

Privacybeleid Gemeente Aa en Hunze



Oktober 2022**Versie 1.0****Inhoud**

1. Inleiding	3
2. Doel en scope privacybeleid	4
3. Beleidsuitgangspunten	5
4. Rollen en verantwoordelijkheden	8
4.1 Bestuurlijke rollen en verantwoordelijkheden	8
4.2 Ambtelijke rollen en verantwoordelijkheden	8
5. Sturing en verantwoording	10
5.1 Sturing	10
5.2 Verantwoording	10
6. Overige elementen Algemene Verordening Gegevensbescherming	12
6.1 Rechten van betrokkenen	12
6.1.1 Uitoefening van rechten	12
6.2 Beveiligingsmaatregelen	12
6.3 Verwerkers en verwerkersovereenkomsten	12
6.3.1 Inschakeling van een verwerker	12
6.3.2 Gemeente Aa en Hunze als verwerker	13

7. Evaluatie en wijziging van het beleid	14
Bijlage 1: Privacybeleid Wpg gemeente Aa en Hunze	15

1. Inleiding

Op 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna AVG) in werking getreden. Vanaf die datum geldt dezelfde privacywetgeving in de gehele Europese Unie (EU). Lidstaten hebben een beperkte vrijheid om aanvullende regelgeving vast te stellen. In Nederland is deze aanvulling gekomen in de vorm van de Uitvoeringswet AVG (UAVG).

Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens bij de gemeente Aa en Hunze in veilige handen zijn. Daarnaast is ook de samenleving kritischer en veeleisender geworden ten aanzien van de wijze waarop met privacygevoelige informatie wordt omgegaan. Deze behoefte uit de samenleving heeft zijn vertaling gekregen in dit beleid en daarbij behorende opgezette governance-structuur.

2. Doel en scope privacybeleid

Binnen de gemeente Aa en Hunze werken we veel met persoonsgegevens van burgers, medewerkers en (keten)partners. Deze verzamelen we voornamelijk voor het goed kunnen uitvoeren van onze gemeentelijke taken. Men moet er op kunnen vertrouwen dat de gemeente Aa en Hunze zorgvuldig en veilig met deze gegevens omgaat. Nieuwe technologische ontwikkelingen, een grotere keten, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente Aa en Hunze is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

De aanleiding voor dit privacybeleid is de actualisatie van het bestaande beleid, wat uit 2018 dateert. Ook de nieuwe verplichtingen rondom de Wet Politiegegevens (WPG) zorgen voor een noodzaak tot actualisatie. Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. De gemeente Aa en Hunze geeft met dit beleid duidelijk richting aan hoe de organisatie omgaat met privacy en laat zien hoe zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen en gegevensverzamelingen van de gemeente Aa en Hunze waarin persoonsgegevens worden verwerkt.

3. Beleidsuitgangspunten

De gemeente Aa en Hunze gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente Aa en Hunze houdt zich hierbij aan de volgende uitgangspunten:

1. Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

2. Risicogerichte benadering

Het waarborgen van privacy is een structureel proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement waar de Functionaris Gegevensbescherming (FG) en de Privacy- en Security Officer (PSO) ondersteuning aan geven. De FG in de toezichhoudende- en adviserende rol en de PSO in adviserende- en ondersteunende rol. De gemeente Aa en Hunze hanteert hierbij een risicogerichte werkwijze.

De eerste stap in het proces om het risico en eventueel te treffen maatregelen te bepalen is het uitvoeren van een Privacy Impact Assessment (PIA). Een teamleider is verantwoordelijk voor het (laten) uitvoeren van een PIA. Een PIA is een (korte) analyse die door de PSO samen met een specialist van het betreffende team wordt uitgevoerd. Uit deze analyse blijkt het risico voor de betrokkene van een verwerking van persoonsgegevens. Aan de hand van deze analyse worden maatregelen geadviseerd om het risico te mitigeren. De verantwoordelijk teamleider is eigenaar van het resultaat van de PIA en neemt een besluit over de te nemen maatregelen. De resultaten van een PIA worden periodiek geëvalueerd. Bij de inkoop van nieuwe applicaties of diensten wordt door middel van een aantal korte vragen bepaald of er een noodzaak is om een PIA uit te voeren.

