2021

Jaarrapportage 2021

GEGEVENSBESCHERMING IN DE GEMEENTE BEVERWIJK

Helga Timmer, Privacy Officer
Paul Bakker, Chief Information Security Officer
Teun de Heer, Functionaris voor Gegevensbescherming
Gemeente Beverwijk
April 2022

Management samenvatting

Sinds de invoering van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018, is informatiebeveiliging en privacy in de gemeente Beverwijk een belangrijk aandachtspunt. In 2018 is het fundament gelegd voor de implementatie van de AVG. De structurele borging van privacy en gegevensbescherming binnen de organisatie is in 2019 gestart. Veel van de beoogde doelen zijn in dat jaar ook behaald. De afgelopen jaren stonden in het teken van een ingrijpende wijziging in de organisatiestructuur, die per 1 april 2020 is ingevoerd.

In 2021 is er voortgebouwd op het basis die in de voorgaande jaren is gelegd. Belangrijk hierin zijn de procesbeschrijvingen, die het mogelijk maken om de gegevensstromen binnen de gemeente zichtbaar te maken en te beheersen. Daarin zijn grote vorderingen gemaakt.

Ook dit jaar is voor een aantal processen een Data Protection Impact Assessment (DPIA) uitgevoerd: op het gebruik van Bodycams door BOA's en op het gemeentelijk cameratoezicht. Dit levert een belangrijke bijdrage aan het beheersbaar maken van de risico's die het verwerken van persoonsgegevens met zich mee brengt.

De hack bij IJmond Werkt! In september 2021 heeft veel tijd en aandacht gevraagd. IJmond Werkt! voert voor een aantal gemeenten, waaronder Beverwijk, het deel 're-integratie' van de Participatie wet uit. Veel persoonlijke gegevens van cliënten zijn door de hackers op internet gezet. De cliënten zijn in een aantal brieven over de gevolgen van de hack geïnformeerd. Zij ontvingen eerst een algemene brief; in een later stadium is iedereen op de hoogte gebracht van de gegevens die van hun persoonlijk zijn gelekt.
De afhandeling van de crisis onder aansturing van de veiligheidsregio is inmiddels geëvalueerd. De afhandeling van de hack vanuit het perspectief van de gemeentelijke organisatie is nog niet geëvalueerd. Daar is wel behoefte aan. Als de gemeente onverhoopt opnieuw met een dergelijk incident te maken krijgt is het van belang dat er vanaf dag 1 helderheid is ten aanzien een aantal onderwerpen, waaronder de inrichting van de crisisorganisatie, risicoanalyse, communicatie en de aansturing/ zeggenschap.

Evenals afgelopen jaren is de stand van zaken op het gebied van gegevensverwerking opnieuw in kaart gebracht aan de hand van het Borgingskader Gegevensbescherming en Privacy zoals dit is opgesteld door de Informatie Beveiligingsdienst van de VNG. Ten opzichte van vorig jaar zijn weer concrete vorderingen gemaakt. Daarnaast is er een pré audit uitgevoerd op de gegevensverwerking door BOA's in het kader van de Wet politiegegevens (Wpg).

In 2022 zal verder worden gewerkt aan het implementeren van maatregelen die volgen uit de BIO en het VNG borgingskader (AVG). Daarbij zal de nadruk liggen op het verder uitwerken van de werkprocessen, het versterken van de IT-infrastructuur met het oog op digitale veiligheid en het vergroten van de bewustwording op dit punt bij medewerkers. Ook zullen de aanbevelingen uit het externe Wpg-auditrapport worden opgepakt.

Inhoudsopgave

Inleiding

Sinds de invoering van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018, is informatiebeveiliging en privacy in de gemeente Beverwijk een belangrijk aandachtspunt. In 2018 is het fundament gelegd voor de implementatie van de AVG. De structurele borging van privacy en gegevensbescherming binnen de organisatie is in 2019 gestart. Veel van de beoogde doelen zijn in dat jaar ook behaald. De afgelopen jaren stonden in het teken van een ingrijpende wijziging in de organisatiestructuur, die per 1 april 2020 is ingevoerd.

