Hoogheemraadschap van Rijnland

Jaarverslag 2020 van de Functionaris Gegevensbescherming

Versie: 1.1
Datum: Januari 2021
Corsanr : 21.003597

Jaarverslag FG 2020

Inleiding

Ieder jaar maakt de Functionaris Gegevensbescherming (FG) van Rijnland een jaarverslag over de stand van zaken met betrekking tot Privacy en het naleven van de Algemene Verordening Gegevensbescherming (AVG) in het voorafgaande jaar. In 2020 is het eerst jaarverslag gemaakt over 2019. Nu ligt het tweede jaarverslag voor, dat 2020 beslaat.

Omdat formeel het dagelijks bestuur de eindverantwoordelijke is, gaat dit jaarverslag na bespreking met de Directie ook naar de portefeuillehouder Privacy en in overleg met haar daarna naar D&H.

Voornemens uit het jaarverslag 2019

Het jaarverslag van vorig jaar eindigde met:

Hoe verder: acties voor 2020 en aanbevelingen voor de toekomst.

Voor 2020 staan de volgende zaken op de agenda om uit te voeren:

- *Uitvoeren van het Awareness-programma (samen met Informatieveiligheid) gedurende heel 2020;*
- *Update maken van het Privacy-beleid;*
- *Uitvoeren van Privacy Impact Assessments (PIA's). (deze worden ook wel aangeduid als DPIA (data protection impact assesments) Dergelijke assessments zijn verplicht als er in een bepaald proces veel persoonsgegevens en/of bijzondere persoonsgegevens worden verwerkt. In 2019 is ervoor gekozen eerst de BIA's (business impact assessments) zoals voorgeschreven in de Baseline Informatieveiligheid voor Overheden (BIO) voor informatieveiligheid uit te voeren en de organisatie nog niet te belasten met het uitvoeren van de PIA's.*
  In 2020 doen we dat voor minimaal drie processen wel:
  - *Cameratoezicht/fysieke beveiliging gebouwen (wettelijk aangewezen voor verplichte PIA);*
  - *Het instroom-doorstroom-uitstroomproces (hierin worden veel én bijzondere persoonsgegevens verwerkt);*
  - *Het vergunningen- en meldingenproces waar het zaaksysteem 'In Proces' voor wordt gebruikt (persoonsgegevens van burgers).*
- *Verder werken aan het implementeren van Privacy by Design en Privacy by Default;*
- *Aanschaf en implementatie van ISMS tooling (voor IB en Privacy).*

In dit jaarverslag kijk ik terug op deze acties en aanbevelingen en bespreek de stand van zaken.

Organisatie Privacy bij Rijnland

FG en kernteam

Bij Rijnland werkt een Functionaris Gegevensbescherming (ca. 0,5 fte) samen met een Kernteam Privacy (twee juristen, een Security officer, een data-architect, een communicatiemedewerker en een beheerder verwerkingenregister, allen voor een zeer beperkt deel van hun totale aanstelling). Gezamenlijk zorgen zij voor het begeleiden van Rijnlanders bij het voldoen aan de AVG, het beantwoorden van vragen, het onderzoeken van Privacy-meldingen uit Topdesk en het al dan niet melden daarvan bij de Autoriteit Persoonsgegevens (AP) etc. Daarnaast heeft dit team gezorgd voor de aanwezigheid van een verwerkingenregister en standaarden voor verwerkersovereenkomsten en

mede-verantwoordelijken-overeenkomsten en verzorgt het team voorlichtingsbijeenkomsten (op verzoek).

Voor het voldoen aan de Privacy-regels uit de Wet Politiegegevens (Wpg) zijn twee medewerkers vanuit Handhaving benoemd als Privacy-contactpersoon (privacy functionaris) voor politie en justitie.

Lijnorganisatie

Vanuit de lijnorganisatie zijn contactpersonen Privacy aangewezen (afspraak 2020 was: twee personen per cluster + een persoon uit de staven). Deze contactpersonen vergaderen één keer per zes weken met de FG en zijn eerste aanspreekpunt voor hun cluster voor vragen over Privacy. Per 1 januari 2021 zijn de clusters opgeheven en zullen afspraken moeten worden gemaakt welke teams een contactpersoon vertegenwoordigt.

