

Privacybeleid gemeente Zaanstad 2024-2026

1. Inleiding

De gemeente werkt met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maken het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Zaanstad is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale- en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) en de Wet politiegegevens (Wpg).

Onze beleidsvorming, inrichting, sturing, meting en verbetering vindt gestructureerd plaats volgens een duidelijke PDCA-cyclus (Plan-Do-Check-Act). En altijd langs dezelfde 5 'privacy-pijlers':

- 1 Beleidsvorming
- 2 Bewustwording
- 3 Privacy instrumenten
- 4 Beveiligen
- 5 Monitoren

Geldigheidsduur

Dit privacybeleid is door Burgemeester en wethouders respectievelijk Burgemeester (openbare orde en veiligheid) vastgesteld. Het beleid wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's) kan het college besluiten tot een tussentijdse herziening.

2. Begripsbepalingen

De definities van art. 4 AVG, respectievelijk artikel 1 Wpg hebben in dit beleidsdocument dezelfde betekenis.

3. Privacy borging

De komende jaren zet de gemeente in op het verder verhogen van de privacy bewustwording en de professionalisering van de privacy functie in de organisatie. Een goede privacy borging is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

Zie ook de 'Visie Informatieveiligheid en Privacy' van Zaanstad.

4. Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen, waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid op hoofdlijn taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, protocollen en regelingen. Dit geldt voor gemeente brede privacy-processen zoals datalekken, maar ook voor domein-specifieke onderwerpen zoals gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning. Privacy is een vast aspect binnen procesmanagement. In alle relevante werkinstructies wordt de privacy standaard en aantoonbaar verwerkt.

Naast dit door het college vastgestelde privacybeleid is informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijk informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen of namens de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de uitgangspunten en principes in dit privacybeleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

De meeste verwerkingen van persoonsgegevens vallen onder de regels van de AVG. Voor enkele specifieke gemeentelijke taken (zoals straattoezicht, toezicht op het water, leerplicht, sociale recherche) is sprake van de uitvoering van een politietaken en is de Wet politiegegevens (Wpg) van toepassing. Op deze verwerkingen zijn op onderdelen iets afwijkende (soms meer vergaande) regels van toepassing. Het privacy-beleid is van toepassing op alle verwerkingen van persoonsgegevens door gemeente Zaanstad, inclusief persoonsgegevens die worden verwerkt in het kader van de uitvoering van een politietaken (politiegegevens).

6. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal beginselen voor de verwerking van persoonsgegevens (artikel 5 AVG). Deze kernbegrippen zijn: rechtmatig, behoorlijk, transparant, gerechtvaardigd doel, noodzaak, juistheid, bewaarbeperking en beveiliging.

Zaanstad onderschrijft de AVG-beginselen en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze beginselen. Bij de inrichting van de processen hanteert Zaanstad daarbij de onderstaande principes.

6.1 Ambitieniveau Zaanstad

Zaanstad werkt aan het vertrouwen bij onze inwoners, bedrijven en belanghebbenden door aantoonbaar en blijvend te innoveren en investeren in privacy en informatieveiligheid. Zaanstad voldoet aan de wettelijke verplichtingen voortvloeiend uit de AVG en de Wpg. De ambitie van Zaanstad is om op de privacyborging een gemiddeld volwassenheidsniveau te bereiken en dit niveau daarna ook vast te houden.

Jaarlijks rapporteert de Functionaris Gegevensbescherming aan het directieteam over de mate van realisatie van deze ambitie, de naleving van de onderliggende normenkaders en doet aanbevelingen ter verbetering.

Zaanstad volgt de landelijke ontwikkelingen en maakt waar mogelijk gebruik van de handreikingen van de VNG. Zaanstad heeft niet de ambitie en ook niet de middelen om landelijk koploper te zijn bij het verder ontwikkelen van het privacy-instrumentarium.