Op alle verwerkingen van persoonsgegevens zijn de beginselen van de AVG van toepassing. In tegenstelling tot de BIO voor informatieveiligheid is er geen standaard framework waaruit de nodige maatregelen blijken. Per geval wordt beoordeeld of er aan de beginselen van de AVG is voldaan en waar nog (maat-)werk nodig is. De FG toetst aan de hand van de uitgevoerde PIA of het privacy-advies aan de wettelijke- en beleidskaders voldoet.

Het uitgangspunt is om eerst een PIA uit te voeren, daarna noodzakelijke maatregelen te treffen en dan pas persoonsgegevens te gaan verwerken. De AVG stelt deze volgorde als eis. Zeker wanneer het gaat om hoge risico's is het voor de betrokkene belangrijk dat de verantwoordelijke teamleider vooraf maatregelen treft. Ook als de inschatting van het risico niet op tijd gebeurt is er al sprake van een mogelijk privacy-risico. Voor hoge risico's kan gebruik worden gemaakt van een

risicoacceptatie-overeenkomst (RAO). Via dit middel kan een teamleider een risico tijdelijk accepteren. Alle risico's worden geregistreerd in het risicoregister. Het risicoregister wordt periodiek besproken met de concerncontroller en teamleider facilitair.

Deze risicogerichte benadering, die sterk lijkt op de risicogerichte benadering vanuit de BIO, zorgt er voor dat de privacy bij de gemeente Aa en Hunze bevorderd wordt op de plekken waar dat het meest belangrijk is.

3. Grondslag en doelbinding

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

4. Dataminimalisatie

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

5. Bewaartermijnen

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

6. Integriteit en vertrouwelijkheid

De gemeente Aa en Hunze gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. De gemeente Aa en Hunze beperkt de toegang tot inzage en wijziging van (persoons)gegevens tot degenen die dit vanuit hun functie nodig hebben. Daarbij zorgt de gemeente Aa en Hunze voor passende bescherming en beveiliging van persoonsgegevens. Dit door bijvoorbeeld het aggregeren, anonimiseren of pseudonimiseren van persoonsgegevens. Een verdere uitwerking van deze beveiliging is vastgelegd in het gemeentelijke informatiebeveiligingsbeleid.

7. Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente Aa en Hunze afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet.

8. 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.

9. Proportionaliteit

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

10. Rechten betrokkene

De gemeente Aa en Hunze respecteert de rechten van betrokkenen en honoreert, voor zover redelijk en mogelijk, de rechten van betrokkenen.

11. Beveiligingsincidenten en datalekken

Een informatiebeveiligingsincident vindt plaats wanneer de beschikbaarheid, vertrouwelijkheid of integriteit van informatie wordt verstoord. Denk aan inbrekers, (stroom-)storingen, het ontbreken van een back-up of het achterlaten van een gevoelig document bij een printer. Als bij dit soort incidenten persoonsgegevens betrokken zijn, dan is er mogelijk sprake van een datalek.¹ Voor de afhandeling hiervan is de procedure voor het afhandelen van kwetsbaarheden, datalekken en beveiligingsincidenten opgesteld. Deze procedure bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop bij een datalek te beperken en de getroffen personen te beschermen. Deze procedure wordt periodiek geëvalueerd en waar nodig aangepast.

¹ Bij een **datalek** gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Ook hierdoor kunnen de betrokken personen namelijk schade leiden.

4. Rollen en verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden er zijn binnen de organisatie op het gebied van privacy. De methodiek waarop dit is gedaan sluit aan bij het in de bedrijfsvoering bekende Three Lines of Defence (3LoD) model. In dit model is het lijnmanagement (de eerste lijn) verantwoordelijk voor de eigen processen en dus ook voor privacy. In de tweede lijn ondersteunt en adviseert de PSO de eerste lijn op het gebied van privacy. In de derde lijn beoordeelt en controleert de interne toezichthouder privacy – de Functionaris Gegevensbescherming – in welke mate de gemeente Aa en Hunze voldoet aan het gemeentelijke privacybeleid.

4.1 Bestuurlijke rollen en verantwoordelijkheden

De gemeenteraad en het college van burgemeester en wethouders

Het college van burgemeester en wethouders van de gemeente Aa en Hunze (college van B&W) is het verantwoordelijke bestuursorgaan voor alle verwerkingen van persoonsgegevens binnen de gemeente Aa en Hunze. Het college informeert de raad over de privacybeleidsvoering via de reguliere planning & control cyclus.

