gemeente Zaanstad
ZNSTD
GEMEENTEBLAD
Officiële uitgave van de gemeente Zaanstad
Nr. 291024
9 november
2020

Beleid Privacy Zaanstad

Inhoudsopgave

1 Inleiding

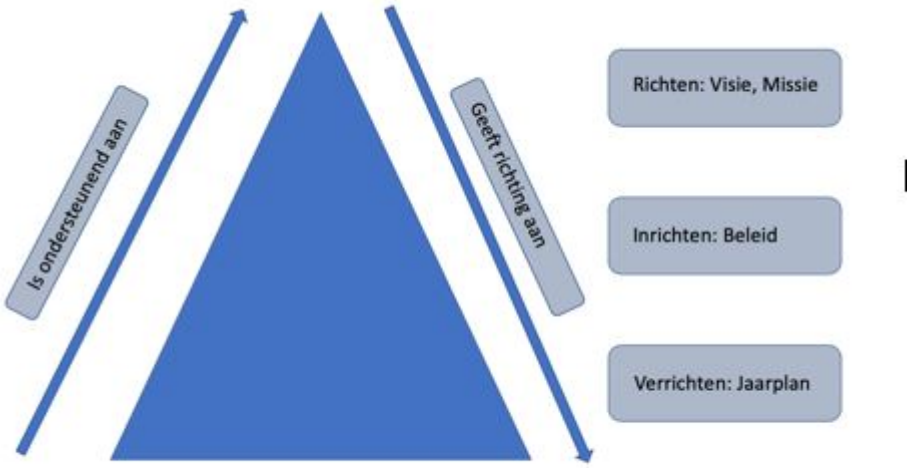
Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing. Deze verordening is de opvolger van de Wet bescherming persoonsgegevens. Deze wet was gebaseerd op de voorganger van de AVG, de Europese dataprotectierichtlijn (95/46/EG).

De AVG zorgt samen met de Uitvoeringswet AVG onder andere voor versterking en uitbreiding van de privacyrechten voor betrokkenen met meer verantwoordelijkheden voor organisaties die persoonsgegevens verwerken.

De AVG legt de verantwoordelijkheid bij ons als organisatie om aan te tonen dat wij aan de privacyregels voldoen. Door te voldoen aan de verantwoordingsplicht (accountability) leveren wij een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Visie Beleid Uitvoering

Het inrichtingsmodel voor de aanpak van Privacy in Zaanstad is gebaseerd op het model zoals in het onderstaande plaatje is weergegeven.



Figuur 1: Sturingsmodel Privacy

Het Waarom van Privacy wordt behandeld in het visie document voor de gemeente Zaanstad. De visie op Privacy geeft richting aan de manier waarop we met privacy en de bescherming daarvan willen omgaan. De visie ondersteunt gemeente Zaanstad bij het opstellen van beleidskaders. Deze kaders

zorgen ervoor dat we de uitvoering in lijn met de visie oppakken. De beleidskaders bieden ondersteuning bij het verrichten van de opdrachten, activiteiten en projecten en bij het toetsen van de uitvoering of conform deze kaders wordt gewerkt. Ook het Governance model, dat onder paragraaf 5.2 wordt behandeld, kent eenzelfde inrichting. Zo sluiten de verschillende lagen van sturen tot en met uitvoeren goed op elkaar aan.

2 Beleid Privacy

2.1 Waarom hebben we beleid voor Privacy?

De visie op Privacy geeft aan welke pijlers wij belangrijk vinden. Door een toekomstgerichte, trendbewuste en veilige gemeente te zijn dragen we bij aan de democratische rechtsstaat. Dit beleid is bedoeld om te laten zien waarop we willen investeren in kennis en kunde. Zo kunnen we actuele vraagstukken rondom gegevensbescherming adequaat aanpakken.

2.2 Voor wie is het beleid bedoeld?

Het beleid is van toepassing op de hele organisatie, op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente Zaanstad. Het college stelt het beleid vast.

