

Algemeen Privacybeleid

Gemeente Smallerland

Inhoudsopgave

1.	Inleiding	3
1.1	Privacy aanpak.....	3
1.2	Bereik.....	4
1.3	Wettelijk kader voor het omgaan met persoonsgegevens	4
1.3.1	Algemene Verordening Gegevensbescherming	4
1.3.2	Wet Politiegegevens.....	4
2.	Uitgangspunten en kaders AVG en Wpg	6
2.1	Rechtmatigheid, behoorlijkheid en transparantie	6
2.2	Grondslag en doelbinding	6
2.3	Dataminimalisatie.....	6
2.4	Bewaartermijn.....	7
2.5	Integriteit en vertrouwelijkheid	7
2.6	Delen met derden.....	7
2.7	Subsidiariteit en proportionaliteit.....	7
2.8	Rechten van betrokkenen	7
2.9	Persoonsgegevens.....	9
3.	Privacy Governance	9
3.1	Bestuursorganen	9
3.2	Directieteam.....	10
3.3	Teammanager.....	10
3.4	Privacybeheerder	11
3.5	Privacy-coördinator	11
3.6	Chief Information Security Officer (CISO).....	11
3.7	Functionaris Gegevensbescherming (FG).....	11
4.	Inbedding in de organisatie	12
4.1	Verwerkingenregister.....	12
4.1.1	Verwerkersovereenkomst	13
4.2	Meldplicht datalekken.....	13
4.3	Data Protection Impact Assessment (DPIA)	14
5.	Beleid tav een aantal specifieke verwerkingen	14
5.1	Profilering (Art. 22 AVG) en tracking.....	14
5.2	Cameratoezicht	15
5.3	Bodycams toezichthouders en boa's.....	15

1. Inleiding

Op 25 mei 2018 is de Wet Bescherming Persoonsgegevens (Wbp) vervangen door de Algemene Verordening Gegevensbescherming (AVG) en –voor de boa’s- de Wet Politiegegevens (Wpg). Dit privacybeleid is het kader voor passende technische en organisatorische maatregelen om persoonsgegevens die de gemeente Smallerland verwerkt te beschermen en te waarborgen, zodat de gemeente voldoet aan relevante wet- en regelgeving. Gemeente Smallerland streeft ernaar om aantoonbaar in control te zijn en daarover op professionele wijze verantwoording af te leggen. Dit houdt in dat wij als gemeente weten welke maatregelen genomen zijn en welke niet.

Het privacybeleid wordt ten minste elke drie jaren herzien (Art. 24.1 AVG) op basis van:

- Een evaluatie van het beleid;
- Trends en veranderingen in de omgeving, zoals wet- en regelgeving;
- Bedrijfsstrategie en -doelstellingen;
- Documentatie van de jaarlijkse verbetercycli (zie boven);
- Terugkoppeling van belanghebbende partijen, bijvoorbeeld opdrachtgevers, cliëntenraden en ondernemingsraden;
- Onafhankelijke beoordelingen;
- Aanbevelingen van relevante instanties, zoals toezichthouders (bijvoorbeeld Autoriteit Persoonsgegevens (AP)) en brancheorganisaties.

1.1 Privacy aanpak

De gemeente Smallerland hecht waarde aan uw privacy bij het uitvoeren van haar werkzaamheden. Inwoners hebben er recht op dat wij zorgvuldig en vertrouwelijk met uw persoonsgegevens omgaan. De reden om de uitgangspunten van het privacybeleid vast te stellen is om de aanpak van privacy te vast te leggen, zodat de privacy wordt gewaarborgd en verantwoording afgelegd kan worden. Dat is ook belangrijk omdat privacy een maatschappelijk relevant onderwerp is.

De gemeente Smallerland wil de privacy waarborgen door een Privacy Management Systeem (PMS) met jaarlijkse verbetercycli toe te passen, zoals deze ook worden toegepast in het kwaliteitsmanagement, bekend als Plan-Do-Check-Act cyclus.

Deze wordt toegepast door jaarlijks:

- Plan: Een actieplan op te stellen, rekening houdend met de bedrijfsstrategie en doelstellingen, risico's, regelgeving, de stand van de techniek en beschikbare middelen (Art. 5.2 AVG)

Het plan wordt opgesteld op basis van:

- evaluatie van de uitvoering en resultaten van het vorige actieplan;
- risicoanalyse ten aanzien van privacy;
- evaluatie van de uitvoering en controle van beheersingsmaatregelen;
- informatiebeveiligingsincidenten en datalekken;
- trends ten aanzien van bedreigingen, kwetsbaarheden en technologische mogelijkheden;
- het privacybeleid en evaluatie van de naleving daarvan;
- strategie en doelstellingen van de organisatie.

