

Evaluatie Algemene Verordening Gegevensbescherming (AVG) en borging in de organisatie.

14 mei 2019

Aan de leden van de raad,

Een jaar geleden, op 25 mei 2018, werd de AVG (Algemene Verordening Gegevensbescherming) van kracht. Deze verordening, die voor de hele Europese Unie van toepassing is, beschermt de rechten van inwoners op het gebied van privacy. Op 15 mei 2018 stelde u het Zwijndrechtse privacybeleid vast (2018-14932) en de wijze waarop de rollen van onder meer Functionaris Gegevensbescherming (regionaal) en Privacycoördinator (lokaal) werden ingevuld. Bij die gelegenheid informeerden wij u ook over de overige implementatie van de AVG en deden wij de toezegging een en ander na een jaar te evalueren. Met deze brief informeren wij u over de lokale, Zwijndrechtse, evaluatie. De regio is nog bezig met een eigen evaluatie.

Wat veranderde er per 25 mei 2018

De gemeente was ook op grond van de voorgaande wetgeving (Wbp, Wet bescherming persoonsgegevens) al verantwoordelijk voor een goede omgang met de privacy van burgers, maar de AVG brengt strengere eisen en een aantal verplichtingen met zich mee. De belangrijkste:

- De gemeente moet een Functionaris Gegevensbescherming (FG) aanstellen, die toezicht houdt op de juiste omgang met persoonsgegevens. De Drechtsteden hebben, uit efficiencyoverwegingen, gezamenlijk twee FG's plus twee Adviseurs Gegevensbescherming aangesteld. De FG's zijn de toezichthouder voor de zeven regiegemeenten en het formele aanspreekpunt voor de Autoriteit Persoonsgegevens. U stelde daar in mei 2018 geld voor beschikbaar.
- De gemeente dient daarnaast een Privacycoördinator aan te wijzen, voor de lokale coördinatie en uitvoering van privacy gerelateerde activiteiten. Die functie is geplaatst bij de afdeling Staf. De betreffende medewerker doet dit werk bovenop de reguliere werkzaamheden, zonder urenuitbreiding. Hoewel er sprake is van een nieuwe wettelijke taak waarvoor nieuwe formatie nodig is, is ervoor gekozen om dit in eerste instantie te organiseren binnen de bestaande formatie. De reden voor deze keus was, dat voorafgaand aan de invoering van de AVG nauwelijks viel in te schatten hoe groot de feitelijke capaciteitsbehoefte zou zijn. We hebben vorig jaar aangegeven dat uit evaluatie zou moeten blijken of er daadwerkelijk formatie-uitbreiding noodzakelijk is. Hierover later in deze brief meer.

portefeuillehouder: Jansen, T.
informatie: Jannes Blokstra
telefoon: 078 770 37 08
e-mail: jblokstra@zwijndrecht.nl
bijlagen:
ter inzage:

- De gemeente moet privacybeleid vaststellen (hebt u op 15 mei 2018 gedaan) en een aantal verplichte registers maken en vullen. Die registers zijn nodig om "accountable" te zijn, wat betekent dat voldaan wordt aan de beginselen van rechtmatigheid voor de verwerking van persoonsgegevens en dat dit kan worden aangetoond (verantwoordingsplicht). Het gaat om:
 - o een register van verwerkingen, met daarin alle processen van de gemeente waarin persoonsgegevens worden verwerkt; wij hebben hier in 2018 veel tijd in gestoken om voor de ruim duizend processen de relevante privacygerelateerde informatie vast te leggen;
 - o een register van verwerkersovereenkomsten, convenanten en privacy protocollen; dit register ontstaat door centraal (in het zaakstelsel) de verwerkersovereenkomsten op te slaan en registreren;
 - o een register van inbreuken op persoonsgegevens, datalekken; dit wordt bijgehouden door de FG's;
 - o een register voor aanvragen en uitvoering van de procedures voor betrokkenen; ook dit houden de FG's bij.
- De gemeente moet eenieder die daarom vraagt binnen vier weken inzage geven in alle over hem of haar geregistreerde persoonsgegevens, en deze op verzoek corrigeren of verwijderen.
- De gemeente moet op grond van de AVG een Privacy Impact Assessment (PIA) uitvoeren wanneer de voorgenomen verwerking waarschijnlijk een hoog risico oplevert voor de mensen van wie gegevens worden verwerkt.