In 2021 is er voortgebouwd op het basis die in de voorgaande jaren is gelegd. Belangrijk hierin zijn de procesbeschrijvingen, die het mogelijk maken om de gegevensstromen binnen de gemeente zichtbaar te maken en te beheersen. Daarin zijn grote vorderingen gemaakt.

De afgelopen jaren is een aantal organisaties in het publieke domein doelwit geweest van hackers. Dit heeft bij verschillende organisaties, zoals bijvoorbeeld de gemeenten Lochem en Hof van Twente tot grote problemen geleid. In 2021 is IJmond Werkt! gehackt. Omdat IJmond Werkt! het deel ‘re-integratie’ van de Participatiewet (mede) voor de gemeente Beverwijk uitvoert, heeft dit een flinke impact gehad op de gemeente. Het onderwerp ‘cyberveiligheid’ staat dan ook hoog op de agenda.

Dit jaarverslag geeft een algemeen beeld van de stand van zaken op het gebied van Privacy en Informatieveiligheid in de gemeente Beverwijk en de vooruitgang die is geboekt ten aanzien van privacy management.

Hoofdstuk 1 - Stand van zaken

1.1 Privacy beleid

Het privacy beleid is op hoofdlijnen geformuleerd, vastgesteld en gepubliceerd op de website van de gemeente. Ten aanzien van sommige specifieke beleidsterreinen, zoals bijvoorbeeld het sociaal domein is dit ook meer in detail uitgewerkt. Dit is belangrijk, omdat op basis van de gekozen uitgangspunten vervolgens in de praktijk duidelijke keuzes kunnen worden gemaakt. Het is van belang dat het privacy beleid de komende jaren verder wordt uitgewerkt.

Het beleid is afgelopen jaar niet uitgebreid in de praktijk getoetst. In 2022 zal daar meer nadruk op komen te liggen.

1.2 Verwerkingsregister

Op grond van artikel 30 lid 1 AVG is de gemeente verplicht een 'Register van de verwerkingsactiviteiten' bij te houden. Dit register:

- geeft een systematisch overzicht van de informatiestromen en de partijen die daarbij zijn betrokken;
- bevat de informatie die nodig is voor risicoanalyse van informatiesystemen;
- is een hulpmiddel bij het uitvoeren van AVG-verzoeken, omdat de categorieën van betrokkenen er in zijn opgenomen.

De verwerkingen zijn voor de gemeente Beverwijk in kaart gebracht en opgenomen in een register. Om te komen tot een systematisch overzicht van alle relevante gegevens zal in 2022 i-navigator worden ingericht. Het is dan nog beter mogelijk om de informatie die betrekking heeft op privacy te integreren in de documentatie op het gebied van informatieveiligheid.

1.3 Rechten van betrokkenen

De AVG heeft als belangrijke doelstelling, dat de betrokkene zoveel mogelijk controle houdt over zijn of haar persoonsgegevens. De betrokkene heeft dan ook een aantal rechten op grond van de AVG, zoals het recht om de eigen gegevens in te zien, een kopie daarvan te ontvangen, eventuele onjuistheden te laten corrigeren of de verwerking door de verantwoordelijke te beperken of zelfs te laten wissen. Deze rechten zijn vanzelfsprekend aan een aantal beperkingen onderworpen.

In de gemeente Beverwijk zijn in 2021 verschillende verzoeken binnengekomen. Een viertal verzoeken betrokkenen heeft verzocht om verwijdering van hun persoonsgegevens. Deze verzoeken zijn ingewilligd. Ook een tweetal verzoeken om inzage in de hun betreffende gegevens zijn (deels) ingewilligd. Eén verzoek is doorgezonden naar een andere gemeente en is ten aanzien van Beverwijk buiten behandeling gelaten.

1.4 Datalekken

Ook als er veel aandacht wordt besteed aan informatiebeveiliging kan het voorkomen dat vertrouwelijke gegevens terecht komen bij onbevoegden, verloren gaan of dat de gemeente de controle over de gegevens (tijdelijk) verliest.