- Do: Het actieplan uit te voeren waarin herhaalde acties zoals rond bewustwording en controle van beheersmaatregelen worden uitgevoerd en beheersmaatregelen worden ingevoerd en/of verbeterd om zo het PMS stapsgewijs vorm te geven;
- Check: De uitvoering van de actieplannen en ingevoerde beheersingsmaatregelen te bewaken, de resultaten te evalueren (Art. 24.1 AVG);
- Act: Bij te sturen, her prioriteren en/of aanvullende maatregelen te nemen of aanbevelingen te doen voor het volgende actieplan (Art. 24.1 AVG).

Binnen de gemeente Smallingerland wordt veel gewerkt met persoonsgegevens van inwoners en bedrijven, medewerkers en samenwerkingspartners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. Om het vertrouwen van de burger te kunnen waarborgen, moet de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaan.

Het college van Burgemeester en Wethouders (College van B&W) en het Management spelen een cruciale rol bij het waarborgen van privacy. De gemeente Smallingerland geeft door dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft.

1.2 Bereik

Het privacybeleid is van toepassing op alle persoonsgegevens die de gemeente verwerkt en geldt daarmee ook voor alle medewerkers van de gemeente die met persoonsgegevens werken.

1.3 Wettelijk kader voor het omgaan met persoonsgegevens

De gemeente Smallingerland is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het privacybeleid. Hiervoor geldt de rechtstreeks werkende Europese verordening, namelijk de AVG. Daarnaast zijn er nog andere wetten die regels bevatten voor het omgaan met persoonsgegevens zoals de Uitvoeringswet (UAVG), Wet basisregistratie personen (Wbrp) en de Wet Politiegegevens (Wpg). Ook voor deze wetten gelden dezelfde uitgangspunten.

1.3.1 Algemene Verordening Gegevensbescherming

Vanuit de Europese verordening 2016/679 heeft de AVG ruimte gelaten voor nationale keuzes, resulterende in de UAVG. De UAVG regelt bijvoorbeeld de instelling en inrichting van de AP dat dient als nationale toezichthouder en heeft de bevoegdheid om bestuurlijke boetes op te leggen. Vanuit de AVG heeft de gemeente een aantal verplichten, bijvoorbeeld:

- Het aanwijzen van een Functionaris Gegevensbescherming (FG);
- Het uitvoeren van een Data Protection Impact Assessment (DPIA), ook wel een gegevensbeschermingseffectbeoordeling genoemd, en;
- Het verantwoorden van de verwerkingen binnen de gemeente.

Om aan het verantwoordingsplicht te voldoen, moet de gemeente Smallingerland een verwerkingenregister, een privacybeleid en datalekregister opstellen.

1.3.2 Wet Politiegegevens

De verwerkingen die uitgevoerd worden door de buitengewoon opsporingsambtenaren (boa's), zoals de boa's op straat, en de leerplichtambtenaren vallen voor hun strafrechtelijke taken niet onder de AVG maar onder de Wet Politiegegevens (Wpg). De AVG is van toepassing indien de medewerker zich bezighoudt met toezichttaken en de Wpg is van toepassing indien gegevens verwerkt worden

door de opsporingstaak. De Wpg beoogt de inbreuk op de persoonlijke levenssfeer in het kader van het verwerken van politiegegevens te verkleinen door het stellen van concrete verplichtingen.

De Wpg is gebaseerd op de Europese Richtlijn (2016/680) en is verder uitgewerkt in een Besluit Politiegegevens en een Besluit Politiegegevens Boa's. De gemeente Smallingerland hanteert als raamwerk voor beheersmaatregelen (Control Framework) het door Wpg-auditoren gehanteerde raamwerk, zoals opgenomen in bijlage 3 en 4 van de NOREA handreiking privacy audit Wpg voor boa's. 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 periodiek een Third Party Memorandum (TPM) te overleggen aansluitend op de NOREA handreiking privacy audit Wpg voor boa's.

De gemeente Smallingerland verwerkt politiegegevens op basis van Artikel 8 van de Wpg (uitvoering van de dagelijkse politietaak) en op basis van de artikelen over te beschikking stellen en verstrekking van politiegegevens (Artikel 15-21 en 23-24). De gemeente verwerkt politiegegevens verder in het kader van Artikel 13 Wpg (ondersteunende taken), voor zover die gegevens onder verantwoordelijkheid van instanties worden verwerkt.

