Gemeente Utrecht

Foto © Hans van Impelen

Verslag
Functionaris voor gegevensbescherming (FG)
2022 en 2023

Colofon

Naam document
Verslag Functionaris voor gegevensbescherming 2022 en 2023 (FG)

Versienummer
1.0

Versiedatum
6 november 2024

Versiebeheer
Het beheer van dit document berust bij de gemeente Utrecht

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
0.1	23-7-2024	Concept (25-7-024 verzonden voor reactie)
0.2	03-10-204	Reactie CIO office ontvangen
0.3	25-10-2024	Reactie verwerkt, enkele tekstuele aanpassingen doorgevoerd
1.0	06-11-2024	Nummering en typo's aangepast

Inhoudsopgave

Samenvatting

Dit FG verslag bevat twee jaren in verband met de tijdelijk langere afwezigheid van de FG en zeer beperkte vervanging. Dit heeft eind 2023 geleid tot werving van een (parttime) plaatsvervanger waardoor de FG functie iets minder kwetsbaar is. Ook met deze extra beschikbare capaciteit blijft het noodzakelijk om keuzes te maken aan welke onderwerpen wel of geen aandacht kan worden besteed.

De Algemene Verordening Gegevensbescherming (AVG) is in 2023 alweer ruim vijf jaar van kracht. Inmiddels is de AVG geïmplementeerd en hebben gemeenten veel kennis uitgewisseld en producten met elkaar gedeeld, zowel online als offline. Bijvoorbeeld via de Vereniging Nederlandse Gemeenten (VNG) via de bijeenkomsten van de Informatie Beveiligings Dienst (IBD) of het Centrum voor Informatiebeveiliging en Privacybescherming (CIP). Ook de reguliere FG overleggen zijn waardevol te noemen. Er is een periodiek G5 FG overleg waar de FG's van het OM en de Politie bij aansluiten en er is een provinciaal FG overleg met de Provincie en de Utrechtse gemeenten.

Ontwikkelingen in rechtspraak en wetgeving bieden steeds meer duidelijkheid bij de vele open normen uit de AVG. De Autoriteit Persoonsgegevens deelt inmiddels forse boetes uit aan organisaties (ook aan gemeenten) die de AVG overtreden en legt aanvullende dwangsommen op om de zaken alsnog in lijn met de AVG te brengen. Ook worden overheidsorganisaties onder verscherpt toezicht gesteld als zij onvoldoende aan de AVG voldoen. De verantwoordingsverplichtingen die de Wet Politiegegevens aan de gemeente oplegt hebben in 2022 geleid tot de eerste externe audit. Het externe auditrapport is medio oktober 2022 ontvangen. Hierin zijn een aantal tekortkomingen geconstateerd waarvan herstel noodzakelijk is. De hierop in 2023 uitgevoerde vervolgaudit door de Interne auditafdeling van de gemeente laat nog onvoldoende verbeteringen zien. Beide auditverslagen zijn door de gemeente aan de Autoriteit Persoonsgegevens toegezonden. Ook klachten van inwoners kunnen voor de Autoriteit Persoonsgegevens (AP) aanleiding geven om een onderzoek in te stellen. Een klacht (AVG) heeft inmiddels geleid tot nadere vragen van de Autoriteit Persoonsgegevens.

De Baseline Informatiebeveiliging Overheid (BIO) geeft invulling aan de AVG en Wpg[1] verplichting om "passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen en deze te kunnen aantonen". De gemeente doet dit risico gebaseerd. De BIO wordt door de gemeente als kader gebruikt om de maatregelen te bepalen.
Het beschermen van de gegevens van inwoners en bezoekers van onze stad was in 2022 en 2023 een belangrijk aandachtspunt. De gemeente heeft een belangrijke voorbeeldfunctie bij de beveiliging van persoonsgegevens en de bescherming van privacy binnen de sector.
De beperkte beschikbaarheid van de benodigde mensen en middelen staat echter steeds meer op gespannen voet met de ambities die de gemeente heeft. Door deze beperkte beschikbaarheid kunnen de gewenste resultaten pas op een veel later moment worden bereikt dan wenselijk.
Om concurrerend te kunnen zijn op de arbeidsmarkt zal de gemeente Utrecht tenminste een beloning moeten bieden die minimaal overeenkomt met wat andere overheids- instellingen bieden. Er zijn ook intern verschillen tussen de organisatieonderdelen waarneembaar. Door minimaal gelijke beloningen te bieden voor vergelijkbare functies blijf je als gemeente aantrekkelijk en kan je personeel ook langer aan de organisatie of het organisatieonderdeel binden. Personeelsadvertenties van andere overheidsorganisaties laten vaker een hoger beloningsniveau zien dan wat de gemeente Utrecht biedt voor vergelijkbare functies. Als geen vaste medewerkers kunnen worden aangetrokken is men aangewezen op veel duurdere inhuurkrachten die dan voor langere perioden moeten worden ingehuurd. In tijden van bezuiniging is dit een extra aandachtspunt.
Als niet aantoonbaar kan worden voldaan aan wettelijke verplichtingen is het risico niet ondenkbaar dat er eventuele maatregelen door de toezichthoudende instanties kunnen volgen. Ook overheidsinstanties ontkomen hier niet aan. Met de beschikbare capaciteit wordt er hard gewerkt om de doelstellingen te halen, maar het lukt helaas niet om in de gemeente Utrecht alles op orde te hebben en te houden en aan alle wettelijke verplichtingen aantoonbaar te voldoen. De gemeente geeft hier risico gebaseerd invulling aan.

De verantwoordelijkheden voor de gemeente Utrecht voor het verwerken van persoonsgegevens van inwoners en bezoekers liggen in hoofdlijnen bij drie bestuursorganen: de burgemeester, het college van B&W en de gemeenteraad. Het college is verantwoordelijk voor het merendeel van de verwerkingen van persoonsgegevens in onze gemeente. Ongeacht welk bestuursorgaan uiteindelijk verantwoordelijk is voor de verwerking presenteert de gemeente zich als gemeente Utrecht naar de inwoners. Om die reden wordt er in dit verslag geen onderscheid gemaakt tussen de verschillende bestuursorganen.
In dit verslag staan de acties en maatregelen die de gemeente Utrecht nam om de doelstellingen en beginselen uit de AVG en Wpg te behalen en te waarborgen.
Ook bevat dit document aandachtspunten en actiepunten voor het jaar 2024 en verder. Adequaat en zorgvuldig omgaan met persoonsgegevens is een blijvend en continu proces. Zeker in relatie met de zich razendsnel ontwikkelende technologische mogelijkheden en de in rap tempo toenemende verplichtingen uit de wet- en regelgeving.
Zowel de juridische als de ethische beoordeling bij de eventuele inzet van nieuwe technologieën krijgen bij de gemeente de nodige aandacht. Ook de diverse aanpassingen die door Europese wet- en regelgeving moeten worden geïmplementeerd vereisen veel aandacht en inspanning.
De gemeente beoogt een uitlegbaar verhaal te hebben in hoeverre zij voldoet aan de eisen die in de wet- en regelgeving en in de Baseline Informatiebeveiliging Overheid (BIO) worden gesteld.

[1] Zie artikel 5 en 32 AVG resp. 4a Wpg.

Hoewel sturing formeel is geregeld zijn de effecten hiervan in de praktijk beperkt waarneembaar waardoor het resultaat niet of niet tijdig wordt behaald en de gemeente hierop kan worden aangesproken door de toezichthouder(s).

Met de beschikbare mensen en middelen heeft de gemeente in 2022 en 2023 wel veel werk verzet op het gebied van gegevensbescherming.

Noemenswaardig zijn:

1. Uitrol van de e-learning gegevensbescherming voor de hele organisatie;
2. Opstellen van verschillende strategische standaarden voor gegevensbescherming;
3. De ontwikkeling van het expertteam gegevensbescherming binnen Domstad-IT;
4. Herziening van de informatie over gegevensbescherming op de website;
5. Migratie naar de Cloud van de kantoorautomatisering.

