Raadsinformatiebrief

Onderwerp	**: Stand van zaken Informatieveiligheid (Privacy & Security)**
Aanleiding	**: Afspraken in de commissie van september 2021**
Datum	**: 17 januari 2022**
Portefeuillehouder	**: J.G.A. Paans**
Schrijver	**: N. Sijrier**

Geachte leden van de gemeenteraad,

U ontvangt deze raadsinformatiebrief 'Stand van zaken Informatieveiligheid'. Bij de bespreking van de RIB 'Rapportage FG Privacy' jongstleden september 2021 is door de commissie gevraagd om een RIB met daarin de actuele stand van zaken. Uiteraard voldoe ik graag aan dat verzoek.

Inleiding
De voorgaande RIB is naar aanleiding van de jaarlijkse rapportage van de FG rondom de stand van zaken wat betreft privacy opgesteld. Deze rapportage is zogezegd een 'peilstok' waarin onze FG (Extern, onderdeel van de Servicegemeente Dordrecht) de stand van zaken opmaakt rondom het privacy beleid en uitvoering daarvan. In deze RIB wil ik niet zozeer ingaan op het afvinken van de bevindingen van de FG, maar meer op de lijn en de structuren die we (mede) naar aanleiding van de jaarlijkse FG rapportage aan het uitvoeren zijn. Daarnaast bevat deze RIB ook een terugkoppeling van de stappen die we aan het zetten zijn op het gebied van informatiebeveiliging. Beide onderwerpen komen samen in de term 'informatieveiligheid'.

Context
Ook in 2021 is er weer landelijke publiciteit geweest rondom datalekken, waarbij de 'Functie elders' aantekeningen over Pieter Omtzigt wellicht de meest in het oog springende te noemen is. Datalekken zijn uiteindelijk het resultaat van falend menselijk handelen (zoals bij Omtzigt), het niet afdoende af kunnen schermen van gegevens (techniek) of het bewust stelen van gegevens (hacking). De GDPR is de Europese wet die regelt dat privacy van uw en mijn gegevens goed wordt geregeld. Deze is in Nederland vertaald in de AVG, welke sinds mei 2018, na een overgangsperiode, actief is.

Onze gegevens en informatie zijn goud waard. Niet alleen voor overheden van andere landen, maar ook voor criminelen die uw en mijn gegevens dan weer gebruiken voor bankfraude, phishing en andere criminaliteit. Om nog maar niet te spreken over het verdienmodel van bedrijven als Google en Facebook die op basis van data die ze over ons verzamelen miljoenenwinsten behalen. Onze gegevens dienen daarom goed beschermd te worden.

In 2020 is de Baseline Informatieveiligheid Overheid ingevoerd. Daarin wordt uitgewerkt aan welke voorwaarden onze informatiebeveiliging moet voldoen. Er liggen veel raakvlakken en paralellen tussen de Baseline en de AVG. In de dagelijkse praktijk gaan deze dan ook vaak hand in hand met elkaar op.

Huidige stand van zaken
De invoering van een Wet gaat meestal gepaard met een aantal golfbewegingen: Eerst zorgen dat je aan de wettelijke verplichting voldoet, zorgen dat je processen daarop ingericht zijn en als laatste zorgen dat de governance (toezicht en toetsing) opgezet wordt.

Voor wat betreft de AVG hebben we de afgelopen jaren gezien dat er hard is gewerkt om te zorgen dat we aan de 'letter van de wet' voldoen: Beleid is geformuleerd, Registers zijn ingericht en overeenkomsten rondom de verwerking van data zijn door de gemeente aangegaan met partners,

toeleveranciers en afnemers. Daarnaast is de organisatie aan de slag gegaan met de inrichting van de processen rondom de AVG, en de aanpassing van de bestaande processen. Ook is als onderdeel van dit onderwerp de bewustwording opgepakt. Zo is er afgelopen najaar een WIPI week georganiseerd waarin security en privacy centraal stonden. Met quizzen en een AVG Safari (er waren in het pand situaties gemaakt waarbij privacy mogelijk in gevaar was) is er aandacht geweest voor de privacy aspecten van het dagelijkse werkveld. Op het laatste deelvlak, de governance, zijn nog weinig activiteiten ontplooid. Dat is dan ook een speerpunt de komende periode.

Wat betreft de uitvoering van Baseline Informatieveiligheid Overheid zijn we nog volop aan de slag met de implementatie van de baseline. Voor Alblasserdam betekent dat, dat we vooral toezicht houden op de implementatie van maatregelen die het SGD (Service Gemeente Dordrecht) neemt.

Voorbeelden daarvan zijn het implementeren van het wachtwoordbeleid, uitvoeren van de juiste backup maatregelen in het netwerk, zorgen voor het juiste niveau van Firewalling, etc. Door het gezamenlijk in de regio uitvoeren van de ICT taken behalen we hier vooral slagkracht doordat er een professionele organisatie kan staan en daarnaast behalen we schaalvoordeel doordat er veel gezamenlijk wordt uitgevoerd.