De gemeente Smallingerland verwerkt *geen* gegevens op basis van:

- Artikel 9 Wpg (onderzoek in een bepaald geval). Wel verlenen boa's in domein V medewerking aan onderzoeken onder verantwoordelijkheid van de politie of andere opsporingsdiensten;
- Artikel 11 Wpg (geautomatiseerd vergelijken en in combinatie zoeken voor een Artikel 9 onderzoek);
- Artikel 17a Wpg (doorgifte aan derde landen, dat wil zeggen landen buiten de Europese Economische Ruimte (EER)).

De gemeente maakt geen gebruik van geautomatiseerde besluitvorming, waaronder profilering als bedoeld in de Wpg Art. 7a.

De toegangsbeveiliging is zodanig ingericht dat alleen Boa's en geautoriseerde toegang hebben tot politiegegevens. Bij de verzending van politiegegevens worden deze altijd versleuteld verstuurd.

De gemeente Smallingerland past de Wpg toe in de volgende domeinen:

- Domein I: Openbare Ruimte
 - De gemeente gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving in de openbare ruimte. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.
- Domein II: Milieu, Welzijn en Infrastructuur
 - De organisatie gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.
- Domein III: Onderwijs
 - De gemeente gebruikt naast bestuursrechtelijke middelen ook strafrechtelijke instrumenten voor toezicht en handhaving van de leerplichtwet, in het bijzonder Art.

16 lid 5 en Art. 26. Daarom zijn binnen dit taakveld Boa's aangesteld en is de Wpg van toepassing.

De interne en externe audits die voor de Wpg verplicht zijn, worden gecoördineerd door de privacycoördinator in team Concern. De gemeente Smallingerland is verplicht om jaarlijks een interne audit en iedere 4 jaar een externe audit te laten uitvoeren en de resultaten van de externe audit te delen met de AP. De betrokkenen worden geïnformeerd over de verwerking van politiegegevens via de website en bij de eerste brief die zij ontvangen over strafrechtelijke handhaving.

2. Uitgangspunten en kaders AVG en Wpg

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

2.1 Rechtmatigheid, behoorlijkheid en transparantie

Wanneer de gemeente met persoonsgegevens werkt moeten de persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Rechtmatigheid houdt in dat de gemeente haar verwerkingen moet kunnen baseren op één van de grondslagen uit de AVG of de Wpg. Behoorlijkheid betekent dat de verwerking op de juiste manier moet plaatsvinden en dat de betrokkene niet misleid mag worden. Transparantie geeft aan dat de betrokkene op de hoogte moet zijn van de verwerking en begrijpt welke persoonsgegevens worden verwerkt om wat voor redenen.

2.2 Grondslag en doelbinding

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt en niet voor andere doelen worden gebruikt, dan waarvoor ze zijn verzameld. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt. De AVG kent zes grondslagen:

- De gemeente heeft **toestemming** van de persoon om wie het gaat om de persoonsgegevens te verwerken;
- Het is noodzakelijk om gegevens te verwerken om **een overeenkomst uit te voeren**;
- Het is noodzakelijk om gegevens te verwerken omdat de gemeente dit **wettelijk verplicht** is;
- Het is noodzakelijk om gegevens te verwerken om **vitale belangen te beschermen**;
- Het is noodzakelijk om gegevens te verwerken om een gemeentelijke taak van **algemeen belang of openbaar gezag** uit te oefenen;
- Het is noodzakelijk om gegevens te verwerken om het **gerechtvaardigde belang** te behartigen.

Op grond van de Wpg worden politiegegevens met het oog op de uitvoering van de dagelijkse politietaken verwerkt.

2.3 Dataminimalisatie

Met dataminimalisatie wordt bedoeld dat de gemeente alleen persoonsgegevens mag verwerken die minimaal noodzakelijk zijn voor het vooraf bepaalde doel.

2.4 Bewaartermijn

De AVG bevat geen specifieke bewaartermijnen voor persoonsgegevens, maar stelt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is. Het hangt dus af in een situatie noodzakelijk wordt gevonden. In bepaalde wetgeving, zoals de belastingwetgeving worden er wel concrete bewaartermijnen vermeld.