De implementatie van de AVG in de Drechtsteden en Zwijndrecht

Voorafgaand aan 25 mei 2018 is in regionaal verband én lokaal hard gewerkt om te voldoen aan de eisen zoals die vanaf die datum golden. Het privacybeleid is vastgesteld, FG's en FG adviseurs benoemd, een privacycoördinator aangewezen, en er is een verwerkingenregister gemaakt, met daarin meer dan duizend gemeentelijke processen, waarbij voor ieder proces is aangegeven of en welke persoonsgegevens worden verwerkt (plus nog een aantal andere relevante gegevens). Dit vergde veel tijd van een aantal medewerkers uit de hele Zwijndrechtse organisatie. In de periode na 25 mei zijn we in Zwijndrecht begonnen waar nodig verwerkersovereenkomsten af te sluiten met externe partijen als die in opdracht van de gemeente persoonsgegevens verwerken.

Zwijndrecht kreeg als eerste gemeente in de regio te maken met een inzageverzoek van een inwoner. In de praktijk bleek, zeker als er nog geen enkele ervaring mee bestaat, hoe lastig het is om een volledig overzicht te maken van alles wat over één persoon bij de gemeente of de regionale organisaties is geregistreerd, omdat vooraf niet bekend is om welke registraties het gaat. In principe moet je alle registraties nalopen. Een dergelijk verzoek is daarmee arbeidsintensief. Naast dit inzageverzoek kreeg Zwijndrecht nog enkele verzoeken met een beroep op de AVG die na verstrekking van concreet gevraagde informatie konden worden afgedaan voordat het formele inzageverzoeken werden.

Bewustwording van medewerkers die omgaan met persoonsgegevens van de eisen die de AVG met zich meebrengt leidde tot voorlichtingsbijeenkomsten (georganiseerd door de lokale privacycoördinator, verzorgd door de FG's), posters in het gemeentehuis, en de Week

van de Informatieveiligheid, Privacy en Integriteit (WIPI), begin oktober (mede georganiseerd door de Zwijndrechtse privacycoördinator). Voor de WIPI werd lokaal en regionaal veel werk verzet, met als resultaat een succesvolle week met veel activiteiten die het privacybewustzijn vergrootten. De week leverde ook aandachtspunten op voor volgende edities. Met name maatregelen om het aantal aan de activiteiten deelnemende medewerkers te verhogen verdienen aandacht.

Een belangrijk knelpunt in het afgelopen jaar was de vraag wie bij privacy over wat gaat, zowel regionaal als lokaal. Wat is de taakverdeling tussen FG's (regionaal), Adviseurs privacy (regionaal), juristen van het Juridisch Kennis Centrum (JKC) (regionaal), privacycoördinatoren (lokaal), informatiemanagers (lokaal) en proceseigenaren (lokaal). Op initiatief van de privacycoördinatoren is dat, in belangrijke mate door de coördinatoren zelf, waaronder de Zwijndrechtse, uitgewerkt. Inmiddels is wel duidelijk geworden dat het afgelopen jaar in alle Drechtstedengemeenten teveel uitvoerende taken bij de privacycoördinatoren zijn neergelegd zodat deze te weinig zijn toegekomen aan de coördinerende taak, die op zichzelf al veel tijd vergt. De privacycoördinatoren waren daarnaast nog veel tijd kwijt aan uitzoekwerk en afstemming.

Het onderwerp waar het afgelopen jaar de meeste discussie over heeft plaatsgevonden (naast de rolverdeling) is de Privacy Impact Assessment (PIA). Het is tot op de dag van vandaag onduidelijk hoeveel PIA's moeten worden uitgevoerd. In principe kan het om vele honderden per gemeente gaan, die allemaal minstens vijf uur en vaak aanzienlijk meer werk vergen van meerdere personen. Proceseigenaren zijn er in eerste instantie zelf verantwoordelijk voor dat hun werkprocessen op orde zijn. Als daartoe een PIA moet worden uitgevoerd is dat in eerste instantie dus ook de verantwoordelijkheid van de proceseigenaar. Die kan daarbij de hulp inroepen van de privacycoördinator en de informatiemanager (beide lokaal). Het zou goed zijn dat er op centraal niveau personen komen die deskundig zijn op dit gebied zodat die bij de uitvoering van de PIA's kunnen ondersteunen; zelfs dan blijft er lokaal nog veel inzet nodig. Regionaal is de afspraak gemaakt dat bij alle nieuwe processen of applicaties standaard een PIA wordt gemaakt, zodat de achterstand niet oploopt en we ervaring met het instrument opdoen.