Ook zijn we lokaal begonnen met toerusting en bewustwording van collega's. Daar waar nodig passen we de processen aan. Voor de governance is nog geen aandacht geweest.

Recapitulatie

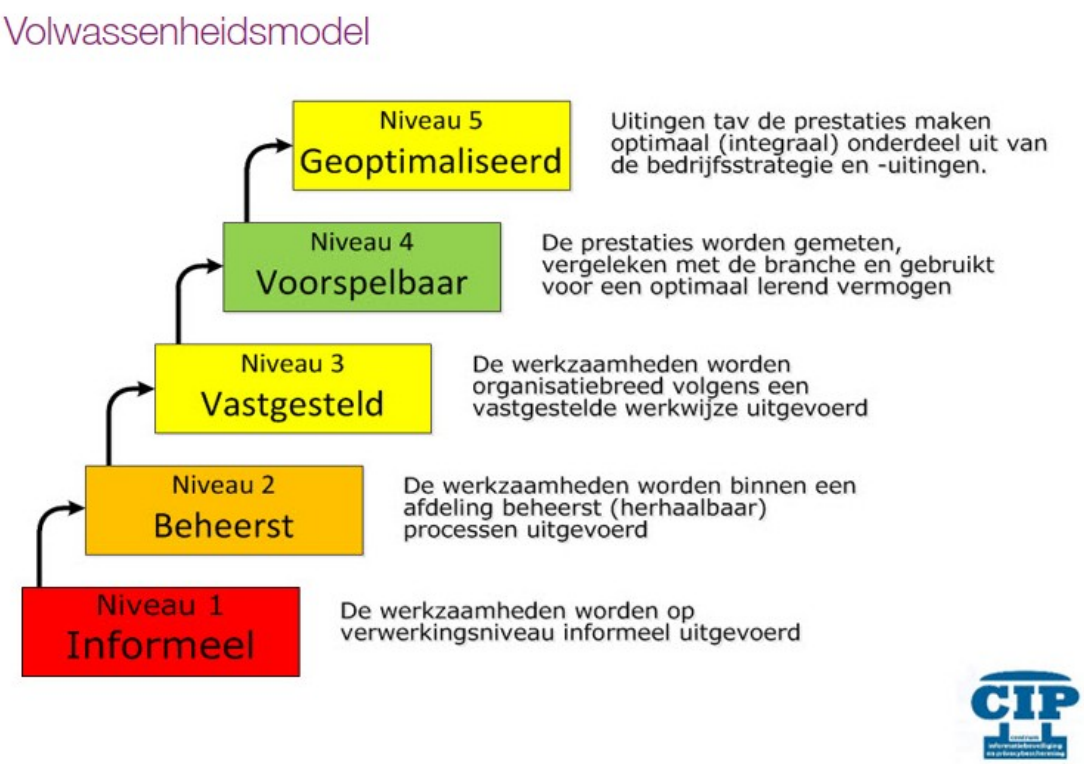
Het jaarplan voor 2021 is slechts deels uitgevoerd. Oorzaken hiervoor zijn met name te vinden in een onderbezetting qua personele uren (in 2021 hebben we door ziekteverzuim minder uren kunnen besteden aan het aandachtsgebied van Informatiemanagement, Privacy en Security) waardoor de uitvoering beperkt bleef tot de meest urgente operationele zaken, zoals het uitvoeren van (verplichte) gegevensbeschermings-effectrapportages, bewustwording en advisering rondom privacy en security.

Vanaf augustus 2021 is de formatie weer op volle sterkt. Hierdoor kwam er weer meer ruimte om uitvoering te geven aan de plannen rondom privacy en security. De COVID-19 pandemie heeft ook hier wel zijn weerslag gehad, met name op het gebied van bewustwording van het personeel.

Hoe verder

Zoals al eerder verwoord is de mars richting wel duidelijk. Verdere bewustwording, toerusting van collega's en het implementeren van Governance, zowel voor Privacy als voor information security.

Wat betreft de implementatie van de Baseline IO ligt er ook nog operationeel werk zoals het in kaart brengen of de juiste beleidslijnen en uitvoerende zaken zijn geïmplementeerd. Om de werkzaamheden richting te geven, is het belangrijk om een doel, een stip op de horizon te hebben. Dit doen we door de mate van volwassenheid van de organisatie rondom deze onderwerpen vast te stellen (de 'Ist') en ook het gewenste niveau van volwassenheid te definiëren (de 'Soll'). Bij zowel de AVG trajecten als de Security trajecten wordt veel het volgende volwassenheidsmodel gehanteerd:



We zijn gestart met een 0-meting om het huidige niveau van volwassenheid te bepalen. Daarbij hoort ook een goed gesprek over het gewenste niveau van volwassenheid. Zo doende komen we tot een werkpakket dat we vertalen in projecten voor de 3 aandachtsgebieden (Processen, bewustwording en Governance) om zodoende de volwassenheid van de organisatie naar een hoger plan te tillen. Hierbij funderen we ons op handvaten en praktijkvoorbeelden die ons aangereikt worden door het Centrum Informatiebeveiliging en Privacybescherming (CIP)[1].