2.3 Welke wettelijke kaders zijn van toepassing?

Verwerkingen van persoonsgegevens zijn gebonden aan wet- en regelgeving. In deze wet- en regelgeving staan bepalingen die aangeven hoe met de bescherming van persoonsgegevens moet worden omgegaan. De belangrijkste wettelijke kaders staan in:

- Artikel 8 Europese Verdrag voor de Rechten van de Mens;
- Artikelen 10 t/m 13 Grondwet;
- De Algemene Verordening Gegevensbescherming en de Uitvoeringswet AVG;
- Wetten gericht op de uitvoering in specifieke sectoren zoals:
    - Wet Maatschappelijke Ondersteuning 2015;
    - Participatiewet;
    - Jeugdwet;
    - Wet Algemene bepalingen Omgevingswet (WABO);
    - Wet openbaarheid van bestuur (Wob);
    - Wet Basis Registratie Personen;
    - Drank- en Horecawet
- Archiefwet
- Het wetboek van Strafrecht

Naast de wet- en regelgeving van buiten kennen we ook eigen kaders die van invloed zijn op de verwerkingen van persoonsgegevens:

- Informatieveiligheidsbeleid;
- Integriteitsbeleid.

3 Ambities en uitgangspunten

Vanuit de visie op Privacy zijn ambities en uitgangspunten afgeleid. Ze staan beschreven in het Visie document. Een samenvatting is hier opgenomen.

Ambities

We leggen onze ambities hoog in het digitaliseren en automatiseren van de werkprocessen. Dit biedt voordelen voor onze inwoners, bedrijven en belanghebbenden. Digitaliseren bevordert gemak en kan procedures vergemakkelijken en versnellen. Omdat niet alle inwoners mee kunnen komen in de digitale ontwikkelingen, houden we de papieren processen in stand.

In maatschappelijke ontwikkelingen staat privacy soms onder druk. Er kleven soms privacy dilemma's, -risico's of ethische vraagstukken aan de inzet van techniek. Wij willen op een veilige, verantwoorde en ethische manier omgaan met onze data.

Uitgangspunten

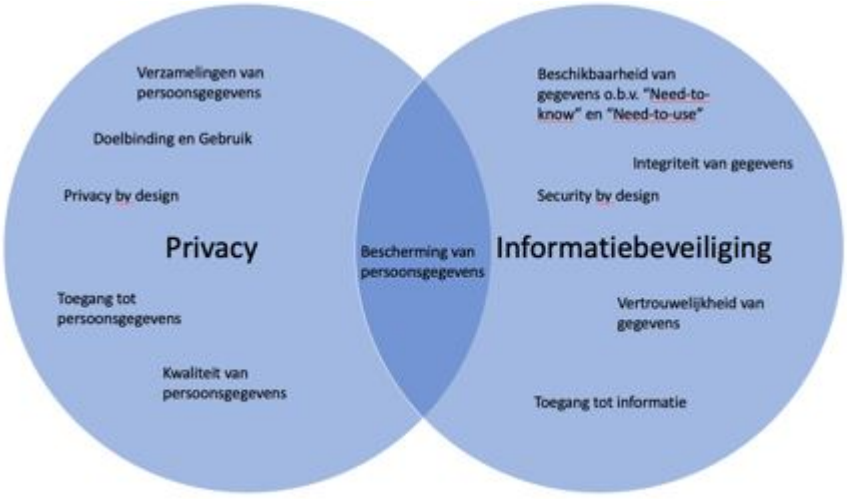
- *Bij dataverzamelingen en datagebruik zetten wij het maatschappelijk belang voorop;*
  Dataverzameling en -gebruik moet noodzakelijk zijn voor het maatschappelijk belang en bijdragen aan de leefbaarheid van de stad en de dorpen;
- *Inwoners kunnen vertrouwen op onze zorgvuldigheid;*
  Inwoners, bedrijven en belanghebbenden moeten erop kunnen vertrouwen dat we zorgvuldig met hun gegevens omgaan[1]. Wij zijn een betrouwbare overheid, zeker omdat mensen niet altijd de keuze hebben om hun (soms zeer privacygevoelige) gegevens aan ons te geven.;

1) AVG artikel 5, lid, 1, a.