Op zich mooie resultaten waarbij ik toch enkele kanttekeningen plaats:
Ad 1. In september 2022 is de e-learning gegevensbescherming gestart die door voor meer dan 7000 personen bij de gemeente beschikbaar is. Omdat deelname niet verplicht is lag het deelnamepercentage in december 2023, 15 maanden na invoering, op circa 30%.
Ik wil bestuur, management en medewerkers van harte aanbevelen om de e-learning te volgen en hiermee aantoonbaar het bewustzijn, het kennisniveau en het volwassenheidsniveau te verhogen. Bestuur en management hebben daarbij een niet te onderschatten voorbeeldfunctie.

Ad 2. Het opstellen van strategische standaarden voor gegevensbescherming is een proces dat zeer lang duurt en zorgvuldig verloopt. Het implementeren van deze standaarden is nog een extra uitdaging. Het implementeren van deze standaarden levert veelal discussie op over prioritering en beschikbare capaciteit hiervoor. Dit zijn veelal discussiepunten tussen de centrale en decentrale organisatieonderdelen. Hierdoor loopt implementatie van deze standaarden forse vertraging op.

Ad 3. De ontwikkeling van een expertteam gegevensbescherming binnen Domstad-IT is een goede aanvulling op de beveiliging van de (persoons)gegevens binnen Domstad-IT. Dit expertteam levert de dienstverlening voornamelijk binnen Domstad-IT. Uitbreiding naar de overige organisatieonderdelen zou zeer wenselijk zijn. Dit bevordert een integrale en eenduidige aanpak.

Ad 4. De herziening van de informatie over gegevensbescherming op de website van de gemeente Utrecht is door het CIO-office in samenwerking met een extern juridisch bureau vormgegeven. Hierdoor is deze informatie duidelijker gemaakt, mede door visualisatie met behulp van infographics. Publicatie hiervan heeft echter nog niet plaatsgevonden waardoor het resultaat voor de inwoners nog niet zichtbaar is.

Ad 5. De migratie van de kantoorautomatisering naar de Cloud is zorgvuldig verlopen. Een extra analyse is op deze Cloudmigratie door een externe organisatie uitgevoerd hetgeen tot een positief advies heeft geleid.
Bij de migratie is de keuze gemaakt om de basisregistraties niet te migreren in verband met de hogere risico's die hieraan verbonden zijn. Mede gezien de geo politieke situatie is dit een verstandige keuze.

Er is steeds meer werk te verzetten om te kunnen voldoen aan de in het Gegevensbeschermingsbeleid 2019-2022 opgenomen ambitie: "certificeerbaar zijn voor gegevensbescherming".
Deze ambitie heeft op basis van de behaalde resultaten niet geleid tot certificering. Dit beleid was geldend tot 1 juli 2022. Gegevensbeschermingsbeleid is gebaseerd op artikel 5 en 24 van de AVG resp. art 4a van de Wpg en is daarmee een wettelijke verplichting.
Medio 2023 is het "Intern strategisch beleidskader voor gegevensbescherming Utrecht" vastgesteld en is de geldigheidsduur van het vorige beleid met terugwerkende kracht met een jaar verlengd.
De norm voor driejaarlijkse bijstelling staat als volgt in de Baseline Informatiebeveiliging overheid (BIO):
"Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld."
In het "Intern strategisch beleidskader voor gegevensbescherming Utrecht" is het volgende aangegeven:
"De integratie van gegevensbescherming in de gemeentelijke planning-en-controlcyclus was een van de speerpunten uit de vorige beleidsperiode. Dat is tot op heden onvoldoende uit de verf gekomen en dus gaan wij de komende periode daar veel op inzetten. Een van de gevolgen hiervan is dat de gemeente Utrecht aan het eind van de vorige beleidsperiode nog niet certificeerbaar was op informatiebeveiliging. De komende beleidsperiode blijven we dit ambitieuze doel nastreven."

Deze hoge ambities en de risico's die zijn verbonden aan de vele gegevensverwerkingen die de gemeente uitvoert leggen in toenemende mate beslag op de beschikbare middelen om de gestelde doelen te behalen. Ook de totstandkoming van diverse nieuwe Europese wet- en regelgeving zal deze druk nog extra verhogen.
In de praktijk merk ik echter dat er meer aandacht lijkt te zijn voor nieuwe ontwikkelingen, zoals bijvoorbeeld Artificial Intelligence (AI) dan aandacht voor het versnellen van het op orde brengen en houden van de reguliere werkprocessen. Als de basis niet op orde is geeft dit extra risico's bij de implementatie van nieuwe ontwikkelingen. Je bouwt dan op een instabiele fundering.
Registraties zoals het register datalekken, de bewaarplaatsen van vastgestelde Data Protection Impact Assessments (DPIA's) en Privacy Risico Analyses (Pra's) blijken onvoldoende op orde.

Veelal ontbreken er documenten waardoor niet snel en aantoonbaar aan de wettelijke verantwoordingsplicht kan worden voldaan. Het register van verwerkingen is opgenomen in het zaaksysteem en gekoppeld aan de online publicatie op de website van de gemeente. Dit register bevatte eind 2023 in totaal 328 verwerkingen.
Ook blijken DPIA's die eerder zijn vastgesteld niet tijdig te worden herzien. Aanbeveling hierbij is dat minimaal eenmaal per 3 jaar of eerder bij wijzigingen de DPIA wordt herzien. Een tweetal verwerkingen bleken (als pilot met cameratoepassingen in de openbare ruimte) te zijn gestart zonder voorafgaande uitvoering van een DPIA. Hierdoor is gehandeld in strijd met artikel 35 van de AVG.
Bij toetsing achteraf bleek de wettelijke grondslag voor deze verwerkingen te ontbreken.

Continue aandacht van het bestuur en management en vooral duidelijke sturing door het bestuur en management op de te behalen resultaten is een essentiële voorwaarde om de gewenste resultaten te behalen. Deze aandacht en sturing blijkt in veel gevallen niet aantoonbaar.

De route om aantoonbaar aan privacywetgeving te voldoen is lang, de gemeente is nog wel op de goede weg. Zonder versnelling, verbetering en sturing op de te behalen resultaten zijn de gestelde doelen ook niet haalbaar in deze beleidsperiode.

Met het huidige tempo is certificeerbaarheid op informatiebeveiliging ook voor de komende beleidsperiode naar mijn inschatting niet haalbaar.
Door beperkt beschikbare capaciteit en middelen kan niet volledig worden aangetoond en verantwoord dat aan de AVG respectievelijk Wpg wordt voldaan.

Inleiding

De gemeente Utrecht is zich bewust van het belang van het beschermen van persoonsgegevens van haar inwoners en bezoekers. We verwerken immers bij de uitoefening van onze taken veel (gevoelige) gegevens van veel (kwetsbare) mensen in veel verschillende domeinen. Ook staan persoonsgegevens van andere burgers, medewerkers, externen en zakenrelaties in onze systemen. Dit is noodzakelijk voor de vele taken die de gemeente uitvoert.
In de Algemene Verordening Gegevensbescherming (AVG) wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. De gemeente dient ondermeer transparant te zijn over welke persoonsgegevens worden verwerkt, voor welk doel dit is en onder welke grondslag dit is toegestaan. Tijdens de verwerkingsduur van persoonsgegevens moeten ze goed worden beveiligd, mogen ze niet onverenigbaar voor een ander doel worden verwerkt en moeten ze na afloop tijdig worden vernietigd of geanonimiseerd.
De gemeente moet kunnen verantwoorden en kunnen aantonen dat zij aan de wettelijke vereisten voldoet. Daarnaast hebben we ook te maken met tal van privacyregels in sectorspecifieke wetgeving. Ook de Wet politiegegevens (Wpg) kent soortgelijke regels en deze zijn gebaseerd op de richtlijn gegevensbescherming rechtshandhaving (Directive (EU) 2016/680). Dit alles heeft gevolgen voor de inrichting van processen en systemen in en van onze gemeente.

Onder de verantwoordelijkheid van zowel het college van B&W, de burgemeester als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dienen we te beschikken over een interne toezichthouder: de Functionaris voor Gegevensbescherming (FG).