6.2 Voldoende capaciteit

Bij de tactische uitwerking van onderstaande principes en bij de operationele uitvoering in de 1e (uitvoerende) en 2e (ondersteunende en adviserende) lijn wordt altijd vooraf gezorgd voor voldoende capaciteit. Dit is het leidend principe bij de toepassing en uitvoering van alle strategische principes voor verwerking van persoonsgegevens.

De borging van privacy in de processen is een optelsom van de inspanningen van de privacy officers en de lijn gezamenlijk. Deze capaciteit is aan beide kanten beperkt.

De gemeente staat bovendien de komende beleidsperiode voor enorme financiële uitdagingen. Daar waar spanning ontstaat tussen de gevraagde en de beschikbare capaciteit worden keuzes gemaakt. Dit gebeurt op basis van een bewuste afweging tussen de wenselijkheid en de afname van de risico's versus de hiervoor benodigde inzet van capaciteit en geld. De keuzes worden gedocumenteerd. Hierdoor is zichtbaar en uitlegbaar waarom sommige zaken wel en andere niet of op een later moment worden opgepakt. Er is sprake van een bewuste acceptatie van de keuzes door de organisatie heen (CD/ opdrachtgever / opdrachtnemer / procesverantwoordelijken).

6.3 Rechtmatige grondslag

Persoonsgegevens worden door de gemeente slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

6.4 Welbepaalde doeleinden

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend). De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

6.5 Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

6.6 Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

6.7 Juiste en actuele gegevens

De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

6.8 Gegevens worden op tijd vernietigd

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer

als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

6.9 Integriteit en vertrouwelijkheid

De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens (zoals bijvoorbeeld gezondheids- en strafrechtelijke gegevens, etnische afkomst of seksuele gerichtheid) te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Wij gebruiken alleen externe digitale toepassingen indien de gegevens daar voldoende veilig zijn en wij grip en zeggenschap hebben op het gebruik ervan.

6.10 Proceshuis, Privacy by Default en Privacy by Design

Zaanstad beschikt over een proceshuis waarin alle gestructureerde activiteiten die plaatsvinden onder de verantwoordelijkheid van de gemeente een plek hebben. Voor de processen waarin persoonsgegevens verwerkt worden is er een gedetailleerde procesbeschrijving beschikbaar. Dit geldt ook voor nieuwe diensten, voorafgaand aan de uitrol. De procesbeschrijving vormt de basis voor de toetsing van de privacy-borging in het proces (checklist privacy/DPIA) en het register van verwerkingen.

De gemeente houdt bij de ontwikkeling van nieuwe en bestaande diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt Privacy by Design genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

6.11 Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

6.12 Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de 'Procedure datalekken'.

6.13 Samenwerking

De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden

Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

6.14 Doorgifte buiten de EER

Zaanstad verwerkt bij voorkeur geen persoonsgegevens buiten de Europese Economische Ruimte (EER). Uitgangspunt is meer concreet dat verwerking buiten de EER alleen is toegestaan als er geen

redelijke alternatieve oplossing binnen de EER beschikbaar is. Bij het inkooptraject wordt dit in de bestekfase meegenomen.

Doorgifte van persoonsgegevens aan landen buiten de EER of een internationale organisatie, geschiedt altijd in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Bij verwerking buiten de EER wordt voorafgaand een Data Transfer Impact Assessment (DTIA) uitgevoerd. De FG adviseert hierop, de proceseigenaar beslist en accepteert de risico's van de verwerking buiten de EER. Bij een negatief advies van de FG (dus het advies om de verwerking buiten de EER niet te doen) moet bij een afwijkend besluit van de proceseigenaar dit besluit door de concerndirectie worden bevestigd.

In de verwerkersovereenkomst worden toereikende beveiligingsmaatregelen over de verwerking buiten de EER afgesproken.

6.15 Transparantie

De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Hoe Zaanstad omgaat met persoonsgegevens is opgenomen in de privacyverklaring op de website van Zaanstad. Meer specifiek informeren wij betrokkenen op het moment dat zij gegevens aan ons verstrekken, bijvoorbeeld door informatie op het aanvraagformulier, een flyer en/of specifieke info per onderwerp op de website.

6.16 Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.