Indien van toepassing is de gemeente verplicht om zich te houden aan de bewaartermijnen die vermeld staan in de specifieke wetgeving. Als er geen sprake is van een concrete bewaartermijn in wetgeving, kan de gemeente deze baseren op selectielijsten. De Vereniging Nederlandse Gemeenten (VNG) heeft een Selectielijst opgesteld om de bewaartermijnen vast te stellen. De actuele selectielijst is de Selectielijst gemeenten en intergemeentelijke organen 2020.

Bewaartermijnen kunnen variëren van een paar jaar tot een paar weken. Wanneer de bewaartermijn is verlopen, is de gemeente verplicht om de gegevens te vernietigen. Echter is een klein deel van de overheidsinformatie belangrijk genoeg om blijvend te bewaren, daartoe is de gemeente verplicht op basis van de Archiefwet. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Met betrekking tot het bewaren van gegevens kent de Archiefwet geen algemene bewaartermijn voor archiefbestanden. Ook hier zijn de selectielijsten leidend.

2.5 Integriteit en vertrouwelijkheid

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze waar nodig vertrouwelijk. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

2.6 Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van het delen van persoonsgegevens, gebeurt dit alleen wanneer daarvoor een grondslag is en maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen.

2.7 Subsidiariteit en proportionaliteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt. Dit wordt bedoeld met subsidiariteit. Proportionaliteit houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot en met de verwerking te dienen doel.

2.8 Rechten van betrokkenen

De AVG geeft inwoners verschillende rechten op het gebied van privacy. De inwoners van de gemeente Smallerland kunnen beroep doen op een aantal rechten wanneer er sprake is van een verwerking met persoonsgegevens. De rechten van de betrokkenen zijn:

- **Recht op duidelijke informatie:** de inwoner heeft het recht om aan de gemeente te vragen of van de betrokkene persoonsgegevens worden verwerkt.
- **Recht op inzage:** de inwoner heeft de mogelijkheid om te controleren of, en op welke manier gegevens worden verwerkt.
- **Recht op correctie:** Als duidelijk wordt dat persoonsgegevens niet kloppen, kan de inwoner een verzoek indienen bij de gemeente om dit te corrigeren.
- **Recht op beperking van de verwerking:** de inwoner heeft het recht aan de gemeente te vragen om minder persoonsgegevens te laten verwerken.

- **Recht om vergeten te worden:** In gevallen waar de inwoner toestemming heeft gegeven om gegevens te verwerken, heeft de inwoner het recht om de persoonsgegevens op verzoek te laten verwijderen.
- **Recht op bezwaar:** de inwoner heeft het recht om bezwaar te maken tegen de verwerking van uw persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking die zwaarder wegen.

Onder de Wpg zijn de rechten van de inwoners anders dan die onder de AVG. Daarvoor kan de inwoner schriftelijk of online een aanvraag indienen. De rechten onder de Wpg zijn:

- **Recht op inzage**
- **Recht op correctie**
- **Recht op vernietiging**

De gemeente heeft het recht om een Wpg-verzoek af te wijzen, onder andere als:

- Het verzoek gerechtelijke onderzoeken of procedures zou belemmeren;
- Het nadelige gevolgen heeft voor het voorkomen van het begaan van strafbare feiten, voor opsporing, onderzoek, vervolging of het opleggen van straffen;
- Dit de rechten en vrijheden van derden zou schaden;
- De gemeente de wettelijke plicht heeft deze politiegegevens te bewaren;
- Het kennelijk een ongegrond of buitensporig verzoek is.

Wanneer een verzoek schriftelijk is ingediend moet de aanvrager zich legitimeren met een geldig identiteitsbewijs. Er zijn twee manieren aanwezig om u te legitimeren. De eerste manier is om fysiek langs het gemeentehuis te komen en daar uw identiteitsbewijs te tonen onder vermelding van het zaaknummer die is gegeven voor uw verzoek. De tweede manier is om een kopie van uw identiteitsbewijs te sturen via mail of post. Hiervoor raadt de gemeente aan om gebruik te maken van de KopieID app van de Rijksoverheid waar uw pasfoto, BSN, en MRZ code kunt doorstrepen. Wij vragen aan iedereen om zich te legitimeren voordat wij een verzoek in behandeling nemen conform Artikel 12 lid 2 en lid 6 AVG en Artikel 25-28 Wpg.

In het verzoek moet helder worden aangegeven wat het verzoek inhoudt. In het kader van de AVG moet de verwerkingsverantwoordelijke binnen één maand na ontvangst het verzoek beoordelen. Indien het een complex geval is kan het beantwoordingstermijn met twee maanden worden verlengd wat wordt bericht bij de betrokkene.