De FG ziet erop toe dat de AVG intern wordt nageleefd. Het college dient erop toe te zien dat de FG naar behoren en tijdig wordt betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid. De uitvoerende taken liggen bij de privacy officers respectievelijk de Decentrale Information Security Officers van de organisatieonderdelen.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden, bevindingen en aanbevelingen. Door tijdelijke afwezigheid van de FG eind 2022 en begin 2023 is dit verslag later verschenen en gecombineerd tot twee jaren.
Dit toont aan dat de functie kwetsbaar is, ondermeer door de beperkt beschikbare middelen en ondersteuning.

Leeswijzer

Dit verslag bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar 2022 en 2023. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn er genomen om te voldoen aan de AVG en Wpg?
In het tweede deel worden aanbevelingen gedaan om gegevensbescherming vanaf het jaar 2024 verder te verbeteren. Hierbij wordt waar nodig tevens aandacht geschonken aan de technische en organisatorische ontwikkelingen die nodig zijn om verbeteringen te bereiken.

Voor het bepalen van de thema's die in dit rapport worden genoemd is gebruik gemaakt van de thema's van de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG).
Er worden zeven thema's onderscheiden:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

Deel 1. Terugkijken naar 2022 en 2023

Het jaar 2023 is het jaar waarin de AVG alweer ruim vijf jaar van kracht is. Voortdurend is er aandacht voor verdere verbeteringen. De snelheid waarmee deze verbeteringen tot stand kunnen worden gebracht zijn echter afhankelijk van de beschikbaar gestelde middelen en capaciteit.
De snelheid waarmee veel nieuwe (Europese) wetten en richtlijnen van kracht zijn geworden of de komende periode nog worden is met de beperkte mogelijkheden voor de organisatie moeilijk bij te houden, vooral als het gaat om de uiteindelijke implementatie hiervan.
De inzetbaarheid van professionals op het gebied van gegevensbescherming (=Privacybescherming en Informatiebeveiliging) in 2022 en 2023 is door verschillende oorzaken (waaronder tijdelijke afwezigheid van meerdere personen en doorstroom naar andere organisatieonderdelen of uitstroom naar andere organisaties) niet volledig geweest.
In dit deel van het verslag zal worden teruggeblikt op hetgeen de gemeente in 2022 en 2023 heeft bereikt en welke werkzaamheden zijn verricht.

1. Beleid

Het gegevensbeschermingsbeleid is een kader waarin de gemeente Utrecht aangeeft aan welke principes zij zich houdt bij de verwerking en bescherming van persoonsgegevens. Het laat zien hoe de gemeente om wil gaan met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.
Om het gegevensbeschermingsbeleid uit te voeren was een Routekaart gegevensbescherming opgesteld en een Stuurgroep gegevensbescherming en een Regiegroep gegevensbescherming ingesteld. De Stuurgroep opereerde op strategisch niveau en de Regiegroep op tactisch niveau. Het programma gegevensbescherming is medio 2023 gestopt en de onderwerpen zijn overgedragen aan de staande organisatie.
De stuurgroep is opgeheven en de regiegroep is gehandhaafd. Daarnaast ie er een Vakgroep gegevensbescherming. In deze vakgroep komen elke twee weken de decentrale information security officers en privacy officers samen met de CISO, de CPO en de FG. In deze vakgroep worden de actuele onderwerpen besproken op het gebied van gegevensbescherming.
Omdat het beleid in 2023 opnieuw in is beschreven is ook de structuur en sturing aangepast.
Aangezien dit beleid ook verschilt van de Privacyverordening gemeente Utrecht heeft dit ook gevolgen voor deze verordening.

2. Processen

Bij de meeste verwerkingen van persoonsgegevens van de gemeente Utrecht vormen de AVG, de uAVG en de specifieke wet- en regelgeving het wettelijk kader. Als het gaat om politiegegevens zijn de Richtlijn (EU) 2016/680 en de Wpg leidend.
Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Bij risicovolle verwerkingen is de gemeente verplicht om een gegevensbeschermingseffectbeoordeling (DPIA[2]) uit te voeren. Of een DPIA moet worden uitgevoerd wordt vastgelegd in een Privacy Risico Analyse (PRA).
Tot en met 2023 zijn er meerdere PIA's en DPIA's uitgevoerd. De FG heeft hierbij een adviserende en toetsende rol. DPIA's worden besproken in het spreekuur gegevensbescherming met de vertegenwoordiger van het betreffende organisatieonderdeel, de decentrale Information Security Officer en de FG. Een privacyjurist is alleen op afroep beschikbaar, evenals de CISO en/of de CPO. Waar nodig worden andere expertises betrokken. Bij een positief advies wordt de DPIA door of namens de IRM'er vastgesteld.
Een centrale registratie van vastgestelde DPIA's is vormgegeven en beschreven in een procesbeschrijving. Deze is beschikbaar via intranet. Uitgevoerde DPIA's zijn slechts voor een deel terug te vinden op de intern door de gemeente voorgeschreven bewaarplaats.
Ter illustratie: in 2023 zijn 40 DPIA's voor advisering voorgelegd aan de FG, hiervan zijn er slechts 11 te vinden op de voorgeschreven bewaarplaats.
Niet alle organisatieonderdelen plaatsen hier de DPIA's ondanks het feit dat de procesbeschrijving dit vereist.
DPIA's moeten volgens de richtlijnen van de AP en VNG elke drie jaar worden herzien of eerder bij wijziging van de verwerking. Een substantieel deel van de op de voorgeschreven bewaarplaats geplaatste DPIA's is inmiddels ouder dan drie jaar.
Door het ontbreken van een eenduidige en volledige registratie is onduidelijk of c.q. hoe op de tijdige herijking van DPIA's wordt gestuurd door het management.
In bijlage 1 is een overzicht opgenomen van de het aantal uitgevoerde DPIA's voor de verwerkingen tot en met 2023. Dit overzicht is gebaseerd op de opgenomen DPIA's in de daarvoor aangewezen registratie.

Aanbeveling:

2.1 gebruik de voorgeschreven bewaarplaats van vastgestelde DPIA's gemeentebreed; genereer op basis van deze registratie de managementinformatie;
2.2 op basis van deze managementinformatie actief en aantoonbaar te sturen op tijdige herijking.

---

[2] De gegevensbeschermingseffectbeoordeling wordt genoemd in de AVG en Wpg en ook wel afgekort tot "DPIA" naar de Engelse term "Data Protection Impact Assessment". Een Privacy Impact Assessment (PIA) is een eerdere versie van de huidige DPIA.

Periodiek wordt een monitor gegevensbescherming door de organisatieonderdelen ingevuld waarin de stand van zaken wordt weergegeven over de gerealiseerde aantallen. Deze monitor wordt gebruikt voor de tertaalgesprekken die door het CIO-office gehouden worden met de organisatieonderdelen.
Bij toetsing van de monitor is door de FG vastgesteld dat de daarin genoemde aantallen verwerkingen een hoger aantal te zien geeft dan het officiële register van verwerkingen. Tevens staan er veel minder datalekken in de monitor dan in het zaaksysteem.
Dit heeft geleid tot aanpassing van de monitor gegevensbescherming. Over de aantallen verwerkingen zijn geen gegevens meer in de monitor opgenomen. Deze worden vastgelegd in het zaaksysteem en gepubliceerd en deze zijn opvraagbaar via de website van de gemeente. Deze aantallen zouden eenvoudig aan de monitor gegevensbescherming kunnen worden toegevoegd.
Met betrekking tot datalekken is in de monitor gegevensbescherming het volgende opgenomen “Nog geen kengetallen rondom datalekken te rapporteren vanuit OO (=Organisatie Onderdeel)”. Sinds de wijziging van het proces datalekken medio 2021 is de tijdige aanvulling van het register datalekken nog onvoldoende waardoor periodieke rapportage niet eenvoudig mogelijk is en het online register datalekken niet kan worden aangevuld.
Over 2022 is een “Jaaroverzicht datalekken” verschenen dat op intranet is geplaatst. Over 2023 is geen jaaroverzicht gepubliceerd op intranet.
Om effectief te kunnen sturen moet de stuurinformatie in de monitor overeenkomen met de actuele cijfers uit de registraties uit het zaaksysteem waarin deze informatie is vastgelegd.

