na de PIA gebeuren?

Nadat de PIA is gedaan moet er een PIA rapport worden opgesteld met daarin de uitkomsten. Voor het opstellen van het PIA-rapport worden de eisen uit het Rijksmodel gehanteerd.

7.2.4 Verdere afspraken uit het beleidskader

- Proceseigenaren hanteren procesplannen. Een procesplan beschrijft een werkproces, de bijbehorende gegevensverwerking en de privacywaarborgen waarmee de werkprocessen zijn omkleed zodat een privacybestendige aanpak ontstaat. Het PIA rapport kan hier invulling aan geven.
- Een proceseigenaar is verantwoordelijk voor het beheer van zijn procesplan. Een procesplan wordt bijgesteld wanneer in de praktijk blijkt dat de maatregelen onvoldoende passend zijn. In ieder geval wordt een procesplan minimaal één keer per 4 jaar geëvalueerd (bij een A1 proces) tot maximaal één keer per jaar bij processen met een hoger risico.
- Proceseigenaren vatten hun procesplannen samen in een lijst van kenmerkende beheersmaatregelen (key controls) voor sturingsdoeleinden en controle.