Een ander arbeidsintensief proces is het maken van verwerkersovereenkomsten tussen de gemeente als verwerkingsverantwoordelijke en externe verwerkers van persoonsgegevens als opdrachtnemers. Daarmee is in het afgelopen jaar in Zwijndrecht een begin gemaakt door voor belangrijke processen zo'n overeenkomst te sluiten, maar er ontbreekt een volledig overzicht van alle processen waarvoor zo'n overeenkomst noodzakelijk is. We zijn inmiddels begonnen met een inventarisatie van alle contracten waarmee de verwerking van persoonsgegevens gemoeid zou kunnen zijn. Als die inventarisatie klaar is kunnen, te beginnen met de meest riskante verwerkingen, meer overeenkomsten worden gemaakt.

Hoe verder

In de komende periode moet het volgende gebeuren:

- Taken en rollen beleggen op de juiste plek (regionaal en lokaal); hoewel het beeld inmiddels redelijk duidelijk is, moet dat nog wel worden geformaliseerd.

- In regionaal verband een Plan van Aanpak maken op basis waarvan de noodzakelijke activiteiten planmatig kunnen worden opgepakt en we voorkomen dat iedere gemeente zelf het wiel moet uitvinden.
- Het register van verwerkingen actualiseren (met name aanpassen aan de overgang van Mozaiek naar KZA). Dit moet per gemeente gebeuren.
- De noodzakelijke verwerkersovereenkomsten in beeld brengen en afsluiten.
- PIA's maken, te beginnen met nieuwe processen en activiteiten, en daarna voor de meest risicovolle processen.
- Privacybewustzijn bevorderen, onder meer door mee te doen aan acties als de Week voor de Informatieveiligheid, Privacy en Integriteit.
- Processen rond inzageverzoeken en andere aan de AVG ontleende rechten optimaliseren
- De verantwoording over privacy verder uitbouwen en optimaliseren.
- De ondersteuning van proceseigenaren verder vormgeven en uitbouwen.

Voor ieder van die activiteiten is, naast de betrokkenheid van andere medewerkers zoals proceseigenaren, inzet van de privacycoördinator noodzakelijk. De uitvoering van alle privacytaken staat of valt met het beschikbaar zijn van capaciteit. Niet alles hoeft (volledig) te gebeuren door of met de privacycoördinator, maar het afgelopen jaar heeft wel geleerd dat, om privacy de aandacht te geven die de AVG van ons vergt, er meer capaciteit nodig is dan de uren die binnen de functie van de huidige coördinator beschikbaar zijn. Het gaat dan om uren voor zowel de privacy coördinatietaak als de privacy adviestaat. In de praktijk blijken proceseigenaren behoefte te hebben aan adviezen over hoe te handelen met inachtneming van de bepalingen van de AVG. Voor specialistische kwesties kan een beroep op het Juridisch Kenniscentrum bij het SCD worden gedaan, maar reguliere vragen, vaak met een juridisch karakter, moeten binnen de organisatie zelf kunnen worden afgedaan. De functie van privacycoördinator blijkt meer raakvlakken met juridische functies te hebben dan met ICT/informatieveiligheid. Een deel van de regiogemeenten heeft privacycoördinatie gecombineerd met juridische functies, en een deel met informatieveiligheidstaken. In Zwijndrecht viel uit praktische overwegingen de keus op de tweede optie, maar de ervaring leert dat de eerste effectiever is. Gezien het onvermijdelijke karakter van de taken van de privacycoördinator en het feit dat het om nieuwe wettelijke taken gaat, en dat het meer werk betreft dan vóór de daadwerkelijke inwerkingtreding van de AVG kon worden voorzien, stellen wij een beperkte formatie-uitbreiding met drie dagen per week (0,67 fte) voor. Dit vergt in 2019 een bedrag van € 30.000, en in de jaren daarna structureel € 58.000. De financiële consequenties worden, gelet op het feit dat het om de onvermijdelijke gevolgen van een nieuwe wettelijke taak gaat, opgenomen in de Eerste bestuursrapportage 2019.

Hoogachtend,

De secretaris,

De burgemeester,