De lijnorganisatie (i.c. de teamleiders) is verantwoordelijk voor het naleven van de AVG en dus voor het actueel houden van het verwerkingenregister, het afsluiten van de juiste verwerkersovereenkomsten wanneer derden met persoonsgegevens van Rijnland werken en het tijdig doen van meldingen van (vermoedelijke) datalekken.

Volwassenheidsniveaus

Bij Informatieveiligheid en Privacy wordt landelijk gewerkt met 5 niveaus van volwassenheid waarop een organisatie functioneert.

Bij het nulonderzoek dat eind 2018 is uitgevoerd, bleek dat Rijnland op dat moment werkte op een niveau dat tussen 2 en 3 zat (afhankelijk van het onderwerp), net als overigens de meeste waterschappen. D&H hebben na bespreking van de rapportage besloten dat Rijnland eind 2020 op niveau 3 zou moeten functioneren.

Het streven van de waterschappen (bestuurlijk besloten door de CBCF in mei 2020) is, dat alle waterschappen streven naar het functioneren op volwassenheidsniveau 4 eind 2021.

In de tweede helft van 2021 zal een waterschapsbrede audit plaatsvinden op Informatieveiligheid en Privacy en daaruit zou dus moeten blijken dat Rijnland tenminste op volwassenheidsniveau 3 functioneert en een heel eind op weg is naar niveau 4.

Als FG constateer ik dat de meeste acties die door het kernteam zijn uitgevoerd om op niveau 3 of hoger te komen vrijwel helemaal gereed zijn. Ik constateer daarnaast dat vanuit de lijnorganisatie veel teams nog weinig proactief zijn op het gebied van voldoen aan de AVG, noch bij het aanschaffen van bijvoorbeeld nieuwe applicaties (werken we daarbij met persoonsgegevens en zo ja, wat moeten we doen om dat op de juiste manier te doen?), noch op het gebied van het afsluiten van verwerkersovereenkomsten en het bijhouden van het verwerkingenregister. In de huidige situatie is het kernteam Privacy een grote drijvende kracht achter het behalen van de privacy en security doelstellingen. Het kernteam moet op veel vlakken nog direct aansturen op de door medewerkers/teams te nemen acties. Om op niveau 3 te komen moet de organisatie organisatie-breed aan privacy werken en moeten we dit kunnen aantonen.

Om vervolgens de volwassenheid van de organisatie op niveau 4 te brengen moeten we zorgen dat niet alleen aan de wet- en regelgeving wordt voldaan, maar dat er vanuit alle onderdelen van de organisatie zelfstandig actie wordt ondernomen en dat kan worden geanticipeerd op privacyrisico's. Daar waar bijvoorbeeld tijdig (voorafgaand aan aanschaf) een Business Impact Analyse (BIA) wordt uitgevoerd via I&A worden de proces-eigenaren wel gewezen op het belang van overleg over Privacy en daarna wordt meestal wel gereageerd en gevraagd om overleg of informatie. Er is dus nog veel te doen voor de organisatie voordat Rijnland op volwassenheidsniveau 4 functioneert!

Bewustwording over de AVG onder de medewerkers is één van de belangrijkste troeven voor het behalen van de volwassenheidsniveaus. Medewerkers moeten ervan doordrongen zijn dat zij altijd en overal zorgvuldig omgaan met persoonsgegevens. Dat moet een continu proces zijn, om de aandacht niet te laten verslappen en om het echt onderdeel van het dagelijkse werk te maken. Het is belangrijk dat Rijnland aan dat continue proces aandacht gaat besteden

Er worden vrij weinig meldingen van (vermoedelijke) datalekken gedaan (minder dan statistisch te verwachten is in een organisatie van de omvang van Rijnland). Dit kan te maken hebben met een gebrek aan bewustwording of kennis over de AVG en datalekken. Het is ook mogelijk dat er een bepaalde drempel wordt ervaren bij het maken van een melding. Hier gaat het kernteam actie op ondernemen.

