Inleiding

Voor u ligt de jaarrapportage van de Functionaris Gegevensbescherming (FG) over 2023. Wegens het vertrek van de FG begin 2023 is de functie van FG op interim basis vervuld gedurende de periode april t/m december 2023. De bevindingen in deze rapportage zijn gebaseerd op de waarnemingen gedurende deze periode.

De jaarrapportage bestaat uit een drietal onderdelen.
In hoofdstuk 1 van de jaarrapportage wordt een aantal positieve ontwikkelingen binnen de organisatie aangestipt en worden constateringen gedaan ten aanzien van de gegeven aanbevelingen uit de vorige jaarrapportage. In hoofdstuk 2 worden een aantal aanbevelingen gedaan om privacybescherming binnen de organisatie op een hoger niveau te brengen. In hoofdstuk 3 wordt verslag gedaan van de werkzaamheden van bureau FG in 2023.

Hoofdstuk 1

Positieve ontwikkelingen

Aanpassing proces datalekken
In 2023 is het proces rondom het melden van datalekken aangepast. Het doel van de aanpassing is er voor zorgen dat datalekken die gemeld moeten worden bij de Autoriteit Persoonsgegevens (AP) binnen de daarvoor geldende wettelijke termijn van 72 uur worden gemeld. Belangrijkste onderdeel van het vernieuwde proces is de invoering van een piketdienst. Iedere werkdag heeft een aantal Privacy Offcers dienst en het is hun taak de datalekken die de betreffende dag aangemeld worden te beoordelen en zonodig te melden bij de AP. Dit heeft er in geresulteerd dat aangemelde datalekken vlot verwerkt worden door de Privacy Officers. Helaas zijn er nog steeds datalekken die te laat gemeld worden bij de AP. Dit komt omdat het dan te lang duurt voordat een datalek aangemeld wordt bij de dienstdoende Privacy Officers. Dit moet een punt van aandacht blijven en onderdeel worden van relevante bewustwordingsprogramma's.

Register van verwerkingen
Het register van verwerkingen is in 2023 voor de eerste keer openbaar gemaakt en gepubliceerd. Deze publicatie wordt 2 keer per geactualiseerd. Naast invulling geven aan het uitgangspunt van transparantie, zorgt dit er tegelijkertijd voor dat de juistheid en actualiteit van het register van verwerkingen hierdoor beter is geborgd. Directies worden nu gedwongen om minimaal twee keer per jaar hun verwerkingen actief te controleren op actualiteit, volledigheid en juistheid.

Aanbevelingen uit jaarrapportage 2023

In de jaarrapportage van 2022 zijn de volgende drie aanbevelingen gedaan:

1. Meet het volwassenheidsniveau.
   De organisatie heeft een begin gemaakt met de implementatie van de Baseline Privacy Amsterdam (BPA). In de loop van 2024 wordt deze op directieniveau verder uitgerold. De BPA beschrijft en meet een eenduidige set van maatregelen waaraan organisaties moeten voldoen om compliant te zijn met de Algemene Verordening Gegevensbescherming (AVG).
2. Verbeter de positie van de FG.

De positionering van de FG is herzien. De FG functie is vanaf 1 januari 2024 gepositioneerd bij directie Dienst Juridische Zaken (DJZ). Deze positionering komt beter tegemoet aan de vereiste onafhankelijke positie van de FG. Naast de positionering is ook de cultuur ten aanzien van privacy binnen de organisatie van belang. Dit betekent niet alleen dat de FG als onafhankelijk toezichthouder rechtstreeks contact dient te kunnen hebben met collegeleden en raadsleden, maar ook dat collegeleden en directeuren bij privacy gevoelige initiatieven tijdig de FG consulteren. Deze cultuuromslag zal nog verder moeten groeien.

3. Vergroot de kennis binnen de organisatie.
   Kennis omtrent datalekken en kennis van de AVG in zijn algemeenheid binnen de organisatie is nog niet van voldoende niveau. Vanuit bureau FG is niet geconstateerd dat aan deze aanbeveling een adequate invulling is gegeven.