Zaanstad heeft hiervoor een proces ingericht. Een aanvraag kan via de website digitaal worden ingediend. Informatieverzoeken worden afgehandeld door de betreffende afdeling.

Bij algemene inzageverzoeken wordt vooraf contact gezocht met de aanvrager om te kijken of het verzoek kan worden verduidelijkt. Met als doel dat betrokkene een meer toegespitst besluit krijgt, dat beter antwoord geeft op de achterliggende vraag van betrokkene.

6.17 Geschillenbeslechting

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website <link>. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

6.18 Verantwoording

Onder de verantwoordelijkheid van zowel het college van B&W als de Burgemeester (openbare orde) vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG en de Wpg intern wordt nageleefd.

6.19 Verwerkingsregister

De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

6.20 Data Protection Impact Assessment (DPIA)

Als een verwerking mogelijk een hoog risico inhoudt voor betrokkenen, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens.

Om dit te kunnen bepalen hanteert Zaanstad een privacy-checklist, waarin een afwegingskader is opgenomen. Op basis van criteria wordt bepaald of een proces DPIA-waardig is. De privacy officer adviseert hierover aan de proceseigenaar.

De proceseigenaar voert vervolgens een Data Protection Impact Assessment (DPIA) uit. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. De proceseigenaar accepteert de restrisico's. Als het niet lukt om (voldoende) maatregelen te nemen om het hoge risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

6.21 Functionaris gegevensbescherming (FG)

De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is intern toezichthouder, heeft een adviserende, informerende en toezichthoudende taak en een onafhankelijke positie in de organisatie. De FG ziet toe op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen. De FG van Zaanstad is het eerste aanspreekpunt voor privacyvragen van burgers (fg@zaanstad.nl).

De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

6.22 Organisatie en Privacy Control Framework

Zaanstad heeft een effectieve organisatie- en rapportage-structuur om de privacy te borgen en te voldoen aan wet- en regelgeving. Dit wordt vastgelegd in een Privacy Control Framework. Het Privacy Control Framework wordt door het directieteam vastgesteld. In het Privacy Control Framework zijn ook de taken en verantwoordelijkheden van alle rollen afgebakend en vastgelegd. Het Privacy Control Framework vormt het bepalende normenkader voor de privacy-inrichting en beheersing.

6.23 PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er zowel gemeente breed als op clusterniveau een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Daarnaast gebruikt de gemeente het borgingsproduct van de VNG als het beoordelingsinstrument voor het waarborgen van privacy compliance binnen de gemeente. Het borgingsproduct is een toetsingskader wat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende (nog te treffen) beheersmaatregelen binnen de gemeente. De Functionaris Gegevensbescherming (FG) rapporteert hierover aan het directieteam en B&W (ter info aan de raad). Los daarvan vinden er op onderdelen specifieke privacy-audits plaats, waaronder de verplichte audits conform de Wet politiegegevens (Wpg).

6.24 Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

6.25 Risico gebaseerde aanpak

Zaanstad hanteert een risico gebaseerde aanpak. Dit houdt in dat de te treffen maatregelen altijd worden afgewogen tegen de risico's die met die maatregel worden gemitigeerd. Alle risico's afdekken is qua capaciteit en kosten niet mogelijk.

Voor privacy vindt hiertoe jaarlijks een privacy risico-inschatting plaats op alle processen en worden DPIA's uitgevoerd op alle processen met een hoog risico. Deze DPIA's worden periodiek herhaald. De frequentie is hierbij afhankelijk van het risico en de specifieke omstandigheden van het betreffende proces. Met een minimum frequentie van eens per 5 jaar.

6.26 Datapakhuis

Gemeente Zaanstad beschikt over een datapakhuis. In dit datapakhuis worden persoonsgegevens van alle belangrijke afzonderlijke informatiesystemen van de gemeente samengebracht. Hierdoor is het mogelijk om informatie beter te ontsluiten en (beleids-)analyses te maken. Analyses vinden altijd plaats op gepseudonimiseerde gegevens. Indien depseudonimisering van persoonsgegevens in een analyse gewenst is, moet voorafgaand een uitgebreid protocol worden doorlopen. Met daarin een zorgvuldige privacy-afweging en een besluit door B&W.