- *Wij beschermen onze informatie;*
  We beschermen al onze systemen en de informatie die we daarin verwerken en hebben opgeslagen;
- *Wij geven toegang tot informatie volgens het " Need-to-know " en " Need-to-Use " principe;*
  Onze medewerkers mogen en kunnen alleen die informatie zien die zij voor hun werkprocessen nodig hebben. We beschermen onze (persoons)gegevens tegen ongeoorloofde toegang;
- *Wij passen Privacy-by-design en Privacy-by-default toe;*
  We nemen privacy afwegingen en informatieveiligheidsmaatregelen vanaf het begin mee bij aanpassingen van processen en systemen.
- *Wij nemen maatregelen gebaseerd op risico acceptatie;*
  We kiezen bij het nemen van informatieveiligheidsmaatregelen voor de juiste balans tussen informatieveiligheid en gebruiksgemak. Zo wordt voorkomen dat die de werkprocessen belemmeren;
- *Wij innoveren en investeren in maatregelen;*
  We vergroten het vertrouwen bij onze inwoners, bedrijven en belanghebbenden door aantoonbaar en blijvend te innoveren en investeren in privacy en informatieveiligheid;
- *Wij blijven verantwoordelijk voor persoonsgegevens "in huis" en "bij derden";*
  We zijn ook verantwoordelijk voor de verwerkingen en de informatie die we door "derden" laten uitvoeren. Daar maken we goede afspraken over met de ketenpartners en leveranciers die we in (verwerkers)overeenkomsten vastleggen.;
- *Proceseigenaren zijn verantwoordelijk;*
  We stimuleren proceseigenaren in onze organisatie in het nemen en voelen van verantwoordelijkheid voor de zorg rond privacy en informatieveiligheid.

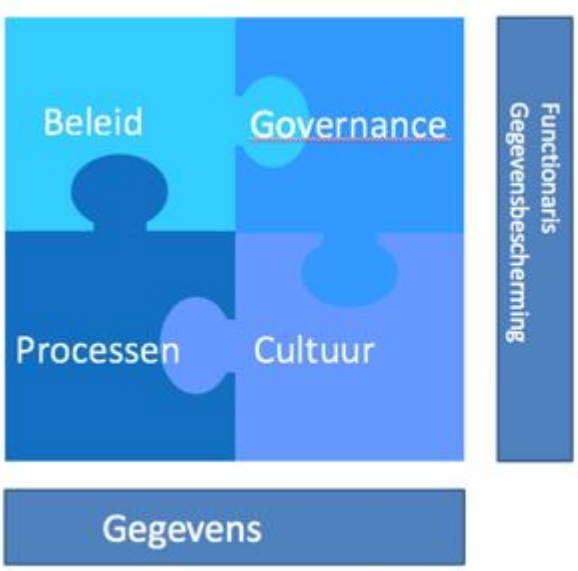
4 Samenhang Privacy en Informatieveiligheid
Privacy en Informatiebeveiliging zijn twee terreinen die met elkaar verbonden zijn. In de bescherming rond persoonsgegevens hebben beide een eigen en een gezamenlijke taak.

Dit blijkt ook uit de AVG (art. 5, lid 1, f) waarin staat dat persoonsgegevens op een veilige manier verwerkt moeten worden door het nemen van de juiste technische en organisatorische maatregelen. Maatregelen die ervoor moeten zorgen dat het verwerken van persoonsgegevens op een passende beveiliging kan rekenen. Op het bijgevoegde plaatje is de overlap aangegeven.



Figuur 2: Samenhang Privacy en Informatieveiligheid

5 Inrichtingsmodel Privacy
In het onderstaande model is aangegeven hoe beleid, governance, processen, cultuur en gegevens zich tot elkaar verhouden. We gebruiken het als een sturingsmodel binnen het werkgebied van Privacy.



