

Visie(r) op Zaanstad! Privacy en Informatieveiligheid, Vertrouwen op een goede basis

Onze visie op Privacy en Informatieveiligheid.

Privacy en Informatieveiligheid zijn twee belangrijke pijlers van onze democratische rechtstaat. Privacy en informatieveiligheid zijn van essentieel belang voor het vertrouwen van onze inwoners in de gemeente en voor het correct en verantwoordelijk omgaan met de gegevens die in onze zorg zijn. Deze meerjarige visie schetst ons pad naar een robuust en toekomstbestendig systeem dat de privacy van onze inwoners waarborgt en de veiligheid van hun gegevens verzekert.

Dat gevoel van veiligheid, dat rust op deze twee pijlers, is een vereiste voor het uitoefenen van andere fundamentele vrijheden zoals de vrijheid om voor je mening uit te komen in spreken en schrijven.

Privacy en Informatieveiligheid zijn twee belangrijke pijlers van onze democratische rechtstaat.

Wij willen als Zaanstad bijdragen aan de democratische rechtstaat door een toekomstgerichte, en veilige gemeente te zijn. Door continue verbetering en aanpassing aan de nieuwste standaarden en ontwikkelingen, waarborgen we de veiligheid van de aan ons toevertrouwde informatie en beschermen we de privacy van onze inwoners met de hoogste integriteit en ethische overwegingen. Ook zorgen we ervoor dat onze dienstverlening zoveel mogelijk kan blijven doorgaan als we last hebben van verstoringen.

Onze ambities.

Onze digitale ambities liggen hoog en onze processen worden vergaand geautomatiseerd. Dit biedt voordelen voor onze inwoners, voor bedrijven en belanghebbenden. Digitaliseren kan procedures vergemakkelijken. Omdat niet alle inwoners mee kunnen komen in de digitale ontwikkelingen, houden we de papieren processen in stand.

Niet alleen onze administratieve processen digitaliseren, ook de openbare ruimte digitaliseert. Gemeenten, bedrijven en kennisinstanties verzamelen en gebruiken steeds meer gegevens.

Aan deze ontwikkelingen kleven ook dilemma's, risico's en ethische vraagstukken. Privacy en informatieveiligheid staan onder druk. Wanneer informatie niet op ieder moment direct beschikbaar is, zijn we onthand. Wij willen gegevens op een veilige, verantwoorde en ethische manier beschikbaar stellen. Alternatieven voor digitale gegevensverwerking zijn er bijna niet meer. Kroontjespen en ganzenveer zijn allang afgeschreven.

Ook dreigingen als cybercriminaliteit en onbedoelde inzage of aanpassing van gegevens door onbevoegden willen we voorkomen.

Onze digitale ambities liggen hoog en bieden voordelen voor inwoners, bedrijven en belanghebbenden.

Hoe kunnen wij zo goed mogelijk gebruik maken van de nieuwe ontwikkelingen en tegelijkertijd de risico's van digitaliseren beperken? De voorwaarden en uitgangspunten werken we uit in beleid voor Privacy en Informatieveiligheid.

Informatie is een belangrijk bedrijfsmiddel.

De processen van onze organisatie zijn afhankelijk van digitale informatie. Dat geldt voor administratieve processen (zoals paspoortuitgifte, verstrekken van uitkeringen) maar ook voor industriële (automatisering)processen in de openbare ruimte zoals riool- en watergemalen, brug- en sluisbediening en verkeersregeling systemen.

Data verzamelen en verwerken tot informatie is geen doel op zich, wel noodzakelijk om onze processen goed te laten verlopen.

Data verzamelen en verwerken tot informatie is geen doel op zich. Informatie is noodzakelijk om de processen in de gemeente goed te laten verlopen. Het is de fundering van gemeentepannen en ontwikkelingen. Wanneer we dit fundament niet goed beschermen zakt ons informatiehuis vroeg of laat in elkaar. Het uitvoeren van de gemeentelijke taken en plannen komt dan in gevaar.

Vaststellen van beleid.

Dit document geeft naast de visie ook op hoofdlijnen onze uitgangspunten rond privacy en informatieveiligheid. Met dit document stelt het college de uitgangspunten vast waarop we beleid baseren. Voor zowel privacy als informatieveiligheid werken we in afzonderlijke beleidsdocumenten (één voor privacy en één voor informatiebeveiliging) uit hoe we invulling geven aan de uitgangspunten. Het beleid wordt door het college van B&W vastgesteld.

Uitgangspunten en leidende principes.

Gemeente Zaanstad baseert de uitgangspunten en leidende principes op onze visie op privacy en informatieveiligheid.

Bij dataverzamelingen en -gebruik 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. Daarbij mag de data alleen worden verzameld voor een gerechtvaardigd doel¹ en niet verder worden verwerkt voor andere doeleinden.

Persoonsgegevens moeten altijd verwerkt worden binnen de wettelijk gestelde kaders, anders is het een onrechtmatige verwerking. Zaanstad maakt bij het inrichten van processen altijd de afweging tussen het te bereiken doel en de inbreuk op de persoonlijke levenssfeer van de inwoners (proportionaliteit). Deze afweging wordt vastgelegd en is uitlegbaar.