Gebleken is dat de deelname aan de Dataquiz, die in 2020 is gestart en op dit moment nog loopt, tot nu toe beperkt is. Ondanks het feit dat de quiz inmiddels al geruime tijd loopt, heeft een groot deel van de medewerkers – waaronder ook teamleiders- nog niet ingelogd op de dataquiz. Concreet: Helaas heeft minder dan de helft van de medewerkers het (verplichte!) niveau brons gehaald en minder dan 25% heeft 'zilver' gehaald (stand medio januari 2021). Voor met name teamleiders ligt hier een duidelijk aandachts- en actiepunt. De leidinggevenden hebben de taak om op structurele basis aandacht te besteden aan privacy en informatiebeveiliging. Daaronder valt ook het stimuleren van deelname aan de Dataquiz.. Mogelijk is er in de organisatie een trainingsmoeheid ontstaan, omdat er meerdere verplichte trainingen en modules bestaan die te maken hebben met privacy en informatiebeveiliging. Een aantal van de Privacy-contactpersonen zijn overigens wel heel actief op dit gebied.

De werkgroep die zich buigt over de Awareness, zal worden gevraagd hier aandacht aan te geven, door bijv. de dataquiz samen te voegen met die Aquademie cursussen. Daarnaast zal het kernteam privacy zich gaan richten om andere middelen die kunnen bijdragen aan de bewustwording in de organisatie.

Omdat juist het internaliseren van het werk met betrekking tot de AVG en het commitment van het managent op dit thema cruciaal zijn voor het behalen van niveau 3 en hoger, is het op dit moment te voorbarig om te spreken van functioneren op niveau 3. Het behalen van niveau 3 zal dit jaar wederom de focus moeten krijgen, alvorens we gaan kijken naar het behalen van niveau 4.

Datalekken en incidentmeldingen

In 2020 zijn er 16 Privacymeldingen in Topdesk gedaan. Slechts twee daarvan zijn gemeld bij de Autoriteit Persoonsgegevens (1x verlies laptop en 1x iets misgegaan bij een digitale commissievergadering, waardoor persoonsgegevens van een burger voor iedereen zichtbaar en

hoorbaar werden uitgewisseld). De overige meldingen waren naar het oordeel van de FG en het kernteam geen datalekken met impact voor mensen.

Het ging een aantal malen om vermoedens van medewerkers dat ze meer stukken konden zien dan zou moeten, maar dat werd in alle gevallen veroorzaakt door de functionele autorisaties en de verbeterde zoekmachine, er waren een aantal gevallen verkeerd verzonden post/bijlagen, hetgeen per direct kon worden hersteld/na overleg met de betrokkene vernietigd, een gestolen iPad (leeggeveegd door Automatisering) en een aantal mensen hadden (hun eigen) paspoort/telefoon/toegangspas laten slingeren. Deze werden alle binnen Rijnland teruggevonden. Tot slot was er een melding dat bij het updaten van Geoweb persoonsgegevens korte tijd zichtbaar zijn geweest voor teveel mensen.

Stand van zaken van de acties voor 2020

Zoals hierboven al aangegeven zijn in het jaarverslag van 2019 een aantal zaken genoemd die in 2020 uitgevoerd moesten worden.