Figuur 3: Inrichtingsmodel Privacy

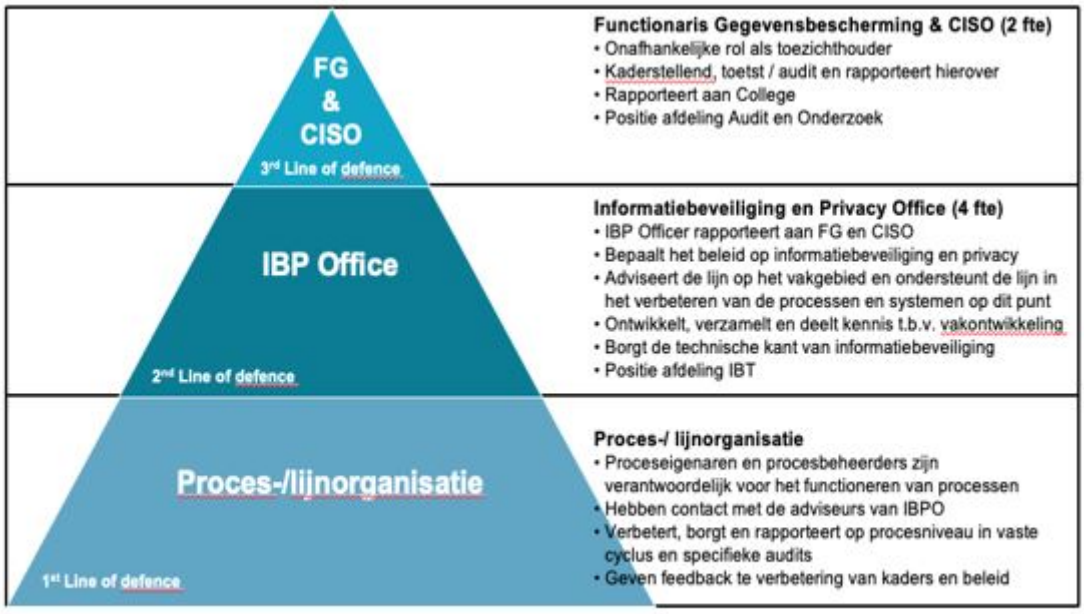
5.1 Beleid
De kaders uit dit privacybeleid vormen de uitgangspunten voor alle documenten die worden ontwikkeld om richting te geven aan de dagelijkse praktijk.
Het gaat dan om o.a.:
- Een privacyprotocol waarin richtlijnen en handvatten staan die alle medewerkers kunnen gebruiken in hun dagelijks werk;
- Privacyverklaring gemeente Zaanstad;
- Procedure Datalekken Zaanstad;
- Procedure Uitoefenen rechten betrokkenen;
- Format verwerkersovereenkomst.

Er zijn ook verschillende landelijke initiatieven voor wetsontwikkeling die het mogelijk maken gegevens tussen verschillende werkvelden uit te wisselen. Deze nieuwe wetten vragen ook om beleidsregels te ontwikkelen die de toepasbaarheid in de gemeente vergemakkelijken. Hierbij valt te denken aan gegevensuitwisseling in het sociaal domein en in de bestrijding van ondermijning.

Beleid wordt jaarlijks getoetst en bijgesteld op basis van een PDCA cyclus.

5.2 Governance

Governance van Privacy
De Governance rond Privacy wordt uitgevoerd volgens het model "Three Lines of Defense". In de onderstaande figuur is dit weergegeven.



Figuur 5: Governancemodel Privacy

De Governance is verder uitgewerkt waarbij:

1. Niveau 1: het gaat om het borgen van de privacy kennis, kunde en aandacht binnen de werkprocessen van de lijn. Accenthouders binnen de lijnorganisatie hebben hierin een belangrijke rol;
2. Niveau 2: het gaat om beleidsvorming, adviseren en faciliteren van de proceseigenaren en/of lijnmanagement. Het team IBPO heeft hier haar rol;
3. Niveau 3: het gaat om kaders stellen, onafhankelijk toezicht, strategisch adviseren, toetsen en rapporteren. Dit wordt ingevuld door de FG en CISO.