Aanbeveling:

- **3.1 Neem de aantallen “verwerkingen van persoonsgegevens” en “meldingen datalekken” uit het zaaksysteem op in de monitor gegevensbescherming.**
- **3.2 Stuur op tijdige en volledige aanvulling (inclusief documentatie) van het register datalekken in het zaaksysteem.**
- **3.3 Vul het externe register datalekken tijdig aan, minimaal eenmaal per kwartaal.**
- **3.4 Betrek de businesscontrollers betrekken bij de validatie van de gepresenteerde cijfers in de monitor.**

Sinds de Corona-maatregelen is het voor veel medewerkers mogelijk hun werkzaamheden vanaf het huisadres uit te voeren. De gemeente heeft binnen zeer korte tijd hierop ingespeeld door thuiswerkplekken (stoelen, zit-sta bureaus, monitoren, toetsenborden, kabels en muizen) beschikbaar te stellen aan de medewerkers.
Door te werken met door de gemeente beschikbaar gestelde beveiligde apparatuur, zoals laptops en mobiele telefoons, is het beheer en de beveiliging hiervan op afstand goed te regelen.
Van de beschikbare Video-vergadertools wordt dan ook regelmatig gebruik gemaakt. Meerdere malen wordt gevraagd om vergaderingen op te nemen zodat deze later kunnen worden teruggekeken. Bij de invoering van video vergadertools is bewust gekozen om de opnamemogelijkheid niet beschikbaar te stellen. Het opnemen van een videovergadering is een verwerking van persoonsgegevens waarop de AVG van toepassing is. Naast de wettelijke grondslag en doelbinding is ook dataminimalisatie een verplichting waaraan invulling moet worden gegeven. Ook de plaats waar de data wordt verwerkt heeft invloed op deze keuze.
De keuze om vergaderingen niet op te nemen (met uitzondering van de openbare raadsvergaderingen) is gebaseerd op de wettelijke verplichting dat bij de verwerking van persoonsgegevens de minst belastende manier de voorkeur dient te hebben. Een verslag van een vergadering of een besluitenlijst is sneller en eenvoudiger te lezen dan het integraal terugkijken van een volledige vergadering. Het opnemen van les- of instructiemateriaal op video is een mogelijkheid die nog niet vaak wordt toegepast. Dit kan voordelen bieden bij het tijd- en plaats onafhankelijk werken.
Het opslaan en beheren van videobeelden vereist een beheersorganisatie (waarin nog niet is voorzien).
Bovendien kost het opslaan en beschikbaar hebben van videobeelden relatief veel ruimte voor dataopslag. Het draaiend houden van deze dataopslag heeft ook negatieve milieueffecten.

Aanbeveling:

- **3.5 Ga door met het verstrekken van door de gemeente beveiligde apparatuur waar mogelijk;**
- **3.6 Handhaaf het beleid om geen opnames van vergaderingen te maken.**
- **3.7 Overweeg de opnamemogelijkheid van les- of instructiebijeenkomsten beschikbaar te stellen.**

3. Organisatorische inbedding

Voor een goede en juiste uitvoering is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen en het belang van gegevensbescherming. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.
De Functionaris voor Gegevensbescherming is organisatorisch ondergebracht bij Concerncoltrol en heeft een onafhankelijke positie binnen de organisatie. De CISO, CPO en CRO zijn onderdeel van het CIO-office en rapporteren aan of via de CIO. Door de positionering van de CISO, CPO, CRO en de FG is er geen rechtstreekse rapportagelijn met het hoogste management in de organisatie. De IBD heeft dit als volgt verwoord op de website: *"In het Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2023 – 2024 staat dat gemeenten stappen zetten, maar dat er meer nodig is om het groeiende gat tussen dreiging en weerbaarheid te dichten. Het Dreigingsbeeld bevat concrete succesfactoren met concrete stappen die gemeenten kunnen zetten om de weerbaarheid te vergroten. De succesfactoren moeten in samenhang met elkaar worden opgepakt. Maar zonder "Eigenaarschap van het management" is dat lastig, zo niet onmogelijk. De IBD heeft daarom 'Gesprekskaartjes voor de Gemeentesecretaris' ontwikkeld; om het eigenaarschap bij het management op de kaart te zetten."*
Dit is onder de aandacht gebracht van de gemeentesecretaris maar werd door hem niet noodzakelijk geacht om een overlegreeks in te plannen.
Ondersteuning van de FG is in slechts in beperkte mate aanwezig. Voor het spreekuur gegevensbescherming is een privacy jurist op afroep beschikbaar en voor het plannen van bijeenkomsten van dit spreekuur is ambtelijke ondersteuning aanwezig. Hierdoor worden veel administratieve zaken door de FG zelf gedaan. Dat de functie kwetsbaar is, is inmiddels gebleken en heeft geleid tot aanstelling van een (parttime) plaatsvervangend FG.
In de AVG, in de Richtlijn (EU) 2016/680 en in de Wpg zijn verschillende wettelijke verplichtingen opgenomen die betrekking hebben op de positie van de FG. Zo moet de verwerkingsverantwoordelijke ervoor zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Ook moet de FG voldoende worden ondersteund en bij de vervulling van de zijn taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van die taken en het in stand houden van zijn deskundigheid.
Helaas is hier niet altijd sprake van, soms wordt de FG pas achteraf betrokken of geïnformeerd of zijn er onvoldoende middelen beschikbaar.
Voorbeelden hiervan zijn de implementatie van een nieuw automatiseringssysteem, de uitvoering van pilots of verwerkingen zonder voorafgaande DPIA of het niet of niet tijdig betrekken van de FG bij besprekingen over de bescherming van persoonsgegevens. Het niet tijdig en naar behoren betrekken van de FG bij aangelegenheden die verband houden met de bescherming van persoonsgegevens of het niet of niet tijdig uitvoeren van een DPIA is in strijd met de AVG resp. de Wpg. Betere ondersteuning van de FG is meer dan wenselijk.

4. Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (betrokkene) zowel actief als passief te informeren over het verwerken, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en - verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om met een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.
Het proces rond de rechten van betrokkenen gaat in de meeste gevallen over inzageverzoeken.
Sinds 2020 wordt dit proces uitgevoerd onder verantwoordelijkheid van Juridische zaken (JZ). Het behandelen van inzageverzoeken is een tijdrovend en intensief proces waarbij informatie van verschillende organisatieonderdelen moet worden gevraagd. Dit heeft geleid tot inzet van meerdere medewerkers bij het afhandelen van inzageverzoeken.
In bijlage 2 is een overzicht opgenomen van het aantal verzoeken van betrokkenen vanaf 2018. Voor 2023 is een forse stijging van het aantal inzageverzoeken te zien.

5. Samenwerking

De gemeente Utrecht werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen moeten ook voldoen aan de AVG. De gemeente Gemeente Utrecht dient afspraken te maken met deze partijen. Voorafgaand aan een verwerking wordt zonodig een DPIA opgesteld.
Andere voorbeelden van samenwerking, bijvoorbeeld over de (methoden van) beveiliging van persoonsgegevens, zijn:
-Er is een Community voor cyberweerbaarheid binnen de regio Utrecht die meerder malen per jaar bijeen komt onder regie van Openbare Orde en Veiligheid.
-Er is een provinciaal FG overleg dat ieder kwartaal bijeenkomt. Naast informatie-uitwisseling zijn de lijnen kort en kent men elkaar.
-Er is een periodiek G5 FG overleg waaraan ook de FG's van de nationale politie en het Openbaar Ministerie aan deelnemen. Ook tussen individuele gemeenten weten FG's snel contact te leggen met elkaar.
-Er wordt samengewerkt met:
-de Informatiebeveiligingsdienst (IBD) van de (VNG).
-het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)
-de Autoriteit Persoonsgegevens.
-het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG)