Hoofdstuk 2

Aanbevelingen

Veel van wat er fout gaat binnen de organisatie is direct of indirect te wijten aan onvoldoende bewustwording/kennis bij medewerkers. Dit geldt voor alle niveaus. Dit uit zich onder andere in het niet of te laat herkennen van datalekken, niet of niet tijdig inroepen van privacy expertise. Dit brengt onnodige privacy risico's voor de burger met zich mee.
Om de bewustwording en kennis omtrent privacy binnen de organisatie te vergroten worden de volgende drie aanbevelingen gedaan:

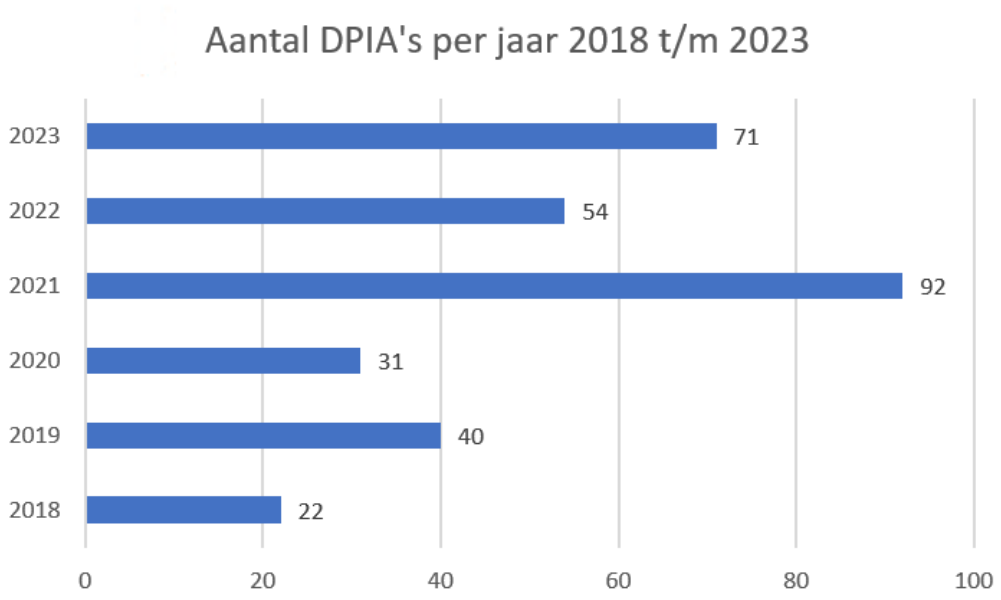
1. Vergroot bewustwording
   Ontwikkel een verplichte AVG training voor alle nieuwe medewerkers en een periodieke herhaaltraining voor bestaande medewerkers. Controleer actief of ook daadwerkelijk is deelgenomen aan de verplichte training
2. Zorg voor basiskennis AVG bij de directies zelf
   Om basiskennis omtrent privacy te borgen en om de zelfredzaamheid ten aanzien van privacy te vergroten schrijft de huidige governance voor dat elke directie over een Privacy Contactpersoon (PCP) beschikt. In de praktijk is gebleken dat niet iedere directie over een PCP beschikt. Bovendien heeft bij de directies die wel over een PCP beschikken de PCP niet altijd de benodigde kennis om deze rol adequaat in te vullen en/of voldoende tijd om aan deze rol te besteden. Een en ander is onder andere het gevolg van het feit dat er geen vastgestelde beschrijving is van de rol en de kennis die deze persoon moet hebben. Aanbeveling: stel een duidelijk profiel op van de PCP en spreek directies er op aan als ze geen PCP hebben aangesteld.
3. Stuur actief op privacy.
   Spreek directies er op aan als er onvoldoende aandacht wordt besteed aan privacy. De BPA en de Quality Assurance instrumenten bieden voldoende indicatoren om te monitoren of directies voldoende invulling geven aan de verplichten die voortvloeien uit de AVG.