Los daarvan moet er ook gekeken worden of de verwerking wel verantwoord is om uit te voeren en van toegevoegde waarde is voor de maatschappij. De vraag is niet alleen kunnen en mogen wij iets verwerken, maar ook willen wij dit wel verwerken? Dit is het ethische component. Als het verwerken van persoonsgegevens juridisch gezien is toegestaan, betekent dat niet per se dat het wenselijk is. Zo willen wij ook reflecteren op onze keuzes om bepaalde verwerkingen wel of juist niet uit te voeren. Sommige gegevensverwerkingen maken een (grote) impact op de maatschappij en dan spelen er extra afwegingen. Wij vinden het belangrijk dat deze afwegingen waar nodig op een juiste, onafhankelijke manier getoetst worden.

Inwoners kunnen vertrouwen op onze zorgvuldigheid.

Inwoners, bedrijven en belanghebbenden moeten erop kunnen vertrouwen dat we zorgvuldig met hun gegevens omgaan². Wij zijn een betrouwbare overheid, zeker omdat mensen niet altijd de keuze hebben om hun (soms zeer privacygevoelige) gegevens aan ons te geven. Wij informeren de inwoners actief over welke gegevens wij voor welke doeleinden verzamelen en verwerken, tenzij wet- en regelgeving ons dit niet toestaat.

Inwoners hebben o.a. recht op inzage en recht op correctie van hun eigen gegevens³. Data is open, inzichtelijk en gedeeld, tenzij wet- en regelgeving, veiligheidsrisico's of beschikkingsrechten op de data dit beperken. Een individu heeft beschikkingsrecht⁴ op zijn of haar data en beslist of dit gedeeld mag worden met anderen en wat er verder mee gebeurt, tenzij wet- en regelgeving dit beperken.

Het vertrouwen op zorgvuldigheid betekend ook dat wij maatregelen nemen om ons te beschermen tegen het niet beschikbaar zijn van essentiële diensten en het ongeoorloofd aanpassen van gegevens.

***Wij beschermen onze informatie* ⁵.**

We beschermen onze applicaties en systemen en de informatie die we daarin verwerken en hebben opgeslagen⁶. Behalve de administratieve systemen met veel persoonsgegevens zijn wij als gemeente

1) AVG-artikel 5

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

3) AVG artikel 15 en 16.

4) AVG artikel 6, lid 1,a.

5) BIO algemeen

6) AVG artikel 5, lid 1, f; artikel 24, lid 1

ook verantwoordelijk voor een aantal industriële systemen in de openbare ruimte. Deze systemen bevatten ook informatie die we moeten beschermen, anders kan dit onze gemeente ontregelen.

Wij geven toegang tot informatie volgens een 'need-to-know' principe ⁷.

We besluiten op basis van het "need-to-know" en "need-to-use" principe op verzoeken om toegang tot informatie. Onze medewerkers mogen en kunnen alleen die informatie zien die zij voor hun werkprocessen nodig hebben. We beschermen onze (persoons)gegevens tegen ongeoorloofde toegang. Waar nodig passen we anonimisering en pseudonimisering toe, zodat gegevens niet direct herleidbaar zijn tot een individu.

Wij passen Privacy-by-design en security-by-design toe ^{8 9}.

We nemen privacy afwegingen en informatieveiligheidsmaatregelen vanaf het begin mee bij aanpassingen van processen en systemen. We zoeken daarbij actief naar oplossingen. We gebruiken daarvoor instrumenten zoals zij uit de AVG en Baseline Informatiebeveiliging Overheid (BIO) worden aangereikt.

Wij streven naar een cultuur van privacy- en informatiebeveiligingsbewustzijn.

We streven naar een organisatie brede cultuur waarin privacy en informatieveiligheid centraal staan. Dit omvat regelmatige trainingen en bewustmakingscampagnes voor alle medewerkers om hen te onderwijzen over de relevante wetgeving, de risico's van gegevensverlies en de noodzaak van bescherming van privacy.

Wij nemen maatregelen gebaseerd op risico acceptatie ¹⁰.

Wij beschermen de privacy en informatie door een mix van maatregelen op het gebied van Mensen, Processen en Techniek. Onze maatregelen zijn risico gebaseerd. Wij 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.

Hackers worden slimmer en de druk op privacy neemt toe. Wij moeten onze beveiliging up-to-date houden. Wij innoveren en investeren aantoonbaar en blijvend in privacy en informatieveiligheid¹¹. Daarmee vergroten wij het vertrouwen bij onze inwoners, bedrijven en belanghebbenden. Hierbij zoeken we de balans tussen de te nemen maatregelen en de betaalbaarheid van de kosten.

Wij blijven verantwoordelijk voor gegevens "in huis" en bij "derden".

We zijn ook verantwoordelijk voor de verwerkingen en de informatie die we door "derden" laten uitvoeren¹²¹³. Daar maken we goede afspraken over met de ketenpartners en leveranciers die we in (verwerkers)overeenkomsten vastleggen.

De Proceseigenaren zijn verantwoordelijk ¹⁴.

Wij stimuleren proceseigenaren in onze organisatie in het nemen en voelen van verantwoordelijkheid voor de zorg rond privacy en informatieveiligheid. Proceseigenaren worden bijgestaan door specialisten uit de organisatie in vraagstukken rondom de AVG en BIO.

Door vast te houden aan deze visie en principes, zullen we een gemeente creëren die bekend staat om haar toewijding aan privacybescherming en informatieveiligheid, waarin inwoners het vertrouwen hebben dat hun gegevens in goede handen zijn en met respect worden behandeld.

7) BIO hoofdstuk 9

8) AVG artikel 25

9) BIO hoofdstuk 14.1 en 14.2

10) BIO hoofdstuk 8.2

11) AVG artikel 25

12) AVG artikel 5, lid 2; artikel 24

13) BIO hoofdstuk 15

14) BIO hoofdstuk 6.1