4.2 Ambtelijke rollen en verantwoordelijkheden

De Gemeentesecretaris

De gemeentesecretaris is als algemeen directeur de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur van het college van B&W. Hij of zij vormt de schakel tussen het bestuur en ambtelijke organisatie en is ambtelijk eindverantwoordelijk voor de implementatie van dit beleid.

Concerncontroller

De concerncontroller is verantwoordelijk voor het bestuurlijk advies over financiële risico's. Openstaande privacyrisico's worden daarom periodiek met de concerncontroller besproken.

Teamleider

De verantwoordelijkheid voor het voldoen aan het gemeentelijke privacybeleid en de onderliggende privacy vereisten ligt op operationeel niveau bij de teamleiders. De teamleiders hebben uitvoeringsgerichte bevoegdheden zoals het beslissen over te nemen maatregelen en ondertekening van verwerkersovereenkomsten. De teamleiders zijn medeverantwoordelijk voor het voldoen aan de verantwoordingsplicht (accountability). Zij informeren de FG – op zijn verzoek – over privacy aspecten binnen de processen waar zij voor verantwoordelijk zijn. Denk hierbij aan onderzoek aan de hand van incidenten of geconstateerde misstanden.

Medewerker

Het naleven van het privacybeleid en de diverse maatregelen omtrent persoonsgegevens, is een taak van alle medewerkers binnen de gemeente Aa en Hunze. Zo wordt van medewerkers verwacht dat zij datalekken melden bij de servicedesk. Medewerkers nemen kennis van de bewustwordingsacties en/of trainingen omtrent privacy. Bij vragen over privacy schakelt een medewerker de PSO in.

Functionaris Gegevensbescherming (FG)

De functionaris gegevensbescherming (FG) is de onafhankelijke toezichthouder van de gemeente Aa en Hunze. De FG ziet toe op de naleving van de AVG, de Wet Politiegegevens (WPG) en het privacybeleid van de gemeente Aa en Hunze. Dit doet hij door controles op bijvoorbeeld genomen beheersmaatregelen, uitgevoerde risicoanalyses en het verwerkingsregister. Daarnaast kan de FG gevraagd en ongevraagd adviseren over vraagstukken met betrekking tot persoonsgegevens. Ook treedt de FG coördinerend op bij datalekken. De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van privacywetgeving door de gemeente Aa en Hunze, onverminderd de opvattingen van landelijke toezichthouders. In het geval van gesignaleerde risico's heeft de FG de mogelijkheid om buiten de hiërarchische structuur om te escaleren.

Privacy- en Security Officer (PSO)

De PSO is het eerste aanspreekpunt voor privacy binnen de organisatie en adviseur voor het management. De PSO adviseert in beginsel over privacyvraagstukken en helpt bij het opstellen van beleid. Waar nodig schakelt de PSO met de FG. Daarnaast ondersteunt de PSO de lijn met het uitvoeren van risicoanalyses, het implementeren van privacy maatregelen, het afleggen van verantwoording over privacy en afhandeling van datalekken. De PSO is tevens de beheerder van het datalekkenregister en het verwerkingsregister. Verder organiseert de PSO bewustwordingscampagnes en voert hij de interne audits uit voor de Wet Politiegegevens.

5. Sturing en verantwoording

5.1 Sturing

Dit privacybeleid wordt op bestuurlijk niveau door het college van B&W vastgesteld en is van toepassing op alle bestuursorganen van de gemeente Aa en Hunze en de ambtelijke organisatie; dit voor zover de AVG of WPG op de betreffende verwerkingen van toepassing is.² Het aanvullende beleid voor de WPG is in bijlage 1 uitgewerkt. Er kan op basis van dit beleid aanvullende procedures geformuleerd worden als specifieke werkzaamheden bij een team dit vereisen. De toepassing van het beleid wordt periodiek getoetst.

Het college van B&W, het directieteam en de teamleiders (c.q. proceseigenaren) sturen op privacy op basis van de volgende uitgangspunten:

1. Het college van B&W stelt het privacybeleid vast;
2. Het college van B&W informeert de raad over de privacy beleidsvoering;
3. Het management voorziet in de noodzakelijke middelen voor de uitvoering van dit privacybeleid;
4. Het privacybeleid vormt samen met het informatiebeveiligingsbeleid het fundament onder een betrouwbare informatievoorziening.