In het kader van de Wpg kan moet de verwerkingsverantwoordelijke binnen zes weken antwoorden op een verzoek tot inzage, binnen vier weken op een verzoek tot rectificatie of vernietiging. Deze termijn kan bij verzoeken tot inzage nog vier weken worden verlengd.

Als er een verzoek wordt ingediend en deze geaccepteerd is, wordt er bij een AVG verzoek een overzicht gegeven met onder andere:

- De verwerkingsdoeleinden;
- De betrokken categorieën van persoonsgegevens;
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- Bewaartermijnen;
- Rechten van betrokkenen;
- Indien van toepassing, het bestaan van geautomatiseerde besluitvorming.

Bij een Wpg verzoek ontvangt de betrokkene een overzicht met onder andere:

- De doelen en de rechtsgrond van de verwerking;
- De betrokken categorieën van persoonsgegevens;
- De vraag of deze persoon betreffende politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en over de ontvangers of categorieën van ontvangers aan wie de gegevens zijn verstrekt, met name ontvangers in derde landen of internationale organisaties;
- Bewaartermijnen;
- Rechten van betrokkenen;
- Herkomst van gegevens.

2.9 Persoonsgegevens

Een persoonsgegeven is informatie die direct over iemand gaat of informatie die naar deze persoon te herleiden is. Onder de AVG wordt er een onderscheid gemaakt tussen persoonsgegevens en bijzondere persoonsgegevens. Onder persoonsgegevens vallen bijvoorbeeld, de naam, het adres en het e-mailadres. Bijzondere persoonsgegevens zijn extra gevoelige gegevens, omdat de verwerking ervan impact kan hebben op de persoon. De AVG en de Wpg zien de volgende persoonsgegevens als bijzondere persoonsgegevens (Art. 9 AVG en Art. 5 Wpg):

- Ras of etnische afkomst;
- Politieke opvattingen;
- Religieuze of levensbeschouwelijke overtuiging;
- lidmaatschap van een vakbond;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon;
- Gegevens over gezondheid;
- Gegevens over seksueel gedrag of seksuele gerichtheid.

Onder de AVG is de verwerking van deze gegevens verboden, tenzij een uitzondering van kracht is.

Onder de Wpg mogen bijzondere politiegegevens alleen worden verwerkt als dat onvermijdelijk is.

3. Privacy Governance

De gemeente Smallerland heeft op verschillende plaatsen in de organisatie verantwoordelijkheden voor de bescherming van persoonsgegevens. De verschillende verantwoordelijkheden, rollen en hun plek in de organisatie worden als volgt beschreven.

3.1 Bestuursorganen

De bestuursorganen van de gemeente Smallerland zijn de 'verantwoordelijke' in de zin van de AVG. Zij zijn verantwoordelijk voor alles wat te maken heeft met de bescherming van persoonsgegevens binnen de gemeente.

De gemeente Smallerland kent:

- Gemeenteraad
- Burgemeester
- Het College van B&W

De gemeenteraad stelt de kaders ten aanzien van privacybescherming op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het College van B&W is grotendeels verwerkingsverantwoordelijke binnen de gemeente.

De gemeente is als publiekrechtelijke rechtspersoon verwerkingsverantwoordelijke voor de verwerking van politiegegevens omdat zij de werkgever is van de Boa's (Bpg Boa Art. 1).

3.2 Directieteam

Het directieteam bestaat uit de gemeentesecretaris/algemeen directeur en concurndirecteur. De uitvoerende verantwoordelijkheid voor privacybescherming ligt bij het directieteam in het mandaat van de Gemeenteraad, de Burgemeester het College. Deze stelt met het managementteam het gewenste niveau van informatieveiligheid en privacy vast voor de gemeente. Daarnaast is het directieteam verantwoordelijk voor de juiste en volledige implementatie van de privacywet- en regelgeving en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan voor wat betreft de wijzigingen.

3.3 Teammanager

De teammanager is verantwoordelijk voor de integriteit (juistheid, tijdigheid en volledigheid), de vertrouwelijkheid (waardoor de persoonsverwerking uitsluitend toegankelijk is voor daartoe geautoriseerde personen) en beschikbaarheid (het bereikbaar en inzichtelijk zijn) van de betreffende persoonsverwerkingen van het betreffende organisatieonderdeel. Een deel van het uitvoeren van deze verantwoordelijkheden kan de teammanager beleggen bij een privacybeheerder.