Tot slot

Er is veel informatie te vinden over de AVG en de Baseline Informatieveiligheid Overheid. Als bijlagen treft u een tweetal informatiedocumenten aan rondom deze onderwerpen, met achtergrondinformatie. Daarnaast voegen we ter informatie ook het (concept) Informatieplan 2022 bij. Het voornemen is om u in het najaar van 2022 via een RIB opnieuw te informeren rondom deze onderwerpen.

Met vriendelijke groet,
burgemeester en wethouders,

de secretaris
S. van Heeren

de burgemeester
J.G.A. Paans

[1] https://www.cip-overheid.nl

Bijlage 1: Achtergrond informatie AVG

De Autoriteit Persoonsgegevens heeft in één webpagina de belangrijkste onderwerpen rondom de AVG en overheden samen gevat. Deze vindt u hieronder weergegeven. De originele pagina vindt u hier: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/overheid/overheid-de-avg

Overheid & de AVG

Overheidsorganisaties beschikken over grote hoeveelheden – vaak gevoelige – persoons-gegevens. Mensen zijn bovendien meestal verplicht om hun gegevens aan de overheid af te staan. Daarom moet iedereen erop kunnen vertrouwen dat u als overheidsorganisatie uiterst zorgvuldig met hun gegevens omgaat.

Dat betekent dat u bijvoorbeeld:

- altijd de juiste wettelijke basis nodig heeft om gegevens te verwerken, vooral als u gegevens uitwisselt
- niet meer persoonsgegevens mag verwerken dan noodzakelijk
- de gegevens goed moet beveiligen.

Deze verplichtingen zijn niet veranderd door de komst van de Algemene verordening gegevensbescherming (AVG). Maar de AVG heeft ook nieuwe verantwoordelijkheden met zich meegebracht.

Verplichtingen AVG

Sinds de AVG zijn er de volgende nieuwe verplichtingen:

Functionaris gegevensbescherming
Alle overheidsorganisaties moeten een functionaris gegevensbescherming (FG) hebben.

Data protection impact assessment (DPIA)
Wilt u gegevens gaan verwerken, maar levert dit een hoog privacyrisico op? Dan moet u eerst een data protection impact assessment (DPIA) doen.

Verantwoordingsplicht
U heeft een verantwoordingsplicht. Dit houdt in dat u moet kunnen aantonen dat uw verwerkingen aan de AVG voldoen.

In de AVG staat een aantal verplichte maatregelen waarmee u aan uw verantwoordingsplicht voldoet, waaronder:

Verwerkingsregister
U bent vrijwel altijd verplicht om een verwerkingsregister op te stellen.

Privacybeleid
U kunt verplicht zijn om een privacybeleid op te stellen. Dit hangt af van welke soort gegevens uw organisatie verwerkt en op welke schaal.

Datalekregister
U moet een datalekregister bijhouden. Hierin registreert u alle datalekken die zich in uw organisatie hebben voorgedaan. Ook de datalekken die u niet hoeft te melden.

Archivering & de AVG
Als overheidsorganisatie bent u op grond van de Archiefwet verplicht om bepaalde informatie blijvend te bewaren. In deze informatie staan vaak persoonsgegevens. Daarom heeft u ook te maken met de AVG. Zie verder: Archivering door de overheid.

Bijlage 2: Achtergrond informatie Baseline Informatieveiligheid Overheid

De Baseline IO is de opvolger van de BIG (baseline Informatieveiligheid Gemeenten). Sinds 2020 is er dus één richtlijn voor de gehele overheid. Er wordt dus niet meer gekeken naar het type organisatie, maar naar de gevoeligheid en vertrouwelijkheid van gegevens, en de maatregelen worden daar op afgestemd. Daarmee is het dan dus ook mogelijk om een specifieke aanpak te maken voor bepaalde typen gegevens.

De baseline zelf bestaat uit een groot aantal (ongeveer 100) richtlijnen. Als deze op een juiste wijze zijn geïmplementeerd, voldoe je aan de minimale eisen rondom security.

Met de introductie van de Baseline is er ook een classificatie systeem geïntroduceerd om de gevoeligheid van informatie in te kunnen delen. Hoe hoger de classificatie, hoe stringenter de veiligheidsmaatregelen.

Het voert te ver om in deze RIB de complete werking van de Baseline Informatieveiligheid Overheid te duiden. Mocht u meer informatie willen over de Baseline Informatieveiligheid Overheid kunt u de volgende website van de IBD/VNG raadplegen:
https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

De VNG publiceert ieder jaar een dreigingsbeeld afgestemd op de nederlandse gemeenten. Deze voeg ik bij ter achtergrond informatie., omdat deze in een beknopte vorm weergeeft de problematieken die op dit moment actueel zijn.