- *Uitvoeren van het Awareness-programma (samen met Informatieveiligheid) gedurende heel 2020*: in 2020 zijn we in zee gegaan met Awareways, die voor Rijnland en HHSK gezamenlijk de zogenaamde 'dataquiz' hebben opgezet. In overleg met de directie is het behalen van tenminste het niveau Zilver verplicht gesteld. In 2020 konden de medewerkers de levels 'brons' en 'zilver' halen, in 2021 zal het level 'goud' volgen. Zoals hierboven al aangegeven valt het aantal deelnemende medewerkers tot nu toe tegen. Rijnland voldoet hiermee formeel aan de vereisten van het jaarlijks uitvoeren van een awarenessprogramma, maar praktisch gezien is maar een beperkt deel van de medewerkers 'bewust' gemaakt. Zoals hierboven al aangegeven zal de werkgroep die zich buigt over de Awareness worden gevraagd aandacht te geven aan op optreden van 'trainingsmoeheid', door bijv. de dataquiz samen te voegen met die Aquademie cursussen. Daarnaast zal het kernteam privacy zich gaan richten om andere middelen die kunnen bijdragen aan de bewustwording in de organisatie.
- *Update maken van het Privacy-beleid;* het Privacybeleid 2020 is op 25 augustus 2020 vastgesteld in D&H
- *Uitvoeren van Privacy Impact Assessments (PIA's)*. Deze worden ook wel aangeduid als DPIA (data protection impact assesments) Dergelijke assessments zijn verplicht als er in een bepaald proces veel persoonsgegevens en/of bijzondere persoonsgegevens worden verwerkt.
  In 2020 wilden we een PIA uitvoeren voor minimaal drie processen, door de Coronapandemie is er echter vertraging ontstaan. Uitgevoerd zijn PIA's voor
  - Het instroom-doorstroom-uitstroomproces (hierin worden veel én bijzondere persoonsgegevens verwerkt);
  - Het vergunningen- en meldingenproces waar het zaaksysteem 'In Proces' voor wordt gebruikt (persoonsgegevens van burgers).

  Het uitvoeren van een PIA voor Cameratoezicht/fysieke beveiliging gebouwen (wettelijk aangewezen voor verplichte PIA) is helaas niet gelukt, met name door vertraging in het project Fysieke toegangsbeveiliging. De PIA staat nu gepland voor Q1 2021.

- *Verder werken aan het implementeren van Privacy by Design en Privacy by Default*; in 2020 is er een architectuurprincipe voor deze onderwerpen vastgesteld in de I-raad, zodat Privacy

een onderwerp is geworden dat helemaal aan de voorkant bij ontwikkeling en aanschaf beoordeeld moet worden. Daarmee is een goed begin neergezet. De implementatie bij de aanschaf van nieuwe software blijft een voortdurend aandachtspunt

- *Aanschaf en implementatie van ISMS tooling (voor IB en Privacy)*. In 2020 is zo'n ISMS systeem, namelijk 'Fully in Control', aangeschaft. In 2021 zal dit moeten worden gevuld zodat het voor heel Rijnland een nuttig instrument is om de IB-en Privacytaken te beheren.

Tot slot: acties voor 2021 en aanbevelingen voor de toekomst

In 2021 zal een PIA voor cameratoezicht en een PIA voor tag-gebruik binnen Rijnland worden uitgevoerd. Omdat beide systemen ook gebruikt kunnen worden als personeelsvolgsysteem wordt de Ondernemingsraad betrokken bij deze PIA's .

Het ISMS systeem 'Fully in Control' (FIC) zal worden gevuld door of in overleg met het kernteam Privacy, met onder meer het verwerkingenregister.

De bewustwording van de medewerkers door middel van de Dataquiz wordt voortgezet onder de hierboven genoemde voorwaarden. Ook zullen een aantal zogenaamde phishingmails worden verstuurd, om het bewustzijn op dat gebied te vergroten.

En in de tweede helft van 2021 zal er een waterschapsbrede audit worden gehouden voor zowel Informatieveiligheid als Privacy, waar de inzet van de organisatie voor gevraagd zal worden, hetzij voor aanleveren van stukken, hetzij voor het deelnemen aan interviews.

Tenslotte: als FG is het ook mijn taak om daadwerkelijk toezicht te houden op de stand van zaken met betrekking tot Privacy in de organisatie. Tot nu is daar, doordat ik samen met het kernteam nog veel werk te verzetten had om van niveau 2 naar 3 te komen, te weinig van gekomen. Het ISMS systeem zal meer mogelijkheden gaan geven voor toetsen van de stand van zaken en het waar nodig aanspreken van mensen in de organisatie. Daarnaast zal ik steekproefsgewijs in de organisatie gaan 'peilen' hoe het is gesteld met onderdelen van de verplichtingen van de AVG, zoals bijvoorbeeld de bewaartermijnen.