5.2 Verantwoording

De verantwoordingsplicht uit de AVG en WPG brengt met zich mee dat de gemeente Aa en Hunze niet alleen de regels moet naleven, maar dit ook moet kunnen aantonen.³ Hiervoor gebruikt de gemeente Aa en Hunze wettelijk verplichte hulpmiddelen en daarop aansluitende werkwijzen. De volgende producten en werkwijzen helpen mee om aan de verantwoordingsplicht te kunnen voldoen:

Wettelijke (verplichte) hulpmiddelen

1. Het bijhouden van een verwerkingsregister;
2. Het uitvoeren van privacy impact assessments (PIA) voor gegevensverwerkingen met een hoog privacy risico;
3. Een overzicht van verwerkingen waar een PIA voor is uitgevoerd en de rapportages van deze PIA's;
4. Een actueel risicoregister;
5. Een actueel register van incidenten (o.a. in verband met persoonsgegevens);
6. Periodieke controles om de juiste werking van de genomen maatregelen te controleren
7. Jaarlijkse interne audit op WPG verwerkingen;

² Dit privacybeleid is niet van toepassing op Gemeenschappelijke Regelingen.

³ De **verantwoordingsplicht (accountability)** houdt in dat je als organisatie moet kunnen aantonen dat de verwerkingen van persoonsgegevens aan de regels van de AVG voldoen. In de AVG staat een aantal verplichte maatregelen waarmee je als organisatie aan de verantwoordingsplicht voldoet. Deze maatregelen zijn o.a. het bijhouden van een verwerkingsregister en het uitvoeren van privacy impact assessments (PIA).

Werkwijzen in Aa en Hunze

1. Wekelijks operationeel overleg tussen FG, CISO, PSO, incidentmanager, functioneel beheer en technisch beheer. Vanuit dit overleg worden nieuwe en openstaande risico's beheerst. Van dit overleg worden notulen gemaakt. Deze worden maandelijks besproken met de teamleider informatiemanagement. De concerncontroller en gemeentesecretaris ontvangen maandelijks een samenvatting van de notulen.
2. Kwartaalgesprekken van de concernmanager met de teamleider waar aspecten van de privacy beleidsvoering binnen een team worden besproken;
3. Kwartaalgesprekken van de FG en CISO met de gemeentesecretaris; hier worden de afgelopen drie maandverslagen besproken;
4. Periodieke overleggen op bestuurlijk niveau tussen de portefeuillehouder in het college en de FG en CISO;
5. Het college van B&W legt jaarlijks – in de paragraaf bedrijfsvoering van de jaarstukken – verantwoording af aan de raad over het voldoen aan de AVG door de gemeente Aa en Hunze. Op deze manier wordt aangesloten bij de bestaande planning en control cyclus.

Naast bovenstaande maatregelen kunnen er extra maatregelen worden genomen waarmee de gemeente Aa en Hunze kan aantonen dat aan de eisen van de AVG wordt voldaan.

6. Overige elementen Algemene Verordening Gegevensbescherming

6.1 Rechten van betrokkenen

Onder de Algemene verordening gegevensbescherming (AVG) hebben mensen meer mogelijkheden gekregen om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt.

6.1.1 Uitoefening van rechten

Om gebruik te maken van hun rechten kunnen betrokkenen een verzoek indienen. Zie voor een uitwerking van deze rechten artikel 15 e.v. van de AVG. Het verzoek kan zowel schriftelijk als via de website van de gemeente Aa en Hunze ingediend worden. Binnen één maand beoordeelt de gemeente Aa en Hunze of het verzoek gerechtvaardigd is. De gemeente Aa en Hunze laat binnen die termijn weten wat er met het verzoek gaat gebeuren. De gemeente Aa en Hunze mag de behandeling van een verzoek met twee maanden verlengen (o.a. vanwege de complexiteit van een verzoek). De gemeente Aa en Hunze behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure.

Als het verzoek niet op tijd wordt opgevolgd, deelt de gemeente Aa en Hunze uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven. Iedere betrokkene heeft de mogelijkheid om bij de gemeente Aa en Hunze een klacht in te dienen of bezwaar te maken of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

6.2 Beveiligingsmaatregelen

De (technische, procesmatige, communicatie en organisatorische) maatregelen omvatten bij de verwerking van persoonsgegevens een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden etc. Tevens wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen.

Wanneer de gemeente Aa en Hunze persoonsgegevens verwerkt of laat verwerken door een derde, zorgt de gemeente Aa en Hunze ervoor dat passende beveiligingsmaatregelen (conform het informatiebeveiligingsbeleid) worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's. De maatregelen zoals deze zijn genoemd in de Baseline Informatieveiligheid Overheid (BIO) worden geacht pAa en Hunzed te zijn.