Voorbeelden van taken van een teammanager met betrekking tot de AVG zijn: het implementeren van het beleid ten aanzien van de betreffende persoonsgegevens die onder zijn verantwoordelijkheid vallen; het belang van privacy procedures onder de aandacht brengen; het afsluiten, beheren en actualiseren van verwerkersovereenkomsten; en het uitvoeren van verzoeken om inzage, correctie en verzetten ten aanzien van persoonsgegevens.

Aangaande de Wpg is de teammanager van het team met daarin Boa's, leerplichtambtenaren en sociale rechercheurs ook verantwoordelijk voor de implementatie van de Wpg. De teammanager met daarin boa's is verantwoordelijk voor de implementatie en uitvoering van de Wpg en heeft in dat kader onder andere de volgende taken:

- Het onder de aandacht brengen van de handreiking/gedragsregels voor boa's bij de medewerkers en het toezien op deze gedragsregels;
- Het bijhouden van een overzicht met geautoriseerde;
- Actueel houden van het verwerkingenregister t.a.v. verwerkingen in het team;
- Bijhouden van een lijst met veel voorkomende verstrekkingen met daarbij de onderbouwing van de grondslag voor de verstrekking;
- Zorgen dat Art. 8 Wpg gegevens
 - Na 1 jaar alleen nog beschikbaar zijn voor gericht zoeken;
 - Na 5 jaar worden verwijderd, dat wil zeggen alleen beschikbaar zijn voor audits en klachtenprocedures;
 - Na 10 jaar worden vernietigd.

De teammanager van het team met daarin boa's heeft de volgende bevoegdheden:

- Het nemen van autorisatiebesluiten in de zin van Art. 6 lid 3, 4, 5 Wpg met behulp van het formulier “Autorisatie verwerking politiegegevens”;
- Het besluiten over toegang tot informatiesystemen met politiegegevens, waaronder het vaststellen van de autorisatiematrix voor het informatiesysteem waarin politiegegevens worden verwerkt.

3.4 Privacybeheerder

De teammanager wijst in elk team een privacybeheerder aan. De privacybeheerder is gericht op de uitvoering en de naleving van de privacywetgeving binnen de diverse teams. De privacybeheerder adviseert en voert activiteiten uit ter bescherming van persoonsgegevens. De taken die vallen onder de privacybeheerder kunnen belegd worden door de teammanager.

3.5 Privacy-coördinator

De rol van de privacy-coördinator heeft een overkoepelend karakter en richt zich op twee taken, deels uitvoerend en deels ondersteunend met betrekking tot de privacy wetgeving. Voorbeelden van taken van een privacy-coördinator zijn: het onderhouden van het algemeen privacybeleid en privacy verklaring- en reglement; coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en hierover adviseren; en advisering en ondersteuning bij het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen.

Met betrekking tot de Wpg is de rol van de privacy-coördinator om jaarlijks te inventariseren of het bereik van de verwerkingen met politiegegevens is gewijzigd. Op basis daarvan worden dit beleid en het verwerkingenregister zo nodig aangepast.

3.6 Chief Information Security Officer (CISO)

De CISO heeft in de gemeente Smallingerland een adviserende, faciliterende en coördinerende rol en zorgt ervoor dat taken belegd zijn op het gebied van informatieveiligheid. De CISO is bijvoorbeeld verantwoordelijk voor: het actueel houden van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan; het adviseren van het college, het directieteam, het managementteam, de concerncontroller; en het coördineren van de uitvoering van informatie veiligheidsmaatregelen uit het uitvoeringsplan.

3.7 Functionaris Gegevensbescherming (FG)

De FG is de (wettelijke) interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving en is het centrale aanspreekpunt voor medewerkers, burgers en de Autoriteit Persoonsgegevens. Daarnaast rapporteert, adviseert en informeert de FG het management en het bestuur hierover. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Voorbeelden van taken van de FG zijn: advies verstrekken aangaande de gegevensbeschermingseffectbeoordeling (DPIA) en toezien op de uitvoering daarvan; optreden als contactpunt voor de AP; en de verwerkingsverantwoordelijke, de verwerker en de werknemers die verwerken informeren en adviseren over hun verplichtingen uit hoofde van de AVG.

Met betrekking tot de Wpg is de FG verantwoordelijk voor het adviseren en informeren over de Wpg; onder andere over de DPIA; houdt toezicht op de uitvoering van de Wpg; en stelt jaarlijks een verslag op met bevindingen.