Overlegstructuren

Om de communicatie en overleggen in het Governancemodel vorm te geven zijn er 3 overleg structuren.

1. Het Strategisch Overleg Privacy Informatieveiligheid (SOPI) wordt 4 x per jaar gehouden. Organisator van het overleg zijn FG en CISO. Deelnemers aan het overleg zijn Sectorhoofd bedrijfsvoering, Afdelingsmanager Audit&Control, Afdelingshoofd Juridische Zaken en Afdelingshoofd IBT. De Concern Controller neemt deel afhankelijk van het onderwerp. Tijdstip van het overleg is een week voorafgaand aan de DO voortgangsrapportage.
2. Het IBPO Overleg.is al operationeel en wordt iedere maand gehouden. Dan sluiten FG en CISO aan. Organisatie van het overleg ligt in handen van IBPO. Alle onderwerpen van operationele aard komen aan bod.
3. Het Informerend Overleg wordt 2 x per jaar gehouden. De organisatie van dit overleg ligt in handen van IBPO. Het overleg heeft tot doel de keyspelers van de organisatie te informeren over onderwerpen rond privacy en informatieveiligheid en informatie op te halen uit de organisatie. Deelnemers zijn IBPO, FG, CISO, Integriteit, Facilitair, Strategie, Business Control BV, Business Control MO, Business Control SO, en verder nog te bepalen.

Overige overleggen

Naast de Governance overleggen vinden er ook andere overleggen plaats. Het gaat om overleggen waarin de privacy officers de accenthouders ondersteunen.

a. Accenthouders
   In dit overleg kunnen de Accenthouders hun vragen stellen en krijgen zij de laatste ontwikkelingen te horen rond Privacy. Het overleg is maandelijks.

Rollen en verantwoordelijkheden rond Privacy

In de onderstaande tabel zijn de rollen en verantwoordelijkheden met betrekking tot privacy opgenomen.

Verantwoordelijk	Rol
Verwerkingsverantwoordelijke (Eindverantwoordelijk)	Burgemeester College

Verantwoordelijk (feitelijk verantwoordelijk)	Directie
Uitvoerend (Proces verantwoordelijk)	Domein directeur, Sectorhoofden, Management teams, Afdelingsmanagers, Teammanagers, Proceseigenaren
Adviserend	Functionaris Gegevensbescherming (FG) Privacy Officer (PO) Chief Information Security Officer (CISO) Security Officers (SO)
Geïnformeerd	Gemeenteraad Functionaris Gegevensbescherming (FG) Belanghebbenden Betrokkenen

Gemeenteraad
De gemeenteraad is zelf verantwoordelijk voor het borgen van de privacy binnen de griffie en de door hen ingestelde commissies.
Daarnaast kan de gemeenteraad door het college worden geïnformeerd over de staat van Privacy in de gemeente. Jaarlijks brengt de FG een verslag uit waarin die staat wordt toegelicht vanuit het perspectief van de onafhankelijke toezichthouder.

Burgemeester
De burgemeester is voor de taakuitoefening een eigen bestuursorgaan en die hoedanigheid verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens in de eigen processen. De burgemeester neemt maatregelen om te waarborgen en aan te kunnen tonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd.

Directie
De directie (directeur van de organisatie) is voor het bestuur van de gemeente ambtelijk opdrachtnemer en eindverantwoordelijk voor de uitvoering van de taken in de organisatie rond Privacy. De directie stimuleert de kennisvergaring en bewustwording bij de medewerkers.

Sectorhoofden, afdelingsmanagers, teammanagers
De sectorhoofden, afdelingsmanagers en teammanagers zien toe op de feitelijke uitvoering van kennisvergaring en bewustwording. Zij zorgen voor het aanstellen van "Accenthouders" die hen in de 1e lijn ondersteunen in de dagelijkse naleving van de AVG.