6. Beveiliging

Onder de AVG geldt de verplichting van gegevensbescherming door ontwerp, is er een registerplicht voor verwerkingen van persoonsgegevens en is er een registratieplicht, documentatieplicht en meldplicht voor datalekken.
Aan beveiliging wordt het nodige gedaan binnen de gemeente Utrecht waarbij telkens meegewogen wordt dat de gemeente ook toegankelijk hoort te zijn voor inwoners en bezoekers en medewerkers hun werk moeten kunnen doen. Bescherming van digitale systemen tegen bedreigingen van buitenaf hebben daarbij voorrang op interne bedreigingen. Het inregelen van autorisaties van medewerkers, het loggen van gebruik van systemen en de periodiek controle hierop zijn daarbij belangrijke aandachtspunten waaraan nog niet alle applicaties aantoonbaar voldoen.
De meldplicht datalekken vraagt veel tijd en aandacht om tijdig (binnen 72 uur) aan de wettelijke verplichtingen te kunnen voldoen. Dit houdt in dat meldenswaardige datalekken gemeld moeten worden aan de AP en/of de betrokkene(n). Hierbij worden de richtlijnen van de Autoriteit Persoonsgegevens aangehouden.
De gemeente Gemeente Utrecht neemt waar mogelijk passende technische en organisatorische maatregelen ter beveiliging van persoonsgegevens. Dat het soms mis gaat blijkt uit het feit dat er datalekken voorkomen.
Het blijft mensenwerk, ondanks de technische ondersteuning. Hoeveel datalekken er precies zijn valt niet te achterhalen. Geconstateerde datalekken worden centraal gemeld via de website van de gemeente Utrecht en automatisch in het zaaksysteem opgenomen. Bij melding van een mogelijk datalek wordt de FG indien nodig betrokken en wordt het datalek behandeld door het verantwoordelijke organisatieonderdeel. Als de FG wordt betrokken wordt niet altijd het FG advies overgenomen m.b.t. de melding AP en/of de melding aan betrokkenen.
Op basis van de gemelde datalekken is inzicht te geven in de ontwikkeling hiervan. De datalekregistratie is wettelijk verplicht waarmee de gehele afhandeling van datalekken moet kunnen worden nagegaan en aangetoond door beschikbaar bewijsmateriaal. Het tijdig en volledig opnemen van alle relevante informatie en documentatie in dit registratiesysteem is een verantwoordelijkheid van de organisatieonderdelen. Net als in 2022 bleek ook eind 2023 niet alle informatie en documentatie in dit systeem aanwezig te zijn waarna verschillende malen is gerappelleerd. Het overzicht datalekken is samengesteld op basis van de beschikbare informatie. De registratie en documentatie van datalekken voldoet niet geheel aan de wettelijke eisen.

In bijlage 3 is een overzicht opgenomen van het aantal datalekken in tot en met 2023.

7. Verantwoording

De AVG legt de verantwoordelijkheid om aan te tonen dat zij aan de AVG voldoet bij de organisatie zelf. Voorafgaand aan de verwerking van persoonsgegevens moet de gemeente aantonen dat deze voldoet aan de AVG of Wpg. Door te voldoen aan deze verplichting levert de organisatie een belangrijke bijdrage aan de bescherming van persoonsgegevens. In het online raadpleegbare register van verwerkingen staan de verwerkingen van persoonsgegevens die de gemeente Utrecht uitvoert. Dit register wordt regelmatig bijgewerkt. Het register is te vinden op de website van de gemeente Utrecht: https://www.utrecht.nl/bestuur-en-organisatie/privacy/privacyverklaring/register-verwerkingen Eind 2023 bevatte het register 328 verwerkingen.
Op de website van de gemeente Utrecht is te vinden hoe Utrecht met privacy omgaat en kunnen mogelijke datalekken of klachten eenvoudig worden gemeld. Ingezet wordt om de informatie op de website verder te verbeteren door het ontwikkelen van privacyverklaringen die worden gekoppeld aan de soort verwerking van persoonsgegevens.

In voorkomende gevallen wordt een beroep gedaan op externe aanbieders om bepaalde onderzoeken uit te voeren. Vanuit de professionaliteit van deze organisaties zou je mogen verwachten dat zij duidelijk kunnen aangeven welke informatie voor het onderzoek minimaal noodzakelijk is. Het tegendeel blijkt als een organisatie aangeeft meer informatie nodig te hebben dan strikt noodzakelijk is. Vanuit de gemeente wordt op basis van een nadere analyse of in een DPIA bepaald welke informatie voor het onderzoek kan worden geleverd waarbij data minimalisatie en mogelijke anonimisering or pseudonimisering belangrijke aandachtspunten zijn. Onderzoeken blijken ook met minder data heel goed mogelijk als de vraag specifiek genoeg wordt gedefinieerd.
Het kennisniveau van het management blijkt in veel gevallen onvoldoende waardoor de druk op de decentrale security en privacy officers onevenredig wordt verhoogd.
Met betrekking tot de BIO wordt door verschillende organisaties geadviseerd om de sturing op volwassenheid van de organisatie vorm te geven. Verwezen wordt naar de beschikbare volwassenheidsmodellen van bijvoorbeeld Cobit, CIP, NOREA e.d.

5 niveaus van het PMM (Privacy Maturity Model):
(1) Ad hoc: procedures of processen zijn vooral informeel, incompleet of worden inconsistent toegepast.
(2) Herhaalbaar: procedures of processen bestaan, maar zijn niet (volledig) gedocumenteerd en omvatten niet alle relevante aspecten.
(3) Bepaald: procedures of processen zijn volledig gedocumenteerd en geïmplementeerd en omvatten alle relevante aspecten.
(4) Beheerst: reviews worden uitgevoerd om de effectiviteit te meten van de getroffen beheersmaatregelen.
(5) Geoptimaliseerd: periodieke reviews worden uitgevoerd en feedback wordt verzameld om te zorgen voor continu verbetering van procedures of processen.

Een volwassenheidsmodel gegevensbescherming biedt het management een handreiking om na te gaan wat de stand van zaken is en welke ontwikkeling nog moet worden doorgemaakt om het minimaal vereiste volwassenheidsniveau 3 te bereiken. Een gemeentebrede meting van het volwassenheidsniveau heeft in de gemeente Utrecht nog niet plaatsgevonden. Op basis van het deelnamepercentage aan de e-learning bewustwording gegevensbescherming, het aan kunnen tonen van de wettelijk vereiste

verantwoordingsdocumenten, uitgevoerde audits en de reacties van management en medewerkers schat ik het gemiddelde volwassenheidsniveau van de gemeente niet hoger in dan niveau 2.

Aanbeveling:
8.1 Voer jaarlijks een meting uit om het volwassenheidsniveau van de gehele organisatie vast te stellen.

8. Conclusie

In 2022 en 2023 heeft de gemeente Utrecht met de beperkt beschikbaar gestelde capaciteit best veel werk verzet om aan de AVG en Wpg te voldoen en de Baseline Informatiebeveiliging Overheid te implementeren in de organisatie, de systemen en de processen.
Voor de Wpg is een de eerste (verplichte) externe audit uitgevoerd en is inmiddels een interne vervolgaudit uitgevoerd. De externe audit heeft een aantal tekortkomingen vastgesteld die dienen te worden verbeterd. Door de (wederom) beperkt inzetbare capaciteit duurt het echter veel langer dan wenselijk om de voorgenomen maatregelen/verbeteringen in te voeren. Uit de het jaar daarna uitgevoerde interne audit is gebleken dat er nog onvoldoende verbetering heeft plaatsgevonden. Op basis van de verplichte toezending van de auditrapportages aan de Autoriteit Persoonsgegevens heeft deze toezichthouder al vragen gesteld over deze rapportages.

Er zijn meerdere punten van zorg voor de organisatie om aantoonbaar te kunnen voldoen aan de AVG, Wpg en BIO. In het tweede deel van het verslag staan aanbevelingen om gegevensbescherming verder in te bedden in de organisatie.

Deel 2. Vooruitkijken naar 2024

Gegevensbescherming onderdeel laten zijn van de processen en systemen, en daarmee aantoonbaar voldoen aan privacywetgeving, is een continu proces. Het vraagt om structurele borging van dit onderwerp.
In 2024 zal centraal staan
-de invulling van de Gegevens bescherming management systeem (GBMS),
-de invulling van bewustwordingsactiviteiten en betrokkenheid hierbij van het management
-het uitvoeren van het beleid voor 2022 tot 2025.