6.3 Verwerkers en verwerkersovereenkomsten

6.3.1 Inschakeling van een verwerker

Wanneer de gemeente Aa en Hunze een partij inschakelt om ten behoeve van de gemeente Aa en Hunze persoonsgegevens te verwerken en het verwerken van de persoonsgegevens

de primaire taak is van deze partij, kan deze partij worden beschouwd als verwerker. De gemeente Aa en Hunze schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst en worden voordat de dienstverlening aanvangt en daarna periodiek getoetst.

De gemeente Aa en Hunze hanteert een standaardformat voor het opstellen van een verwerkersovereenkomst, met daarin de vereisten waar een verwerkersovereenkomst minimaal aan moet voldoen.

6.3.2 Gemeente Aa en Hunze als verwerker

In voorkomende gevallen treedt de gemeente Aa en Hunze op als verwerker voor derden. Hierbij zijn deze derden de verwerkingsverantwoordelijke. De gemeente Aa en Hunze streeft er in deze gevallen naar voor deze verwerkingen heldere en eenduidige voorwaarden op te stellen voor gelijksoortige verwerkingen. De gemeente Aa en Hunze biedt daarbij aan de verwerkingsverantwoordelijke voldoende garanties voor het zorgvuldig verwerken van gegevens door het toepassen van passende technische en organisatorische maatregelen. De afspraken omtrent de verwerking worden schriftelijk vastgelegd in een verwerkersovereenkomst, voordat de dienstverlening door de gemeente Aa en Hunze aanvangt.

7. Evaluatie en wijziging van het beleid

Dit privacybeleid treedt in werking na vaststelling door het college van B&W. Dit beleid wordt periodiek door de FG geëvalueerd en indien nodig herzien. Hierbij wordt onder andere gekeken naar de doeltreffendheid van het beleid.

Bijlage 1: Privacybeleid Wpg gemeente Aa en Hunze

De gemeente Aa en Hunze is als werkgever van boa's verwerkingsverantwoordelijke in de zin van de Wpg en hanteert het volgende beleid bij de verwerking van persoonsgegevens die onder de Wet Politiegegevens valt.

Algemeen beleid

1. De gemeente Aa en Hunze hanteert als raamwerk voor beheersmaatregelen (Control Framework) het door Wpg-auditors gehanteerde raamwerk, zoals dat is opgenomen in bijlage 3 en 4 van de NOREA handreiking privacy audit Wpg voor boa's.
2. Wanneer gebruik gemaakt wordt van een informatiesysteem dat wordt beheerd door een leverancier (bijvoorbeeld SaaS), dan wordt met de leverancier een verwerkersovereenkomst afgesloten en dient deze een Third Party Memorandum (TPM) conform de NOREA handreiking privacy audit Wpg voor boa's.
3. De gemeente Aa en Hunze voert voor elke verwerking van politiegegevens een DPIA uit. Daarin worden de volgende principes getoetst en geborgd:
 - a. gegevensbescherming door beveiliging en ontwerp;
 - b. gegevensbescherming door standaard-instellingen.
4. De organisatie verwerkt politiegegevens in domein III Onderwijs, op basis van artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en op basis van de artikelen over ter beschikking stellen en verstrekking van politiegegevens (art. 15-21 en 23-24 Wpg).
5. De organisatie verwerkt *geen* gegevens op basis van
 - a. art. 9 Wpg (onderzoek in een bepaald geval). Wel verlenen Boa's medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten;
 - b. art. 11 Wpg (geautomatiseerd vergelijken en in combinatie zoeken voor een art. 9 onderzoek);
 - c. art. 13 Wpg (ondersteunende taken);
 - d. art. 17a Wpg (doorgifte aan derde landen, d.w.z. landen buiten de Europese Economische Ruimte);
 - e. art. 7a Wpg (geautomatiseerde besluitvorming).
6. Toegangsbeveiliging is zodanig ingericht dat alleen Boa's en geautoriseerden toegang hebben tot politiegegevens.
7. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.
8. Betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en -indien van toepassing- bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