Functionaris Gegevensbescherming
- ziet toe op de naleving van de AVG en UAVG.
- is onafhankelijk en kan voor de uitoefening van zijn rol geen aanwijzingen ontvangen van de verantwoordelijke of van de organisatie die de FG heeft benoemd (artikel 37 AVG).
- is contactpersoon voor de Autoriteit Persoonsgegevens (AP).
- houdt toezicht op de opvolging van aanbevelingen die voortvloeien uit Data Protection Impact Assesments (DPIA).
- rapporteert periodiek aan de directie over de staat van Privacy in de organisatie en jaarlijks aan de Verantwoordelijken in de gemeente.

Rapportages en verantwoording rond Privacy
Op diverse niveau's en vele gremia vindt er toezicht en verantwoording plaats over de uitvoerring van het privacybeleid. Deels zijn deze al benoemd, maar hier een overzicht van de verantwoordingen en communicatie met alle verantwoordelijken:
1. Begroting en jaarrekening. Hierin worden de speerpunten uit het privacyjaarplan toegelicht en indien nodig de financiële middelen hiervoor geregeld.
2. Jaarverslag Privacy. Deze wordt opgesteld door de FG.
3. Specifieke privacy-audits door Audit. Deze komen voort uit het Audit-jaarplan of op initiatief van de FG.
4. Voortgangsrapportage aan het DO, 4 maal per jaar.
5. Raadsvragen en informerende presentaties aan de raad. Op verzoek van de raad.
6. Vragen en onderzoeken Autoriteit persoonsgegevens. Deze onderzoeken zijn niet structureel, maar vaak op basis van door de AP ontvangen signalen.
7. Informerende presentatie in de OR. Op verzoek van de OR.
8. Vragen van burgers, belangrengroeperingen en journalisten over de wijze waarop gemeente Zaanstad omgaat met Privacy.

5.3 Processen, procedures en techniek
De processen van de gemeente Zaanstad zijn beschreven in het Proceshuis dat is opgetekend in Engage. Aan een proces is een Proceseigenaar gekoppeld. Hiermee is inzichtelijk en controleerbaar onder wiens

verantwoordelijkheid het proces wordt uitgevoerd. De Proceseigenaar heeft een verantwoordelijkheid in de naleving van de regels van de AVG binnen het proces.
Daar kunnen procedures voor worden opgesteld en werkinstructies.
Voor de invulling van technische maatregelen wordt verwezen naar het Informatie Beveiligingsbeleid dat wordt opgesteld door de CISO.

Om op een veilige manier met persoonsgegevens om te gaan zijn, al in het implementatieproject AVG, de volgende normen en uitgangspunten opgesteld.

Grondslag en doelbinding
Voor alle verwerkingen van persoonsgegevens beschikt Zaanstad over een wettelijke grondslag. De gemeente heeft inzichtelijk welke persoonsgegevens zij bijhoudt, voor welk doel zij deze bijhoudt, waar ze vandaan komen en met wie ze worden gedeeld. De gemeente houdt een Register van Verwerkingen bij waarin dit beginsel is uitgewerkt.

Subsidiariteit
Bij de verwerking van persoonsgegevens wordt erop toegezien dat een inbreuk op de persoonlijke levenssfeer van de betrokkenen zoveel als mogelijk wordt beperkt. Er wordt altijd nagegaan of het doel ook met minder ingrijpende middelen kan worden bereikt.

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

Rechtmatigheid, behoorlijkheid, transparantie
De gemeente heeft processen ingericht zodat personen, van wie de organisatie (bijzondere) persoonsgegevens verwerkt, hun rechten kunnen uitoefenen. Personen, van wie de gemeente persoonsgegevens verwerkt, worden tijdig en begrijpelijk geïnformeerd over de verwerking.

Transparantie heeft ook beperkingen wanneer er sprake is van legitieme uitzonderingen. Dit kan zijn in situaties die betrekking hebben op de openbare orde en veiligheid. De gemeente kan, met inachtneming van wet- en regelgeving, een voorbehoud maken op het transparantiebeginsel.