Er wordt gesproken over een beveiligingsincident als er sprake is van een inbreuk op de beveiliging van vertrouwelijke gegevens. Als het risico bestaat dat de privacy van betrokkenen ook daadwerkelijk is geschaad moet het incident ook worden gemeld bij de Autoriteit Persoonsgegevens (AP) en wordt er gesproken van een datalek.

In 2021 zijn er 10 situaties gemeld waarbij er mogelijk sprake was van een beveiligingsincident. Deze situaties zijn allemaal onderzocht. Van alle incidenten zijn de onderzoeksverslagen beschikbaar. Indien nodig is overlegd door de PO met de CISO en/of de FG om het risico van de inbreuk in kaart te brengen. In 7 gevallen ging het om een datalek dat moest worden gemeld bij de Autoriteit Persoonsgegevens (AP).

In september heeft er een hack plaatsgevonden bij IJmond Werkt! IJmond Werkt! voert voor een aantal gemeenten, waaronder Beverwijk, het deel re-integratie van de Participatie wet uit. Veel persoonlijke gegevens van cliënten zijn door de hackers op internet gezet. De directie van IJmond Werkt! heeft direct FoxIT gevraagd een onderzoek in te stellen naar de aard en omvang van de inbreuk. Nadat de hackers een deel van de persoonsgegevens op internet hebben gepubliceerd is er een crisisteam gevormd onder aansturing van de Veiligheidsregio Kennemerland. In de loop van oktober is het crisisteam weer opgeheven en heeft afstemming tussen IJmond Werkt! en de vier gemeenten plaatsgevonden via een wekelijks afstemmingsoverleg.

De cliënten van IJmond Werkt! zijn in een aantal brieven over de gevolgen van de hack geïnformeerd. Zij ontvingen eerst een algemene brief; in een later stadium is iedereen op de hoogte gebracht van de gegevens die specifiek betreffende hun persoon zijn gelekt.

De afhandeling van de crisis onder aansturing van de veiligheidsregio is inmiddels geëvalueerd. De afhandeling van de hack vanuit het perspectief van de gemeentelijke organisatie is nog niet geëvalueerd. Daar is wel behoefte aan. Als de gemeente onverhoopt opnieuw met een dergelijk incident te maken krijgt is het van belang dat er vanaf dag 1 helderheid is ten aanzien een aantal onderwerpen, waaronder de inrichting van de crisisorganisatie, risicoanalyse, communicatie en de aansturing/ zeggenschap.

IJmond Werkt! Heeft een opbouwplan opgesteld om de ICT infrastructuur en de werkprocessen op een hoger plan te brengen. De uitvoering van dit plan zal gedurende 2022 door de gemeente worden gevolgd.

1.5 Data Protection Impact Assessment

Een Data Protection Impact Assessment (DPIA) is een procedure waarbij systematisch de mogelijke gevolgen worden onderzocht van een (nieuw of bestaand) informatiesysteem, een proces of manier van werken, bekeken vanuit het perspectief van de bescherming van persoonsgegevens. In de AVG is dit begrip vertaald als ‘gegevensbeschermingseffectbeoordeling’. De verplichting om voor risicovolle verwerkingen een DPIA uit te voeren is in de plaats gekomen van de meldingsplicht die was voorgeschreven in de Wbp. Als instrument is de DPIA niet nieuw. Vaak wordt nog de oude afkorting gebruikt: PIA (Privacy Impact Assessment).

De AVG schrijft in artikel 35 lid 1 voor dat een DPIA verplicht is als de verwerkingen ‘waarschijnlijk een groot risico inhouden voor de rechten en vrijheden van betrokkenen’. Hierbij moet voornamelijk worden gelet op de volgende vier aspecten:

- de aard van de verwerking (bijvoorbeeld bijzondere persoonsgegevens);
- de reikwijdte van de verwerking (bijvoorbeeld samenwerking met ketenpartners);
- de context (bijvoorbeeld sociaal domein);
- de doeleinden (bijvoorbeeld bestuurlijke aanpak criminaliteit).