Rollen, taken en bevoegdheden

1. De **Privacy en Security Officer** inventariseert jaarlijks of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden dit beleid en het verwerkingenregister indien nodig aangepast. De interne en externe Wpg-audits worden daarnaast door de Privacy en Security Officer(s) gecoördineerd.
2. De **Teamleider** van het team met daarin Boa's is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken:
 - a. het onder de aandacht brengen van de handreiking/gedragsregels voor Boa's bij de medewerkers en het toezien op deze gedragsregels;
 - b. het bijhouden van een overzicht met geautoriseerden;
 - c. actueel houden van het verwerkingenregister t.a.v. verwerkingen in het team;
 - d. bijhouden van een lijst met veel voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking;
 - e. zorgen dat art. 8 gegevens;
 - i. na 1 jaar alleen nog beschikbaar zijn voor gericht zoeken;
 - ii. na 5 jaar worden verwijderd, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures;
 - iii. na 10 jaar worden vernietigd.
3. De **Teamleider** van het team met daarin Boa's heeft de volgende bevoegdheden
 - a. het nemen van autorisatiebesluiten in de zin van art 6 lid 3, 4 en 5 Wpg, met behulp van het formulier "Autorisatie verwerking politiegegevens";
 - b. het besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix voor het informatiesysteem waarin politiegegevens worden verwerkt.
4. De **Functioneel Beheerder** bewaakt beveiliging van de applicatie, onder andere door logbestanden te analyseren.
5. De **Functionaris Gegevensbescherming**:
 - a. adviseert en informeert over de Wpg, onder andere over DPIA's;
 - b. houdt toezicht op de uitvoering van de Wpg;
 - c. werkt samen met de AP en is contactpunt voor de AP;
 - d. stelt jaarlijks een verslag op met bevindingen;
 - e. voert de volgende controles uit:
 - i. steekproefsgewijze beoordeling van Processen Verbaal, ten minste jaarlijks, op de volgende criteria:
 - werken conform de gedragsregels;
 - adequaat hanteren van doelbinding;
 - noodzakelijkheid, rechtmatigheid, juiste en volledige verwerking van politiegegevens;

- vastlegging van de herkomst en wijze van verkrijging;
 - alleen verwerken van bijzondere politiegegevens wanneer dit onvermijdelijk is;
 - onderscheiding tussen feitelijke en subjectieve gegevens, c.q. feiten en persoonlijke oordelen;
 - onderscheiden tussen verschillende categorieën van betrokkenen, zoals verdachten, slachtoffers, getuigen en veroordeelden;
 - vastlegging en rechtmatigheid van ter beschikkingstellingen en verstrekkingen.
- ii. controle van correcte en tijdige uitvoering en documentatie, o.a. van de reden van afwijzing, van verzoeken van betrokkenen, zoals vernietiging en rectificatie van politiegegevens;
 - iii. controle van correcte en tijdige opvolging van datalekken, zoals documentatie, analyse en meldingen aan AP en betrokkenen;
 - iv. controle van toewijzing van autorisaties;
 - v. controle van bewustmaking en opleiding van boa's en andere geautoriseerden;
 - vi. controle van uitvoering van de audits en opvolging van de bevindingen;
 - vii. toetsen van tijdige uitvoering en/of actualisering van DPIA;
 - viii. toetsen van het testen en evalueren van de doeltreffendheid van de beheersmaatregelen, bijvoorbeeld n.a.v. de DPIA;
 - ix. controle van volledigheid en juistheid van het verwerkingsregister voor zover het Wpg verwerkingen betreft.

Specifiek beleid ten aanzien van het cluster veiligheid (Domein I: Openbare ruimte)

De organisatie gebruikt alleen bestuursrechtelijke middelen voor toezicht en handhaving. Daarom zijn binnen dit taakveld geen boa's aangesteld en is de Wpg niet van toepassing.

Specifiek beleid ten aanzien politiegegevens bij de uitvoering van de leerplichtwet (Domein III: Onderwijs)

De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving van de leerplichtwet, in het bijzonder art 16 lid 5 en art 26 LPW. Daarom zijn binnen dit taakveld boa's aangesteld en is de Wpg van toepassing.

**Specifiek beleid ten aanzien politiegegevens bij de uitvoering van de Participatiewet
(Domein V: Werk, Inkomen en Zorg)**

De organisatie heeft de taken m.b.t. de Participatiewet gedelegeerd aan het Werkplein Drentsche Aa. Binnen dit taakveld zijn bij de gemeente geen boa's aangesteld. De gemeente is niet verantwoordelijk voor deze Wpg verwerkingen.