Notitie van de rekenkamer bij het eindrapport ‘Bescherming persoonsgegevens in Hilversum’

Achtergrond

Er zijn inmiddels enkele jaren verstreken sinds de Algemene Verordening Gegevensbescherming (AVG) in werking trad (25 mei 2018). De rekenkamer was benieuwd hoe Hilversum ervoor staat op het gebied van de bescherming van persoonsgegevens en heeft daarom een onderzoek naar dit onderwerp uitgevoerd. De onderzoeksresultaten zijn te vinden in het bijgevoegde rapport. Deze notitie is bedoeld als begeleiding bij het onderzoeksrapport.

Net als vele andere ondersteunende functies is ook de bescherming van persoonsgegevens iets waarvan velen vinden dat het vanzelfsprekend is en gewoon goed moet gebeuren. Het is geen erg politiek onderwerp dat in de directe belangstelling staat van de gemeenteraad.
Er zijn altijd risico’s, maar pas op het moment dat er iets niet goed gaat, bij een incident, wordt duidelijk wat het belang is van een goede uitvoering en is er aandacht voor het onderwerp.

Dit rapport geeft inzicht in de stand van zaken in Hilversum op het gebied van bescherming van persoonsgegevens en laat zien welke risico’s er zijn en welke maatregelen daartegen genomen kunnen worden. Het vraagt ook om belangstelling van college en gemeenteraad juist in periodes dat er geen incidenten zijn; het gaat daarbij om preventie.

Conclusies over de bescherming van persoonsgegevens in Hilversum

Hilversum heeft er de afgelopen jaren voor gezorgd dat voldaan wordt aan de organisatorische inrichting conform de huidige wet- en regelgeving. Ook in de uitvoering is er veel aandacht voor bescherming van persoonsgegevens. Wel zijn er op bepaalde gebieden achterstanden en moeten verbeteringen plaatsvinden (zie hieronder). In het rapport wordt de stand van zaken verduidelijkt door scores ten opzichte van een normenkader.

Door verbeteringen worden de risico’s voor gemeente en inwoners verkleind. Het aanjagen en volgen van dit proces is een punt van aandacht voor de gemeenteraad.

Organisatorische inrichting, beleid en uitvoering

Het rapport geeft een overzicht van de relevante wet- en regelgeving en de organisatorische en juridische vormgeving daarvan. Het beleid van de gemeente Hilversum wordt behandeld. Er is aandacht voor de uitwerking in werkprocessen, bijbehorende verantwoordelijkheden en werkinstructies.
Aan de hand van twee casussen (Smart City, Participatiewet) wordt verduidelijkt hoe in de praktijk omgegaan wordt met het onderwerp en welke maatregelen daarbij getroffen zijn. Daarin komt duidelijk de aandacht voor het onderwerp naar voren en de positieve punten van de situatie in Hilversum.

Punten ter verbetering

Lang niet alle werkprocessen zijn systematisch onderzocht op privacyrisico’s. Dit zou moeten gebeuren via zogenaamde DPIA’s (*Data Protection Impact Assessments*), maar daarbij zijn flinke achterstanden ontstaan.

Bij ontwikkeling van producten en diensten zou standaard aandacht moeten zijn voor privacy (*'privacy by design'*). Dat is niet ontwikkeld en er zit weinig vooruitgang in. Dat geldt ook voor aandacht voor privacy in ketens van activiteiten (ketenregie).

Medewerkers worden wel bijgeschoold op het gebied van informatiebeveiliging, maar dit zit niet standaard in het inwerkprogramma voor nieuwe medewerkers. Het ontbreekt op sommige plaatsen in de organisatie aan relatieve basiskennis over privacy. Daardoor is de aandacht voor privacy van burgers niet volledig geïntegreerd in het dagelijks handelen van alle medewerkers.

Er is geen structureel overleg tussen lijnmanagers (verantwoordelijk voor privacy) en het team dat voor ondersteuning zorgt (het PIT: Privacy & Informatieveiligheid Team). Ook wordt soms door uitvoerende afdelingen afstand ervaren tot het PIT.

Risico's

Bovenstaande punten kunnen, zolang ze niet zijn verbeterd, gevolgen hebben. Ze geven kans op extra risico's voor inwoners en gemeente.

Zo kan als de gemeente gehackt wordt, diefstal van privacygevoelige informatie plaatsvinden. Door het niet zorgvuldig omgaan met persoonsgegevens, kunnen incidenten met gegevens optreden, zoals bijvoorbeeld een datalek. Incidenten en tekortkomingen kunnen leiden tot negatieve beeldvorming over het functioneren van de gemeente. Deze kunnen ook leiden tot schade voor gedupeerde burgers (aantasting privacy), schadeclaims en boetes van bijvoorbeeld de Autoriteit Persoonsgegevens.

Informatievoorziening aan de gemeenteraad

Jaarlijks wordt door de onafhankelijke toezichthouder op de naleving van het privacybeleid (volgens de AVG is dit de FG, de Functionaris Gegevensbescherming) een verslag gemaakt van bevindingen over de implementatie en voortgang van de gegevensbescherming in Hilversum. Dit belangrijke verslag werd niet geagendeerd maar voor kennisgeving aangenomen. Juist dit verslag is echter een uitstekende aanleiding om als raad te spreken over gegevensbescherming, privacy en het bijbehorende beleid. Het college zou daarbij kunnen aangeven wat de bevindingen betekenen voor de burger en voor de raad.

Aanbevelingen

In het rapport zijn aanbevelingen opgenomen voor college en raad.

Voor het college zijn deze in het kort:

- Stuur op het inlopen van achterstanden en laat regelmatig DPIA's uitvoeren.
- Bevorder bij elke medewerker het bewustzijn om correct om te gaan met gevoelige informatie van inwoners. Maak dit ook onderdeel van het inwerktraject van nieuwe medewerkers.
- Bespreek met de raad de gewenste informatievoorziening op het gebied van gegevensbescherming. Besteed bij beleidsinhoudelijke onderwerpen expliciet aandacht aan privacy.

Aan de raad wordt de volgende aanbeveling gedaan:

- Besteed proactief aandacht aan de informatie die er al is. Gebruik hiervoor ook het verslag van de FG en laat dit op de agenda opnemen als te bespreken onderwerp.