Bijzondere aandacht is vereist wanneer er sprake is van inzet van nieuwe technologieën.

Het is onrechtmatig om een nieuw proces te starten of ingrijpend te wijzigen zonder voorafgaand een DPIA uit te voeren. In de jaren tot 2020 zijn er DPIA's uitgevoerd op de processen:

- Leerplicht
- Bezwaarschriftencommissie
- Drank & horecavergunning
- Leerlingenvervoer
- Identificatieapparatuur balie
- Cameratoezicht drie straatjes
- WMO
- Ziekteverzuim
- Schuldhulpverlening
- Uitkering Bijstand
- Sociale wijkteams
- Verlenging cameratoezicht drie straatjes
- Evaluatie DPIA Leerlingenvervoer
- Wvggz
- Vroegsignalering schulden
- Ondermijning

In 2021 is een aantal DPIA's uitgevoerd, namelijk:

- Gebruik Bodycam's door BOA's Handhaving.
- Cameratoezicht centrum.

Het is van belang dat binnen de gemeente aandacht blijft voor het tijdig uitvoeren en evalueren van DPIA's in die gevallen waarin de wijze waarop persoonsgegevens worden verwerkt in meer of mindere mate wordt gewijzigd en dit voor betrokkenen leidt tot risico's voor de persoonlijke levenssfeer.

1.6 Wpg

Sinds 1 maart 2019 valt de gegevensverwerking door Bijzonder Opsporingsambtenaren (BOA's) in het kader van hun handhavingstaken onder de Wet Politiegegevens (Wpg). In 2021 is een pré audit Wpg uitgevoerd voor Beverwijk voor de domeinen Handhaving, Leerplicht en Sociale Recherche. Zoals als werd verwacht leverde dit een aantal aanbevelingen op die medio 2022 zullen worden opgevolgd. Voor de verplichte externe audit die volgt uit de Wpg heeft de Autoriteit Persoonsgegevens (AP) landelijk uitstel verleend tot eind 2022. De gemeente Beverwijk heeft dan ook een goede uitgangspositie om aan deze verplichting te voldoen en de daaruit voortvloeiende maatregelen te implementeren.

Hoofdstuk 2 – Borgingskader Gegevensbescherming en Privacy

2.1 Algemeen

VNG Realisatie heeft criteria ontwikkeld om de Algemene Verordening Gegevensbescherming te vertalen naar een Borgingskader Gegevensbescherming en Privacy, met het oog op de gemeentelijke organisatie. Hiermee beoogt VNG Realisatie gemeenten concrete handvatten te bieden om een goede omgang met persoonsgegevens in de gehele organisatie te waarborgen.

In de gemeente Beverwijk is de stand van zaken op het gebied van gegevensverwerking in 2018, 2021 en in 2021 getoetst aan dit borgingskader. In dit jaarverslag zal niet worden ingegaan op details. Hiervoor wordt verwezen naar de respectievelijke rapportages. In dit jaarverslag zal alleen worden gekeken naar de algemene lijn, met een korte toelichting.

2.2 Structuur borgingskader

Voor het VNG Borgingskader Gegevensbescherming en Privacy zijn 65 criteria opgesteld, verdeelt over 7 categorieën. Deze categorieën dekken gezamenlijk min of meer alle aspecten die samenhangen van gegevensbescherming. Alle criteria dienen in onderlinge samenhang te worden gelezen. De criteria verwijzen ook naar relevante criteria uit andere categorieën. Alle criteria tezamen beschrijven de ‘geborgde situatie’ voor een gemiddelde gemeente.

De categorieën zijn:

- beleid;
- processen;
- organisatorische inbedding;
- rechten van betrokkenen;
- samenwerking;
- beveiliging;
- verantwoording.