1. Beleid

De ervaring leert dat het proces van totstandkoming van nieuw beleid veel tijd vraagt.
Het gegevensbeschermingsbeleid 2019-2022 is door het college van B&W vastgesteld op 25 juni 2019 en was geldig tot 1 juli 2022. Dit beleid is door de directieraad in 2023 met terugwerkende kracht voor een jaar verlengd.
In 2023 is het “Intern strategisch beleidskader voor gegevensbescherming Utrecht” opgesteld en vastgesteld door de directieraad en geldt voor 2023-2026. Voor 2024 en verder worden er meerdere Europese wetten en richtlijnen van kracht alsmede op deze richtlijnen gebaseerde nationale wet- en regelgeving. De wet- en regelgeving heeft invloed op het vastgestelde beleid. Onduidelijk is of en in hoeverre rekening wordt gehouden met benodigde extra middelen om dit nieuwe beleid tijdig tot uitvoering te kunnen brengen. Uitvoering met de huidige beschikbare capaciteit en middelen heeft tot gevolg dat het langer duurt voordat op basis van de uitvoering van het beleid aantoonbaar en tijdig aan alle onderdelen van de AVG, de Wpg en BIO wordt voldaan.

Aanbevelingen:

1.1 Herzie het beleid tussentijds op basis van de van kracht wordende wet- en regelgeving in de beleidsperiode.

1.2 Stel eventuele extra benodigde middelen beschikbaar om dit beleid ook tijdig tot uitvoering te kunnen brengen.

2. Processen

Bewaartermijnen: bij verschillende verwerkingen is gebleken dat informatie langer wordt bewaard dan de hiervoor vastgestelde bewaartermijnen. Dit is ook van toepassing op het papieren archief dat extern is opgeslagen.
Hier is vanaf 2020 zowel door Het Utrechts Archief (HUA) als door de FG op gewezen.
In 2021 is een aanbesteding uitgevoerd en is een onderzoeksbureau ingehuurd. De uitkomsten zijn in 2022 opgeleverd en hebben in 2023 geleid tot uitbreiding om dit op orde te brengen.
Dit heeft echter nog niet geleid tot het voortvarend en regelmatig uitvoeren van vernietigingsprocessen.
Te lang bewaren van persoonsgegevens is strijdig met zowel de Archiefwet als met de AVG respectievelijk Wpg en kan tot maatregelen en/of forse boetes van de toezichthoudende instanties leiden. Het behoeft geen verder betoog dat het bewaren op onjuiste plaatsen zich kan onttrekken aan het beheer door de recordmanagers waardoor tijdige verwijdering of vernietiging niet kan plaatsvinden.

Aanbeveling:

2.1 Geef voorrang aan het verbeteren van de beheerprocessen zodat documenten en persoonsgegevens op de juiste plaats worden bewaard en tijdig (= direct na afloop van de bewaartermijn) aantoonbaar worden verwijderd conform de hiervoor geldende voorschriften.

3. Organisatorische inbedding

De organisatorische inbedding ontwikkelt zich in Utrecht geleidelijk op organische wijze.
Gegevensbeheer en gegevensbescherming zijn gescheiden van elkaar georganiseerd. Bij een nauwere samenwerking tussen deze twee disciplines kunnen voordelen worden behaald.
Om concurrerend te kunnen zijn op de arbeidsmarkt zal de gemeente Utrecht tenminste een beloning moeten bieden die minimaal overeenkomt met wat andere overheids- instellingen bieden. Er zijn ook intern verschillen tussen de organisatieonderdelen waarneembaar. Door minimaal gelijke beloningen te bieden voor vergelijkbare functies blijf je als gemeente aantrekkelijk en kan je personeel ook langer aan de organisatie of het organisatieonderdeel binden. Personeelsadvertenties van andere overheidsorganisaties laten vaker een hoger beloningsniveau zien dan wat de gemeente Utrecht biedt voor vergelijkbare functies. Als geen vaste medewerkers kunnen worden aangetrokken is men aangewezen op veel duurdere inhuurkrachten die dan voor langere perioden moeten worden ingehuurd. In tijden van bezuiniging is dit een extra aandachtspunt.

De Functionaris voor Gegevensbescherming is organisatorisch ondergebracht bij Concerncontrol en heeft vanuit de wet een onafhankelijke positie binnen de organisatie. De CISO, CPO en CRO zijn onderdeel van het CIO-office en rapporteren aan of via de CIO. Door de positionering van de CISO, CPO, CRO en de FG is er geen rechtstreekse rapportagelijn met het hoogste management in de organisatie. Hierdoor krijgt gegevensbescherming niet de prioritering en aandacht die het zou moeten hebben.

Aanbeveling:

3.1 Onderzoek hoe de samenwerking tussen gegevensbeheer en gegevensbescherming het beste gestalte kan krijgen zodat aantoonbaar zowel aan de archiefwet als aan de AVG en Wpg

kan worden voldaan en verantwoord kan worden dat persoonsgegevens en documenten tijdig worden verwijderd respectievelijk vernietigd.

3.2 Onderzoek de verschillen in beloning van de DISO's en Privacyofficers binnen de verschillende onderdelen van de organisatie en breng deze zoveel mogelijk in overeenstemming met de beloningsstructuur van andere overheidsorganisaties.

3.3 Onderzoek hoe de positionering van de CISO, de CPO, de CRO en de FG kan worden verankerd in de organisatie waardoor een rechtstreekse rapportagelijn met de Algemeen directeur/gemeentesecretaris respectievelijk het college van B&W ontstaat.

4. Rechten van betrokkenen

Aan de rechten van betrokkene wordt volgens een rechterlijke uitspraak onvoldoende invulling gegeven. De gemeente kijkt naar mogelijkheden om hier beter invulling aan te geven. Deze ontwikkelingen worden gevolgd. Aandacht voor tijdige afhandeling van inzageverzoeken is een aandachtspunt in verband met de (te) lange afhandelingsduur. Informatievergaring hiervoor is een proces dat over verschillende organisatieonderdelen verloopt en afhankelijk is van meerdere personen. Er zijn digitale middelen beschikbaar om deze informatie sneller en efficiënter te kunnen ontsluiten.
Bij overschrijding kan, na ingebrekestelling, een beroep worden gedaan op een dwangsom. Een dwangsom kan, na ingebrekestelling, oplopen tot maximaal € 1.442,00 per inzageverzoek.

Aanbevelingen:

4.1 Stuur als management nadrukkelijk(er) op de tijdige en volledige afhandeling van inzageverzoeken.

4.2 Geef managementinformatie over inzageverzoeken vorm en neem dit op in de monitor gegevensbescherming.

4.3 Onderzoek de mogelijkheid om geautomatiseerd naar persoonsgegevens te zoeken binnen het applicatielandschap.

5. Samenwerking

Het beheer van de overeenkomsten met derde partijen (verwerkers) en het controleren van gemaakte afspraken over beveiligingsmaatregelen met deze partijen verdient nog steeds extra aandacht en inspanning. Hiervoor is in 2020 een inventarisatie uitgevoerd die verder niet heeft geleid tot structurele beheersing en een actueel bijgehouden registratie van derde partijen. Derde partijen dienen zich aan de gemeente te verantwoorden over de beveiliging van persoonsgegevens die zij voor of in opdracht van de gemeente verwerken. Zonder volledig en actueel overzicht in deze partijen is niet vast te stellen of deze partijen om verantwoording is gevraagd en zijn eventuele risico's niet zichtbaar. De gemeente is hierdoor kwetsbaar, zeker als een of meerdere derde partijen de zaken rond beveiliging van (persoons)gegevens niet op orde hebben.

Aanbeveling:

5.1 Richt een centrale registratie van overeenkomsten in zodat het beheer van derde partijen inzichtelijk wordt gemaakt en bij eventuele kwetsbaarheden direct met de juiste partij contact kan worden gelegd.

6. Beveiliging

Periodiek dienen de gemaakte afspraken met derde partijen over de afgesproken beveiligingsmaatregelen te worden getoetst op bestaan en werking.