6.27 Artificiële Intelligentie (AI), Algoritmes en geautomatiseerde besluitvorming

De ontwikkelingen in het gebruik van AI gaan razendsnel. Zaanstad volgt dit op de voet en zorgt voor een actueel beleid en instructies voor het gebruik van algoritmes en AI door medewerkers en in onze processen.

6.27-1 Artificiële Intelligentie

Het benodigde AI-beleid zal vorm krijgen in 2024. Hierbij is het essentieel om eerst de impact van de AI-wet en het algoritme register te onderzoeken, inclusief het begrijpen van de wettelijke vereisten, de implicaties voor Zaanstad, het vaststellen van verplichtingen en optionele keuzes, en het toewijzen van verantwoordelijkheden binnen de gemeente. Deze bevindingen moeten vervolgens worden geïntegreerd in het bredere kader van het opstellen van AI-beleid voor Zaanstad op alle managementniveaus. Op strategisch niveau moet duidelijk zijn wat onze ambitie is voor het verantwoord toepassen van AI in onze bedrijfsvoering. Op tactisch niveau moeten spelregels, leerprocessen via pilots, besluitvormingsprocessen voor AI-toepassingen, governance en aanbestedingsrichtlijnen worden ontwikkeld. Ten slotte moet op operationeel niveau dit beleid worden geïntegreerd in onze processen rond AI-toepassingen, inclusief periodieke evaluaties om de effectiviteit van ons beleid te beoordelen.

6.27-2 Algoritmes

Zaanstad kan ter ondersteuning, nu en in de toekomst, gebruik maken van algoritmes die volgens de concept AI-Act van de Europese Unie kwalificeren als algoritmes met een hoog risicogehalte. We kunnen informatie gebruiken om bijvoorbeeld (risico-)groepen in kaart te brengen. Als wij beoordelen dat iemand tot een bepaalde (risico-)groep behoort, kunnen wij altijd uitleggen hoe wij tot die beoordeling zijn gekomen.

Voorafgaand aan het gebruik van algoritmes met een hoog risico vindt voorafgaand altijd een zorgvuldige afweging plaats en een besluit hierover op bestuurlijk niveau (B&W). Voor de definities van de impact van algoritmes wordt aangesloten bij AI-Act van de Europese Unie en daarop gebaseerde landelijke handreikingen.

Indien wettelijk verplicht dan zal het betreffende algoritme opgenomen worden in een openbaar te publiceren algoritme-register.

6.27-3 Geautomatiseerde besluitvorming

Wij vertrouwen nooit zonder meer op een computeranalyse. We gebruiken geen algoritme of AI gedreven systemen voor geautomatiseerde besluitvorming met directe rechtsgevolgen voor betrokkenen. Er volgt dus altijd een menselijke beoordeling en afweging voorafgaand aan het besluit.

6.28 Innovatie en monitoren burgers

Innovatieprojecten bij Zaanstad hebben niet het primaire doel om informatie over individuele inwoners te verzamelen of inwoners te volgen in de openbare ruimte. Zaanstad is transparant over apparatuur die aanwezig is in de openbare ruimte en het doel daarvan.

6.29 Betrouwbare en veilige overheid

Zaanstad verstrekt geen informatie aan andere inwoners of voor commerciële doeleinden. Wij verkopen, verruilen of verhandelen persoonsgegevens nooit aan derden.

6.30 Privacy medewerkers en burgers versus Wet Open Overheid (Woo)

Onze gemeenteraad heeft voor wat betreft de openbaarmaking van informatie het ambitieniveau bepaald: maximaal transparant.

Zaanstad heeft dus de intentie om open en transparant naar buiten te zijn, maar borgt gelijk ook de privacy van haar medewerkers en inwoners. De gemeenteraad weegt dit af in het beleid voor openbaarmaking. Het college en burgermeester houden hier rekening mee in de uitvoeringspraktijk.