De criteria zijn vervolgens nader gespecificeerd in 189 maatregelen. Per maatregel is beoordeeld of, en in welke mate, de gemeente voldoet. Onderstaande beoordelingen zijn mogelijk:

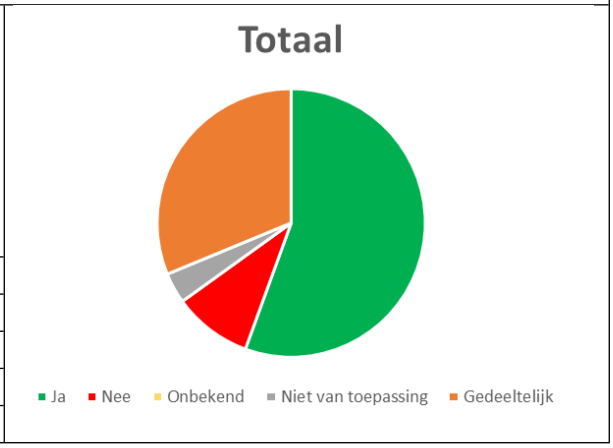
- Onbekend: het is niet bekend of de gemeente voldoet aan deze maatregel.
- Ja: de gemeente voldoet aan de genoemde maatregel.
- Nee: de gemeente heeft deze maatregel nog niet geïmplementeerd.
- Gedeeltelijk: de gemeente heeft de maatregel gedeeltelijk geïmplementeerd.

Niet van toepassing: de maatregel is niet van toepassing voor de gemeente.

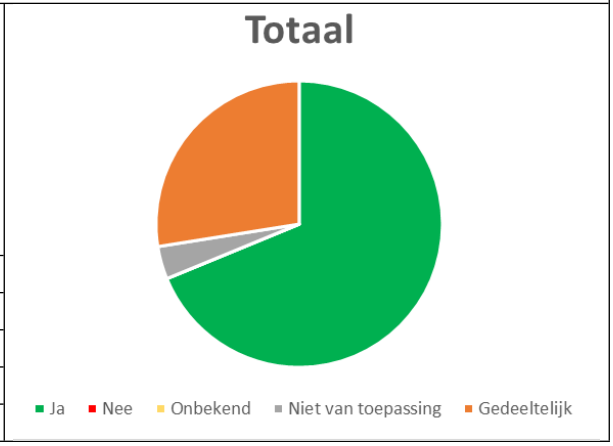
2.3 Score borgingskader

Zoals aangegeven is de inrichting van het privacy management in de gemeente Beverwijk getoetst in 2018, 2020 en 2021. In dit jaarverslag zijn ter vergelijking de totaalscores opgenomen over de jaren 2020 en 2021.

Totaalscore 2020		
Resultaat		**Maatregelen**
Ja		105
Nee		18
Onbekend		0
Niet van toepassing		7
Gedeeltelijk		59



Totaalscore 2021		
Resultaat		**Maatregelen**
Ja		130
Nee		0
Onbekend		0
Niet van toepassing		7
Gedeeltelijk		52



Ten opzicht van vorig jaar is het aantal maatregelen dat is geïmplementeerd verder is gestegen. Bijna 70% van de maatregelen staat op groen. Daarnaast is met de implementatie van de overige maatregelen minimaal een start gemaakt. Een deel van de maatregelen heeft betrekking op het in kaart brengen van de gegevensstromen, zowel binnen de gemeente als tussen gemeente en derde partijen. Ook moet er nog aandacht worden besteed aan organisatorische en technische maatregelen op het gebied van gegevensbeveiliging en monitoring.

2.4 Plannen voor 2022

In 2022 zal verder worden gewerkt aan het implementeren van maatregelen die volgen uit de BIO en het VNG borgingskader (AVG). Daarbij zal de nadruk liggen op het verder uitwerken van de werkprocessen, het versterken van de IT-infrastructuur met het oog op digitale veiligheid en het vergroten van de bewustwording op dit punt bij medewerkers. Ook zullen de aanbevelingen uit het externe Wpg-auditrapport worden opgepakt. Daarnaast zal het opgestelde privacy beleid en procedure datalekken waar nodig worden geactualiseerd.