Aanbeveling:

6.1 Geef opdracht om deze toetsing door de proceseigenaren te laten uitvoeren.

6.2 Koppel deze verantwoording aan de aanbevolen centrale registratie.

Het periodiek controleren van autorisaties en het (inrichten van) periodieke controle op logbestanden verdient evenals in voorgaande jaren nog de nodige aandacht. Deels worden autorisaties centraal gekoppeld aan het hiervoor beschikbare systeem. Applicaties die hier (nog) niet op zijn aangesloten moeten op een andere manier worden gecontroleerd. Het koppelen van applicaties aan het centraal beschikbare systeem gaat trager dan wenselijk.
Een richtlijn (strategische standaard) voor controle van autorisaties is in 2021 opgesteld waarmee een aanbeveling uit het FG-verslag 2019-2020 is opgevolgd. Implementatie van deze strategische standaard is nog onvoldoende. Bovendien is vooralsnog onduidelijk of de hiervoor benodigde capaciteit en middelen beschikbaar zijn of beschikbaar worden gesteld.

Aanbeveling:

6.3 Maak bij het vaststellen van strategische standaarden direct daarop aansluitend een implementatieplan met een duidelijk tijdspad waarbinnen de implementatie moet plaatsvinden en stel de benodigde capaciteit en middelen hiervoor beschikbaar.

7. Verantwoording

Het aandachtsveld gegevensbescherming is continu in beweging. De technische ontwikkelingen gaan razendsnel en ook de daaraan verbonden nieuwe risico's. De gemeente heeft een hoog ambitieniveau en de wens om certificeerbaar te zijn voor gegevensbescherming. De visie van de gemeente Utrecht is dat zij een voorbeeldfunctie heeft in de sector voor wat betreft privacy en informatiebeveiliging. Dat dit verplichtingen schept moge duidelijk zijn. De praktijk is echter weerbarstiger.
De mate waarin de gemeente deze dreigingen het hoofd kan blijven bieden houdt nauw verband met de aanwezige kennis, expertise en beschikbare middelen en mensen. Als niet tijdig wordt ingespeeld op deze ontwikkelingen wordt het risico gelopen dat later extra hoge kosten moeten worden gemaakt voor herstel.
Het behalen van de doelen uit de Routekaart gegevensbescherming was hiervan afhankelijk. Deze routekaart is bij het einde van het programma gegevensbescherming vervallen. Hoewel in het nieuwe beleid sturingsmechanismen zijn opgenomen is de werking hiervan nog niet optimaal. Onduidelijk is hoe hierop in de praktijk op wordt gestuurd door het verantwoordelijk management. Bij het ontbreken van de noodzakelijke kennis en expertise, mensen en middelen om de doelen uit het vastgestelde beleid te behalen worden resultaten pas op een (veel) later moment bereikt dan wenselijk.

Aanbeveling:

7.1 Breng de ontwikkeling van de benodigde capaciteit, kennis en expertise op het gebied van gegevensbescherming periodiek in beeld en stuur vanuit het hoogste management en bestuur tijdig bij als hier tekorten blijken. Mede op basis van de diverse nieuwe (Europese) wet- en regelgeving is structurele aandacht hiervoor (meer dan) noodzakelijk.

8. Conclusies

Op het gebied van gegevensbescherming is er in 2024 en verder nog veel winst te behalen.

Met name zijn er tekortkomingen/verbeterpunten op het gebied van:
- Het (periodiek) vaststellen van het volwassenheidsniveau van de organisatie;
- Het tijdig uitvoeren en herzien van DPIA's, na 3 jaar (of eerder bij wijzigingen)
- Het beheer van de overeenkomsten met derde partijen (verwerkers);
- Het controleren van gemaakte afspraken over beveiligingsmaatregelen met derde partijen;
- Het aantoonbaar handhaven van bewaartermijnen;
- De periodieke controle van autorisaties;
- Het (inrichten van) en uitvoeren van periodieke controles op logbestanden.

Door het niet of onvoldoende voldoen aan de wettelijke vereisten kan de gemeente nog onvoldoende aantonen (of verantwoorden) of c.q. in welke mate zij aan de AVG, Wpg en de BIO voldoet.

06-11-2024,

Hans van Impelen
Functionaris voor gegevensbescherming (FG)

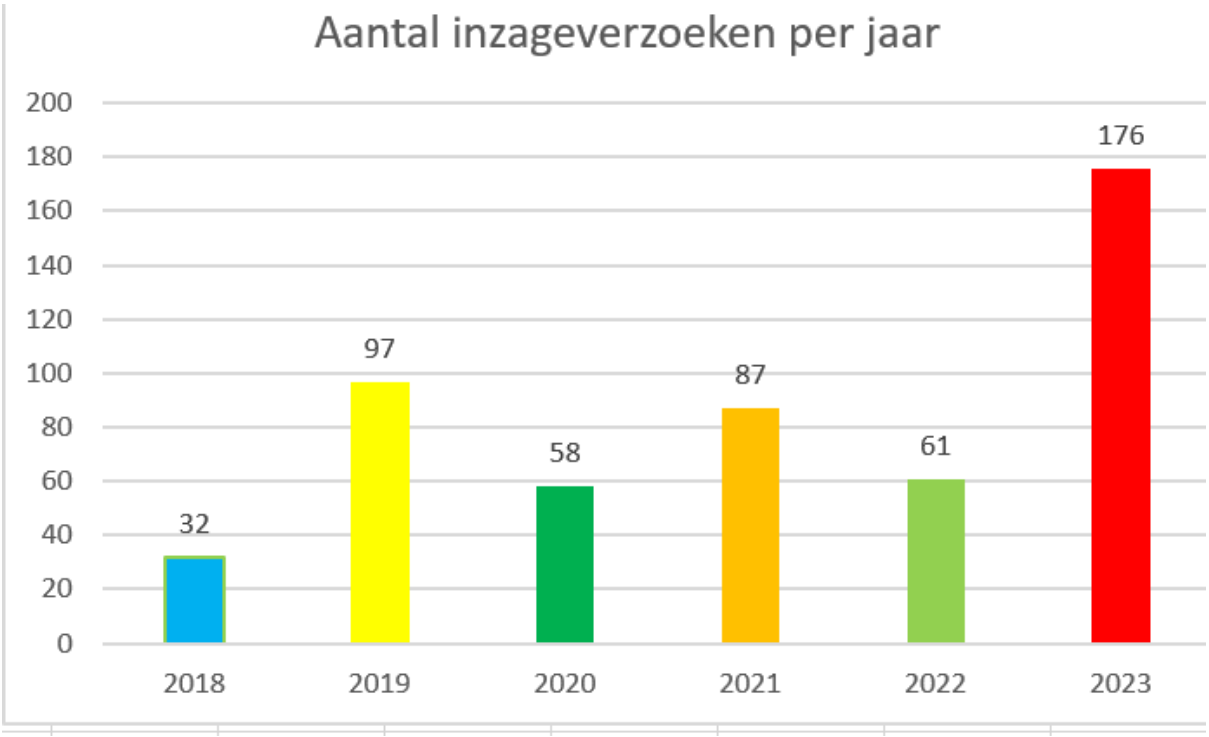
Bijlage 1 - Overzicht aantal DPIA's per organisatieonderdeel (Bron: SharePoint)

Organisatieonderdeel	Aantal vastgelegde documenten
2.01 Bedrijfsvoering- en strategie netwerk (BSN)	11
2.02 Ruimte	38
2.03 Vastgoedorganisatie Utrecht (VGU)	0
2.04 Openbare orde en veiligheid (OOV)	7
2.05 Culturele Zaken (CZ)	1
2.06 Maatschappelijke ontwikkeling (MO)	20
2.07 Wijken	1
2.08 Werk en inkomen (W&I)	41
2.09 Volksgezondheid (VG)	8
2.10 Vergunningen toezicht en handhaving (VTH)	10
2.11 Stadsbedrijven (SB)	11
2.12 Publiekszaken (PBZ)	10
2.13 Raadsorganen	0
Totaal	158

In 2023 is op 40 DPIA's FG advies gegeven. Hiervan zijn in totaal 11 DPIA's op de in de "Procesbeschrijving data protection impact assessment (dpia)" voorgeschreven plaats vindbaar.