Het gaat hierbij om de balans tussen het geven van optimale transparantie aan onze inwoners en organisaties en het beschermen van de privacy van betrokkenen. We houden rekening met belangen die openbaarmaking in de weg kunnen staan waarbij de AVG en de uitvoeringswet op de AVG leidend zijn

voor wat betreft privacy. Zo worden alle naar personen te herleiden gegevens uit documenten onleesbaar gemaakt op een enkele uitzondering na: denk aan de naam van de burgemeester of degene die mandaat hebben om te ondertekenen.

7. Rollen en Verantwoordelijken

Het governancemodel van de gemeente biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, de concerndirectie en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy Officer en de CISO.

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	Proceseigenaren en Concerndirectie De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	Het college van B&W, Burgemeester
C	Consulted/ Adviserend	Privacy Officer CISO/ISO Functionaris Gegevensbescherming
I	Informerend/ Geinformeerd	Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) Functionaris Gegevensbescherming Belanghebbende(n)/Betrokkene(n)

Rollen en verantwoordelijkheden

College van B&W

Het College is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de de privacywetgeving binnen de gemeente;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

Proceseigenaren, clustermanagers en concerndirectie

Zaanstad stimuleert proceseigenaren in het voelen en nemen van verantwoordelijkheid en eigenaarschap voor de privacy en informatieveiligheid in hun processen. In de 1e lijn is voldoende capaciteit beschikbaar bij accenthouders privacy en bij procesbeheerders om de privacy in te regelen en te monitoren. Privacy is één van de taken die onderdeel uitmaken van het bredere procesmanagement/procesbeheer binnen Zaanstad. Binnen de concerndirectie is de gemeentesecretaris eindverantwoordelijk voor de privacyborging.

De proceseigenaren/afdelingshoofden en clustermanagers zijn verantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling c.q. het cluster, alsmede voor de uitvoering van het privacybeleid.

De proceseigenaren en clustermanagers hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen processen en afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de processen en afdeling;
- Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;

- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de procesbeheerders en accenthouders binnen de eigen afdeling;
- Bevordert duurzame privacycultuur;
- Betreft PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezicht houdende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:

- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het College van B&W.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor de proceseigenaren rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van DPIA's en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert (in afstemming met vakjuristen) over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Privacy Accenthouder

De Privacy Accenthouder is het eerste aanspreekpunt voor privacy-issues vanuit de afdeling en heeft een monitorende, ondersteunende en stimulerende functie rondom het naleven en uitvoeren van het privacybeleid. De accenthouders werken hiertoe actief onderling samen en ook met de Privacy Officer.

De minimale benodigde inzet bedraagt gemiddeld 1 uur per week per afdeling. Deze inzet kan incidenteel en tijdelijk hoger liggen, bijvoorbeeld bij nieuwe ontwikkelingen/ proceswijzigingen, een complex datalek of andere speciale omstandigheden.

De activiteiten binnen de afdeling door de accenthouder zijn concreet:

- Het signaleren van privacy-vraagstukken en het beantwoorden van privacy-vragen van medewerkers op de afdeling;
- Deelname aan accenthouders-overleggen en kennisbijeenkomsten;
- Kennis van de processen op de afdeling (Engage);
- Invullen jaarlijkse monitor FG;
- Ondersteuning procesbeheerder bij checklist privacy en vragen van PO of FG;
- Ondersteuning procesbeheerder bij het actueel houden van het Register van Verwerkingen en andere AVG-verplichtingen (zoals AVG-verzoeken);
- Hulp bij de afwikkeling van datalekken;
- Bijdragen aan cluster-specifieke werkinstructies en protocollen;
- Ondersteuning bij DPIA (in de toekomst).

Andere rollen en verantwoordelijkheden

Afdeling	Betrokkenheid
Juridische Zaken	Ondersteunen van Privacy Officer ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
CISO	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseren van de organisatie bij datalekken (volgens de meldprocedure). Tijdig melden van Informatiebeveiligingsincidenten bij PO/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie, inclusief privacy.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).