



AVG Jaarrapportage 2020

NOTITIE

AAN:

5-3-2021

VAN:

Auteur

STATUS:

Ter afstemming

Op grond van artikel 38 lid 3 AVG brengt de functionaris gegevensbescherming (FG) jaarlijks verslag uit aan de gemeentesecretaris en het College van Burgemeester en Wethouders. Voor u ligt de AVG jaarrapportage 2020. In deze rapportage beschrijft de FG de stand van zaken op het gebied van de implementatie van de AVG binnen de Gemeente Breda en de wijze waarop persoonsgegevens beschermd worden.

Hoewel in 2020 belangrijke progressie is gemaakt, zijn niet alle gewenste doelen behaald. Dit komt niet zozeer door gebrek aan ambitie, maar wel door specifieke kenmerken van Breda als organisatie. Hierna ga ik daarom niet alleen in op de belangrijkste resultaten van 2020 op de grootste uitdagingen voor 2021. Maar zal ik ook specifiek duidelijk om welke 'root causes' het lastig is om de privacy ambities van Breda te realiseren.

Belangrijkste ontwikkelingen 2020

Het strategisch beleid voor gegevensbescherming is goedgekeurd. Een revisie / aanvulling op dit beleid wordt in Q1 2021 goedgekeurd.

De organisatie van privacy is verder geïnstitutionaliseerd

- Voordeel: snellere kennisontwikkeling en betere samenwerking in centrale team
- Gezamenlijke aanpak gegevensbescherming (Concern Information Security Officer) is actief, door wekelijks overleg. Ook sluit Information Security Officer als vaste deelnemer aan in privacy overleg
- Striktere scheiding FG (toezicht) en Privacy Organisatie (advies), zichtbaar 'dualisme' bij DPIA's (privacy risico analyses)
- Privacy organisatie heeft een kwaliteitsimpuls gehad. De bijdrage van Team gegevensbescherming wordt ook beter gewaardeerd door de collega's. Nadeel: door zichtbaarheid komen ook veel vragen los, wat druk legt op capaciteit Team gegevensbescherming .
- De beoogde structuur met privacy ambassadeurs in de lijn is nog niet in stelling gebracht cq effectief: de achterliggende gedachte is dat de lijn zelf verantwoordelijk is en zelf voor capaciteit moet zorgen. En dit is nog niet gebeurd.

Voor 2020 stonden een aantal structurele verbeteringen op de rol, maar deze zijn niet allemaal gerealiseerd. Als belangrijkste verbetering zijn voor een aantal privacy processen eerste werkprocessen geïmplementeerd: datalekprotocol, uitvoeren Pre-PIA / DPIA (privacy risico analyses).

Grootste uitdagingen 2021

In de jaarrapportage 2019 zijn uitgebreid de verbeterpunten behandeld. In 2020 is daar beperkt voortgang in geboekt. Hieronder is opgenomen wat de actuele status is van de in 2019 benoemde verbeterpunten.

- De basis moet op orde. Zolang er geen **overzicht is in de gegevens die verwerkt worden** en de wijze waarop dat gebeurt, is het onmogelijk een gedegen risico-inschatting te maken en de rechten van betrokkenen beter en naar behoren te borgen – *geen voortgang*
- ± Vanuit de organisatie wordt regelmatig aangegeven dat er veel behoefte is aan bewustwording. Medewerkers willen graag weten **wat de AVG voor hun werkzaamheden betekent**. Op maat gemaakte bewustwordingssessies zijn van belang om medewerkers hierin mee te nemen – *beperkt voortgang*
- ± Zonder **expertise** op het gebied van gegevensbescherming kan de Gemeente Breda persoonsgegevens onvoldoende beschermen. De Gemeente Breda dient over voldoende **capaciteit** te beschikken om aan de vraag vanuit de organisatie te voldoen – *beperkt voortgang*
- ± De **behandeling** van **AVG-verzoeken** moet beter. Uit de evaluatie van de functionaris gegevensbescherming is gebleken dat het proces, de technische ondersteuning, de inhoudelijke behandeling en de communicatie met betrokkenen beter kan – *beperkt voortgang*
- De Gemeente Breda dient over te gaan van implementatie naar vaste inbedding en strategie, waarbij meer **betrokkenheid en eigenaarschap** van de directie vereist is – *geen voortgang*
- ± Het ontbreekt op afdelingsniveau nog te veel aan helder beleid, waardoor het voor medewerkers niet duidelijk is **wat van hen verwacht wordt** – *beperkt voortgang*
- Betere **leiding en sturing** is nodig om zicht te krijgen op de werkzaamheden en om plannen daadwerkelijk tot uitvoering te brengen – *geen voortgang*

In 2020 zijn goed onderbouwde werkpakketten opgesteld om deze zaken aan te pakken, maar door een gebrek aan capaciteit / middelen bij Team gegevensbescherming zijn deze niet allemaal in 2020 gestart.