De FG voert ook de volgende controles uit:

- 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 beschikking stellingen en verstrekkingen
- Toetsen van tijdige uitvoering en/of actualisering van DPIA;
- Toetsen van het testen en evalueren van de doeltreffendheid van de beheersmaatregelen, waaronder beveiligingsmaatregelen, bijvoorbeeld naar aanleiding van de DPIA;
- Controle van de toewijzing van autorisaties en de controle daarvan door de systeemeigenaar;
- Controle van de verwerkersovereenkomst op actualiteit en actuele bijbehorende certificaten en verklaringen;
- Controle van bewustmaking en opleiding van boa's en andere geautoriseerde;
- Controle van (nieuwe) arbeidsovereenkomsten, screening etc.
- Controle van de hantering van afschermings-, verwijderings- en vernietigingstermijnen;
- Controle van de rechtmatigheid van verstrekkingen;
- 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;
- Controle van correcte en tijdige opvolging van datalekken, zoals documentatie, analyse en meldingen aan AP en betrokkenen;
- Controle en uitvoering van de audits en opvolging van de bevindingen;
- Controle van volledigheid en juistheid van het verwerkingenregister voor zover het Wpg verwerkingen betreft;

4. Inbedding in de organisatie

Om de kwaliteit en het vertrouwen van de inwoners te waarborgen is de gemeente verplicht zich te kunnen verantwoorden met betrekking tot het verwerken van persoonsgegevens. Dit houdt in dat de gemeente een verwerkingenregister, een meldplicht van datalekken en deze bij te houden, het uitvoeren en coördineren van DPIA's, en het kunnen aantonen dat er op een rechtvaardige manier toestemming is gevraagd bij de betrokkene voor het verwerken van gegevens.

4.1 Verwerkingenregister

Het bijhouden van het verwerkingenregister is een verplichte maatregel onder de AVG. De gemeente Smallerland kent een transparante dienstverlening en houden daarom een AVG en Wpg register van de verwerkingsactiviteiten bij. Hierin wordt het volgende in het AVG register onder andere vastgelegd:

- Naam en contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de FG;
- Wat het doel is van de gegevensverwerking;
- Welke persoonsgegevens er worden verwerkt;
- Waar de persoonsgegevens zijn verkregen;
- Wie verantwoordelijk is voor de gegevensverwerking;
- Welke categorieën van betrokkenen aanwezig zijn bij de gegevensverwerking;
- Aan wie de persoonsgegevens eventueel worden verstrekt;
- Welke besluiten geautomatiseerd worden genomen;
- De bewaar- en vernietigingstermijnen;
- De getroffen beveiligingsmaatregelen.

In het Wpg register legt de gemeente onder andere het volgende vast:

- Naam en contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de FG;
- Wat het doel is van de verwerking;
- Een beschrijving van de categorieën van betrokkenen;
- De categorieën van persoonsgegevens;
- In voorkomend geval, gebruik van profilering;
- Aan wie de persoonsgegevens eventueel worden verstrekt;
- Welke grondslag geldt voor de verwerking;
- De bewaar- en vernietigingstermijnen;
- De getroffen beveiligingsmaatregelen;
- Toekenning van autorisaties.

4.1.1 Verwerkersovereenkomst

Wanneer een andere organisatie door de gemeente wordt ingeschakeld voor de verwerking van persoonsgegevens, moet er een verwerkersovereenkomst afgesloten worden. Bijvoorbeeld door het aanbieden van online applicaties door de leverancier (clouddienstverlening).

Met een verwerkersovereenkomst wordt afgesproken dat de andere partij de persoonsgegevens niet voor eigen doelen mag verwerken. Dus, het is alleen toegestaan om verwerkers in te schakelen als die voldoende garantie bieden dat zij aan de wettelijke vereisten voldoen.

4.2 Meldplicht datalekken

Ondanks alle toegepaste beveiligingen en zorgvuldigheid kan er zo nu en dan toch een datalek plaatsvinden. Er is sprake van een datalek als persoonsgegevens (per ongeluk) in verkeerde handen zijn gekomen, onbevoegd of onbedoeld zijn gewijzigd of verloren zijn gaan. Bijvoorbeeld als u een brief krijgt die niet voor u is bestemd. Om dit inzichtelijk te houden is de gemeente wettelijk verplicht om een datalekregister op te stellen. Als u een datalek tegenkomt, kunnen medewerkers en inwoners dit melden bij onze Functionaris Gegevensbescherming. Na de melding van een datalek onderzoeken wij de oorzaak van het datalek en proberen de gevolgen ervan te beperken. Als het nodig is, wordt een melding gedaan bij de Autoriteit Persoonsgegevens en/of de inwoner. De gemeente houdt een (intern) register bij waarin alle informatiebeveiligingsincidenten worden geregistreerd.