Hoofdstuk 3

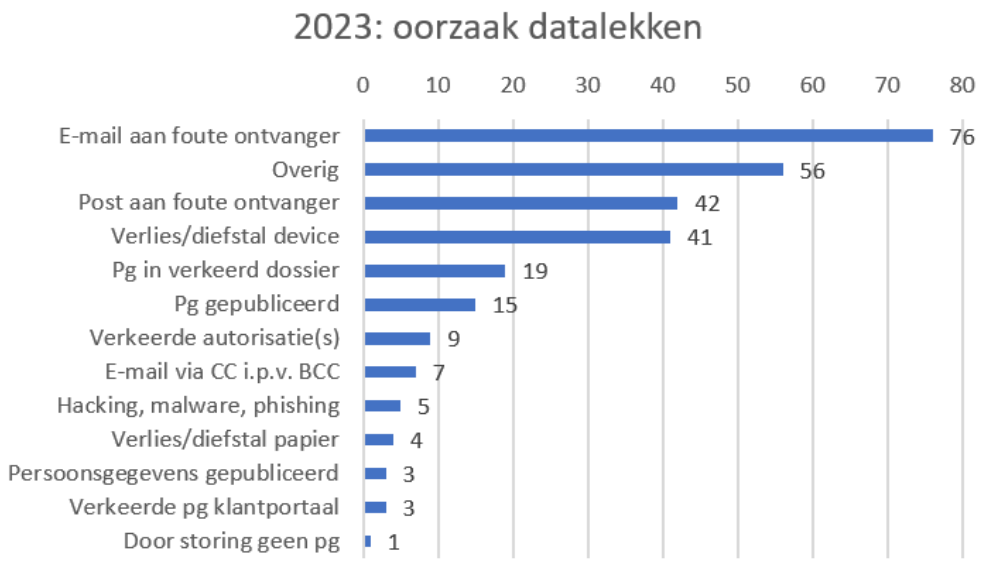
Werkzaamheden FG

FG Inbox
Bureau FG heeft een samenwerking met de gemeentelijke klachtencoördinator. De FG komt hierbij in actie als de klacht betrekking heeft op privacybescherming en de klacht niet tot tevredenheid van de burger door de organisatie zelf is opgelost.
In 2023 heeft de FG 2 interne klachten ontvangen en 20 externe klachten.

Data Protection Impact Assessments (DPIA`s)
Een DPIA is een door de AVG voorgeschreven instrument om de privacyrisico's van een verwerking in beeld te brengen met het doel deze risico's te mitigeren. Het is wettelijk verplicht een DPIA uit te voeren als er sprake is van een hoog risico verwerking ten aanzien van persoonsgegevens. Binnen de organisatie is de afspraak gemaakt dat de FG advies geeft op de DPIA voordat deze door het verantwoordelijke organisatieonderdeel wordt vastgesteld. In 2023 heeft het bureau FG 71 DPIA`s van advies voorzien.



Datalekken
Er zijn in 2023 281datalekken geregistreerd. Van deze 281 datalekken waren 34 datalekken dusdanig ernstig dat deze gemeld zijn bij de Autoriteit Persoonsgegevens.
25 meldingen zijn binnen de wettelijk voorgeschreven termijn van 72 uur gedaan en 9 meldingen zijn te laat gedaan.



WPG

De Wpg verplicht om jaarlijks een interne audit naar de toepassing van de Wpg in de gemeente uit te voeren (artikel 3 lid 1 regeling periodieke audit politiegegevens). Daarnaast schrijft artikel 33 lid 3 van de Wpg voor dat de verwerkingsverantwoordelijke binnen een jaar een hercontrole dient uit te voeren op de onderdelen die niet voldoen aan de gestelde voorwaarden. In dit kader heeft DMC een audit uitgevoerd die zich richt op de verwerking van politiegegevens in de domeinen V (Inkomen), II (Sport & Bos) en I/II/IV (Toezicht en Handhaving Openbare Ruimte).

Uit dit audit van DMC bleek het volgende:
Niet alle beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens zijn opgezet en geïmplementeerd. Dit betekent dat de gemeente Amsterdam nu al ruim vijf jaar niet aan de Wpg voldoet. Wel is er sprake van een duidelijke opwaartse lijn ten opzichte van de externe privacy audit over de periode 1 juli 2020 tot en met 30 juni 2021. Zo geldt voor de directies Toezicht en Handhaving Openbare Ruimte (THOR) en Sport en Bos dat er geen normen meer zijn die in het geheel niet voldoen aan de Wpg. Dit komt mede doordat in de applicatie CityControl een onderscheid gemaakt wordt tussen verwerkingen onder de AVG en de Wpg. Dit onderscheid was nog niet gerealiseerd ten tijde van de externe privacy audit.

De gemeente heeft in 2023 een Privacy Officer aangesteld die zich alléén bezig houdt met de WPG implementatie.