Root causes - waarom Privacy als onderwerp het in Breda moeilijk heeft

Root cause 1 - Breda is een moderne gemeente én een centrumgemeente. Zij verwerkt gegevens met tientallen partners, zowel namens zichzelf als namens andere gemeentes. In deze samenwerkingsrelaties zijn de onderlinge relaties niet altijd scherp afgebakend. Consequentie is dat de Gemeente op het punt van regievoering op gegevensbescherming tekort schiet.

Dit vertaalt zich in gebrekkig zicht op welke gegevens worden uitgewisseld, beperkte specifieke afspraken en gebrek aan sturing daarop. Beleidsambtenaren zijn niet bekend met de noodzaak om in samenwerkingsrelaties een sturingsmechanisme voor gegevensbescherming af te spreken.

Suggesties:

- Creëer zicht op samenwerkingsrelaties, met name in gevoelige domeinen zoals jeugd, veiligheid en sociaal domein

- Stel vast welke regierol Breda heeft (formeel of informeel)
- Ga na welke afspraken zijn gemaakt over gegevensbescherming en vul deze aan daar waar nodig
- Beleg de regierol binnen de afdeling die de uitwisseling aanstuurt
- Ga beleidsmatig na op welke punten de 'bastion' gedachte beleidsmatig moet worden ingewisseld voor de 'netwerkrol' gedachte
- Voorzie in middelen om veilig samen te werken (samenwerkingsomgeving, samen vergaderen, gegevens uitwisseling via mail, gegevensuitwisseling via app, ...)

Root cause 2: Breda houdt niet van richtlijnen en heeft er ook relatief weinig. Andere gemeentes vullen abstracte kaders uit de AVG aan door eigen zienswijzes te formuleren en deze door het College te laten bekrachtigen. Breda niet. Gevolg is dat keuzes op de werkvloer worden gemaakt en uitgangspunten en argumenten achteraf niet reproduceerbaar zijn. Dit is bij discussies rondom privacy belemmerend, bijvoorbeeld bij inhoudelijke discussies rondom grondslag & doelbinding, dataminimalisatie (wat hebben we nodig en waarom) en rollen & verantwoordelijkheden op het gebied van privacy.

Suggesties:

- Voorkom dat discussies ontstaan door gebrek aan kennis of perspectief om dit aan te pakken. Neem landelijke voorbeeld richtlijnen als uitgangspunt (bv WMO, RIEC, ondermijning) en adopteer deze. Pas de uitvoering aan.
- Maak gebruik van netwerken en ervaringen van andere gemeentes (binnen en buiten Breda, VNG) en zoek naar protocollen en best-practices.
- Stel vast dat de lijn verantwoordelijk is voor het definiëren van richtlijnen. Team gegevensbescherming heeft hierbij een faciliterende rol.

Root cause 3: Bredase ambtenaren houden niet van gedoe. Men wil vooral weten wat van hen wordt verwacht en hoe ze met zo min mogelijk gedoe en inspanning toch kunnen blijven doen wat men gewend is. Men ziet de verantwoordelijkheid voor gegevensbescherming niet als onderdeel van het eigen takenpakket, wat zich vertaalt in gebrekkige kennis en kunde.

Suggesties:

- Betrek team gegevensbescherming bij discussies over richtlijnen en protocollen.
- Voer samen DPIA's (privacy risico analyses) uit
- Bespreek cases en deel deze, eventueel ook met andere gemeentes
- Stel vast dat de lijn verantwoordelijk is voor het uitvoeren van DPIA's. Team gegevensbescherming heeft hierbij een faciliterende rol.

Root cause 4: De toon van de top is dat Breda graag de ruimte zoekt en best wat risico wil nemen, dit wordt ook zo in de praktijk gebracht in het dagelijkse werk. Daar waar risico's worden genomen, kunnen ook fouten worden gemaakt. De huidige inrichting van gegevensbescherming past daarbij: de kans dat er in de Gemeente Breda dingen fout gaan met Gegevensbescherming is, naar mijn inschatting, groter dan bij andere Gemeentes. De top zou veel genuanceerder kunnen zijn in wat wordt

bedoeld met 'we willen risico nemen', zodat ook de ondergrens van gegevensbescherming beter kan worden bewaakt.

Suggesties:

- Nuanceer uitgangspunt in 'het nemen van verantwoorde risico's' als het gaat over de verwerking van persoonsgegevens
- Voer DPIA's uit en bepaal op basis van de uitkomsten ervan welke risico's passend zijn
- Laat de afweging over risico's maken door de mensen die ook het mandaat hebben voor eventuele consequenties ervan
- Maak risico's expliciet door de kans en impact zoveel mogelijk te kwantificeren, beleg ze bij de lijnverantwoordelijke en bewaak / stuur hier op