Bijlage 2 - Overzicht rechten van betrokkenen

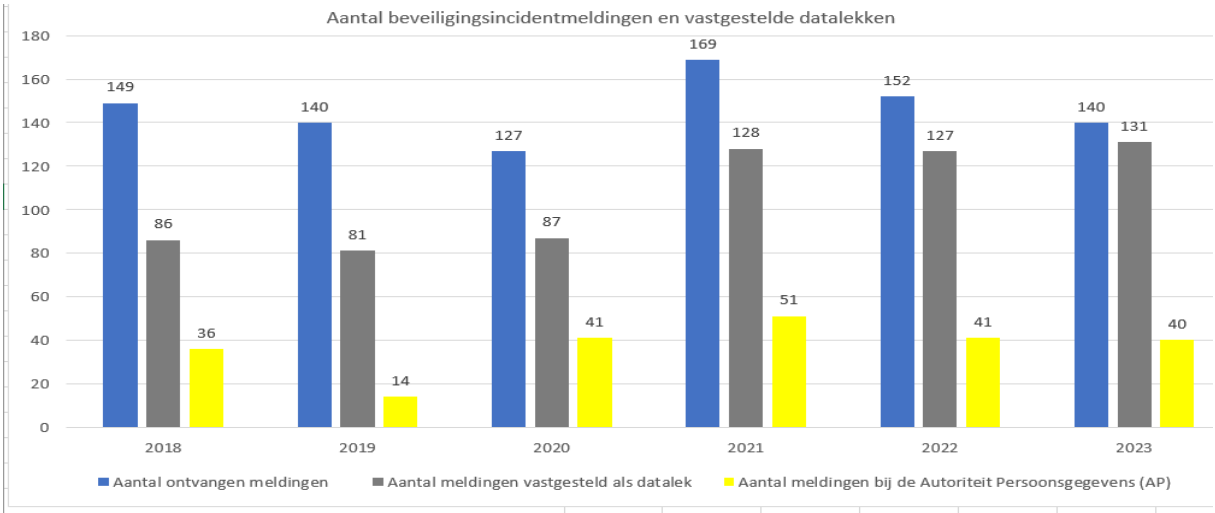
Bron: zaaksysteem	
Inzageverzoeken per jaar	**Aantal**
2018	**32**
2019	**97**
2020	**58**
2021	**87**
2022	**61**
2023	**176**
Eindtotaal	**511**



Het nagaan waar persoonsgegevens worden verwerkt is een tijdrovende aangelegenheid.
Bij niet tijdige besluitvorming op een inzageverzoek kan betrokkene, na ingebrekestelling, een beroep doen op een dwangsom waarvan het bedrag kan oplopen tot maximaal € 1.442,-.
Over eventuele correctie- en verwijderingsverzoeken zijn geen gegevens bekend.

Bijlage 3 - Overzicht datalekken

Bijlage 3 - Overzicht datalekken						
bron: zaaksysteem zaaktype “Melding datalek behandelen”						
Jaar:	2018	2019	2020	2021	2022	2023
Aantal ontvangen meldingen	149	140	127	169	152	140
Aantal meldingen vastgesteld als datalek	86	81	87	128	127	131
Aantal meldingen bij de Autoriteit Persoonsgegevens (AP)	36	14	41	51	41	40
Datalekken in percentage van de meldingen	58%	58%	69%	76%	84%	94%
Meldingen AP in percentage van de datalekken	42%	17%	47%	40%	32%	31%



Bron: zaaksysteem

Het register datalekken is een wettelijk verplichte registratie (AVG artikel 33 en artikel 32 en 33a Wpg).

De hierboven opgenomen overzichten bevatten meldingen die via de website van de gemeente Utrecht zijn ingediend en opgenomen in het register datalekken. Deze meldingen worden automatisch opgenomen in het zaaksysteem en via een interne mailsignalering worden de verschillende actoren geïnformeerd over de melding. Hierna wordt de melding beoordeeld en wordt de verdere opvolging en afhandeling opgepakt.

In 2022 werden 127 (84%) van de 152 ontvangen meldingen vastgesteld als datalek.
In 2023 werden 131 (94%) van de 140 ontvangen meldingen vastgesteld als datalek.
Het aantal datalekken dat bij de Autoriteit Persoonsgegevens (AP) is gemeld is in 2023 vergelijkbaar met 2022.
De oorzaak van datalekken is vaak terug te voeren op een menselijke fout die onder tijdsdruk wordt gemaakt.

Een typefout in een e-mailadres of automatische aanvulling van een e-mailadres zijn hier meestal de oorzaak van. Bij het verzenden van brieven komt het voor dat twee (of meer) brieven in één envelop worden verzonden, een verkeerde bijlage wordt toegevoegd of een onjuist of een voormalig adres wordt gebruikt.
Op de website van de gemeente Utrecht worden overzichten van datalekken gepubliceerd dat, op het moment van het schrijven van deze FG rapportage, is bijgewerkt tot juni 2023. Dit overzicht is niet actueel en wordt niet consequent bijgehouden.
Medio 2021 is deze veranderde werkwijze ingevoerd waarbij de meldingen bij de Autoriteit Persoonsgegevens door de organisatieonderdelen zelf worden verricht. Het tijdig aanvullen van de registratie datalekken met noodzakelijke informatie en documenten in het zaaksysteem is een blijvend punt van zorg en voldoet niet aan de wettelijke verplichtingen.
Periodieke rapportage en terugkoppeling naar de organisatie en naar inwoners geeft een onvolledig beeld zolang deze registratie niet actueel is.
Bovendien voldoet het register datalekken niet aan de in artikel 33 AVG en artikelen 32 en 33a Wpg opgenomen verplichtingen omdat de documentatie onvolledig is en het register niet tijdig wordt aangevuld met de wettelijk voorgeschreven documentatie met inbegrip van de feiten over de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.

Bijlage 4 - 10 tips voor professionele datalekregistratie

In 2022 en 2023 is de registratie van datalekken in het register datalekken (zaaksysteem) onvoldoende verbeterd. Zowel de tijdige afhandeling van datalekken als het toevoegen van de vereiste documentatie blijven onvoldoende.

Voor de volledigheid worden (nogmaals) de tips van de Autoriteit persoonsgegevens hieronder opgenomen.

AUTORITEIT
PERSOONSGEGEVENS

10 tips voor professionele datalekregistratie

Deze tips zijn zowel van toepassing op het registreren van datalekken die u verplicht bent te melden bij de Autoriteit Persoonsgegevens (AP) als om incidenten die u niet hoeft te melden. De tips vormen een aanvulling op de Q&A's over datalekken op onze website.

Omschrijf incidenten, de gevolgen en de corrigerende maatregelen **duidelijk en volledig.**

Maak expliciet onderscheid tussen **corrigerende en preventieve maatregelen**. Leg corrigerende maatregelen altijd vast in het datalekregister. Het kan nuttig zijn deze maatregelen mee te nemen in de plan-do-check-learn-act cyclus.

Voorkom versnippering van registraties: maak **één overzichtelijke registratie** die voor elk organisatieonderdeel tot op hetzelfde detailniveau wordt ingevuld. Overweeg bijvoorbeeld om de registratie inzichtelijk te maken voor alle medewerkers zodat zij het overzicht kunnen checken voordat zij zelf iets registreren.

Heeft uw organisatie een **functionaris gegevensbescherming** (FG)? Neem dan per incident op of de FG betrokken is en, zo ja, in welke mate.

Neem per incident op of het datalek is **gemeld bij de AP en de betrokken personen** en motiveer waarom dat wel of niet is gebeurd.

Wees **transparant naar de getroffen personen** als er een datalek is geweest. Communiceer hier duidelijk en tijdig over. Bewaar het bewijs van die communicatie en neem deze op in de registratie.

Stel een handleiding op of verzorg een training voor de **medewerkers die de datalekregistratie invullen.** Deze instructie kan onderdeel uitmaken van een gedocumenteerde meldingsprocedure voor de meldplicht datalekken.

Leg vast welke **andere organisaties** betrokken zijn geweest bij een inbreuk. Bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of subverwerkers. Dit is handig als een organisatie nieuwe verwerkersovereenkomsten sluit met de desbetreffende verwerkers.

Overweeg om de datalekken in te delen naar **aard, gevolgen en betrokkenen en mogelijke maatregelen.**

Bespreek de datalekregistratie regelmatig op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check-learn-act cyclus. Zo kunnen organisaties leren van fouten. De FG of privacycontactpersoon van uw organisatie kan bij deze besprekingen een actieve rol vervullen.