Data Privacy Impact Assessments (DPIA)
De gemeente Zaanstad voert risicoanalyses uit (DPIA) op verwerkingen die mogelijk een verhoogd risico opleveren.

Privacy by Design en Privacy by Default
De gemeente Zaanstad houdt bij de start van het ontwerpen of inrichten van projecten, informatiesystemen, datasets rekening met Privacy en Informatiebeveiliging.
De gemeente Zaanstad heeft de inrichting, instellingen van projecten, programma's, website(s) of diensten dusdanig georganiseerd dat maximale privacy en informatiebeveiliging wordt geborgd.

5.4 Cultuur, bewustwording
Bewust worden en bewust blijven moet in het DNA van de organisatie gaan zitten. Hiervoor worden trainingen en bijeenkomsten georganiseerd.

e-Learning
De gemeente zet in op het gebruik van e-Learning als instrument in het bewustmaken van medewerkers in de omgang met informatie. Medewerkers kunnen de modules op eigen tempo volgen.
Met regelmaat worden instaptrainingen georganiseerd om medewerkers kennis te laten maken met e-Learning en hen daarna in staat te stellen de modules zelf af te ronden.

Workshops
De Privacy Officers organiseren workshops waarin zij dieper ingaan op de beginselen van de AVG en wat dit betekent voor de werkzaamheden in de lijn.

Informatiebijeenkomst Accenthouders
Deze bijeenkomst wordt 2 x per jaar georganiseerd om actualiteiten rond wetgeving en verdiepingsvragen rond Privacy te behandelen. IBPO presenteert hier haar jaarplannen en speerpunten.

5.5 Data en Gegevens
De gemeente gaat zorgvuldig om met data en gegevens. De inwoners van de gemeente en ook de medewerkers van de organisatie mogen ervan uitgaan dat de gegeven informatie vertrouwelijk wordt behandeld.

Verwerkersovereenkomsten met derden
De gemeente maakt gebruik van derde partijen in de uitvoering van werkzaamheden waartoe zij zelf geen mogelijkheden bezit. Hierbij valt te denken aan leveranciers van software, netwerkdiensten, data-opslag. De gemeente maakt alleen gebruik van derde partijen als verwerkers van persoonsgegevens (aantoonbaar) voldoende garanties kunnen bieden om de verwerking van (persoons)gegevens te laten voldoen aan de AVG-vereisten. Hiervoor wordt zoveel mogelijk gebruik gemaakt van de modelovereenkomst van VNG-realisatie.

Dataminimalisatie
De gemeente verwerkt alleen die persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. Er wordt gestreefd naar minimale gegevensverwerking.

Bewaartermijn(en)
De gemeente bewaart persoonsgegevens niet langer dan nodig is. Het gebruiken en bewaren van persoonsgegevens kan nodig zijn om gemeentelijke taken goed uit te voeren of om wettelijke verplichtingen na te kunnen leven. Voor de bewaartermijnen wordt aangesloten bij de "Selectielijst gemeenten en intergemeentelijke organen 2017".
Daar waar wet- en regelgeving, zoals de selectielijst, geen uitsluitsel geeft over bewaring van persoonsgegevens, dienen die persoonsgegevens volgens de AVG geen dag langer bewaard te worden en terstond te worden vernietigd.

6 Uitvoering Privacy / Roadmap
In de uitvoering van werk rond Privacy wordt jaarlijks een Uitvoeringsplan gemaakt. Het Uitvoeringsplan en de onderwerpen die voor het uitvoeringsjaar belangrijk zijn, worden opgenomen in een zogenaamde Roadmap. De Roadmap geeft houvast in de uitvoering, de prioritering van de onderwerpen en het bewaken van de voortgang. Het geeft tevens houvast in de uitvoering, zodat opgaan in de dynamiek van de dag zoveel mogelijk wordt voorkomen.