Om de schade van een datalek zoveel mogelijk te beperken onderneemt de gemeente vijf stappen:

1. Zorgen voor overzicht op de situatie;

2. Onmiddellijke maatregelen nemen om de schade van het datalek te beperken door de risico's in te schatten;
3. Bepalen of het datalek wel of niet gemeld moet worden aan de AP;
4. Bepalen of het datalek wel of niet gemeld moet worden aan de betrokken personen;
5. Registreren van het datalek in het datalekregister.

Door een datalekregister op te stellen en de datalekken te evalueren, leert de gemeente van de eerdere datalekken om toekomstige datalekken te verminderen.

4.3 Data Protection Impact Assessment (DPIA)

Een DPIA (gegevensbeschermingseffectbeoordeling) is een instrument om de privacy risico's van een gegevensverwerking in kaart te brengen. De AP raadt aan om één keer per 3 jaar een DPIA uit te voeren voor verwerkingen met een hoog risico. De Europese privacytoezichthouders hebben 9 criteria opgesteld om te beoordelen of de verwerking van persoonsgegevens een hoog privacy risico oplevert voor de betrokken personen.

De AP heeft ook een definitieve lijst vastgesteld van verwerkingen van persoonsgegevens waar een DPIA verplicht is. Deze lijst is afgestemd met andere privacytoezichthouders in de EU. Indien er sprake is van een verwerking met persoonsgegevens binnen de opgestelde lijst, dan is de gemeente verplicht om een DPIA uit te voeren. Dit zijn verwerkingen met betrekking tot: heimelijk onderzoek, zwarte lijsten, fraudebestrijding, creditscores, financiële situatie, genetische persoonsgegevens, gezondheidsgegevens, samenwerkingsverbanden, cameratoezicht, flexibel cameratoezicht, controle werknemers, locatiegegevens, communicatiegegevens, Internet of Things, profilering, observatie en beïnvloeding van gedrag, en biometrische gegevens.

Bij het uitvoeren van een DPIA worden onder andere de volgende principes getoetst en geborgd:

- Gegevensbescherming door beveiliging en ontwerp
- Gegevensbescherming door standaardinstellingen

5. Beleid tav een aantal specifieke verwerkingen

5.1 Profilering (Art. 22 AVG) en tracking

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie. Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.

Gemeente Smallerland maakt geen gebruik van profilering.

Door middel van tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. De verzamelde gegevens door tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens

gepseudonimiseerd of geanonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

Gemeente Smallingerland maakt geen gebruik van tracking.

5.2 Cameratoezicht

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet Art 151c. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat en gemeentelijke locaties. Camera's kunnen een grote inbreuk maken op de privacy van degene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's. Het gebruik van camera's door particulieren op de openbare weg is alleen mogelijk door toestemming van de burgemeester. Daarvoor wordt er een convenant afgesloten tussen de particulieren en de burgemeester waarin o.a. de grondslag, het doel, de maatregelen tegen verlies, en de bewaartermijn in opgenomen worden.

Gemeente Smallingerland maakt gebruik van cameratoezicht zoals beschreven in de Algemene Plaatselijke Verordening (APV) Smallingerland. In de APV staat dat de burgemeester kan besluiten tot plaatsing van vaste camera's voor een bepaalde duur ten behoeve van het toezicht op een openbare plaats. Wanneer de burgemeester gebruik maakt van bovenstaande bevoegdheid wordt dit gepubliceerd op de website van de gemeente en in de Breeduit. De openbare plaatsen die in de APV zijn aangewezen waar de burgemeester camera's kan laten plaatsen zijn parkeer- en bedrijfsterreinen, winkelcentra en busstations.

5.3 Bodycams toezichthouders en boa's

De gemeente Smallingerland maakt gebruik van bodycams bij toezichthouders en boa's. Dit wordt toegepast om de veiligheid van de werksferen van de boa's en toezichthouders te versterken. De bodycams worden ook gebruikt om agressie en (bijna) ongevallen te registreren om bij te dragen aan de-escalatie bij dreigende situatie gericht tegen toezichthouders en boa's.