gemeente Zaanstad
ZNSTD
GEMEENTEBLAD
Officiële uitgave van de gemeente Zaanstad
Nr. 291025
9 november
2020

Visie Privacy en Informatieveiligheid Zaanstad

Onze visie op Privacy en Informatieveiligheid.
Privacy en Informatieveiligheid zijn twee belangrijke pijlers van onze democratische rechtstaat. Privacy is een grondrecht is en een fundamentele vrijheid, maar het gaat het ook om de bescherming van (persoons)gegevens en vertrouwelijke informatie.

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, trendbewuste en veilige gemeente te zijn. Daarom blijven wij investeren in kennis en kunde. Zo kunnen wij actuele vraagstukken rondom privacy en informatieveiligheid goed aanpakken. De bescherming van de privacy van onze inwoners richten wij in volgens de meest passende normen van informatiebeveiliging. Wij volgen daarom trends en ontwikkelingen op de voet.

Onze ambities.
In Zaanstad werken we steeds meer datagestuurd en gebruiken we onze data (en Big Data) om ons te ondersteunen in onze (maatschappelijke) vraagstukken.

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 data..

Aan deze ontwikkelingen kleven ook dilemma's, risico's en ethische vraagstukken. Privacy en informatieveiligheid staan soms onder druk. Wanneer informatie niet op ieder moment direct beschikbaar is, zijn we onthand. Wij willen onze data 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 zijn er dreigingen als cybercriminaliteit en onbedoelde inzage of aanpassing van gegevens door onbevoegden die wij willen 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 verkeersregelingsystemen.

> 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 gemeenteplannen 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 doel[1] en niet verder worden verwerkt voor andere doeleinden.

Inwoners kunnen vertrouwen op onze zorgvuldigheid.
Inwoners, bedrijven en belanghebbenden moeten erop kunnen vertrouwen dat we zorgvuldig met hun gegevens omgaan[2]. 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 gegevens[3]. Data is open, inzichtelijk en gedeeld, tenzij wet- en regelgeving, veiligheidsrisico's of beschikkingsrechten op de data dit beperken. Een individu heeft beschikkingsrecht[4] 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.

Wij beschermen onze informatie [5] ***.***

We beschermen onze systemen en de informatie die we daarin verwerken en hebben opgeslagen[6]. Behalve de administratieve systemen met veel persoonsgegevens zijn wij als gemeente 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 nemen maatregelen gebaseerd op risico acceptatie [10] ***.***

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
7) BIO hoofdstuk 9
8) AVG artikel 25
9)
10) BIO hoofdstuk 8.2

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 informatieveiligheid[11]. 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 uitvoeren[12][13]. 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.

11) AVG artikel 25
12) AVG artikel 5, lid 2; artikel 24
13) BIO hoofdstuk 15
14) BIO hoofdstuk 6.1