VIJFHEERENLANDEN

JAARRAPPORTAGE 2022 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

mevrouw mr. L. de Keijzer-Krens CIPP/E CIPM, juli 2023

Inhoudsopgave

Inleiding

Als gemeente werken we met persoonsgegevens van inwoners. Het is belangrijk dat we hier zorgvuldig mee omgaan en alles doen om te voorkomen dat deze gegevens in verkeerde handen komen. De wetgever heeft hiervoor richtlijnen opgesteld in de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Denk hierbij bijvoorbeeld aan kwaliteitseisen, zorgen voor inzagemogelijkheden voor betrokkenen en verplichtingen rondom transparantie.

De bestuursorganen van de gemeente zijn verantwoordelijk voor de verwerkingen van persoonsgegevens in onze gemeente. Het gaat vooral om het college van burgemeester en wethouders en de burgemeester als zelfstandig orgaan. De gemeenteraad is zelf verantwoordelijk voor de verwerkingen binnen de gemeenteraad en de griffie.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. De Functionaris Gegevensbescherming (FG) is de interne toezichthouder op de naleving van de AVG, Wpg en gerelateerde wetgeving en beleid. Onder het interne toezicht vallen niet alleen gegevensverwerkingen binnen de gemeente, maar ook verwerkingen door partijen die taken uitvoeren voor de gemeente. Tenzij sprake is van delegatie blijft het college namelijk eindverantwoordelijk en aansprakelijk als betrokkenen problemen ondervinden door gegevensverwerkingen binnen samenwerkingsverbanden e.d.

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 haar toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en haar de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van haar deskundigheid. De uitvoerende taken liggen bij de Privacy Officer.

De FG adviseert gevraagd en ongevraagd gemeentebreed en brengt verslag uit aan het college en de gemeenteraad. In dit verslag kijkt de FG terug op hoe binnen de gemeente in 2022 is omgegaan met privacygevoelige data en de eerder gedane aanbevelingen en geeft daarnaast aanbevelingen voor een optimale omgang met persoonsgegevens.

Samenvatting

Vijf jaar na inwerkingtreding van de AVG kan ik zeker constateren dat de organisatie vele stappen in de goede richting heeft gezet. Mijn conclusie over 2022 is dat er diverse ontwikkelingen zijn geweest en we ondanks beperkte capaciteit met elkaar goede stappen hebben gezet in de bescherming van persoonsgegevens en de naleving van relevante wetgeving. Dit zal de komende tijd verder moeten worden opgepakt. Ik adviseer om nader gevolg te geven aan de vorig jaar gedane aanbevelingen, te weten:

- Controleer alle gegevens in het register van verwerkingen op compleetheid en juistheid
- Maak een planning voor de uitvoering van nieuwe en te herziene DPIA's
- Vergroot de capaciteit van de Privacy Officer binnen team Control dan wel stel (een) privacy officer(s) binnen de teams aan
- Zet de huidige bewustwordingscampagne voort, aangevuld met een interactiever karakter zoals e-learning, phishing en/of escaperoom
- Betrek het subteam Privacy en Informatiebeveiliging (PIN) (vroegtijdig) bij regionale samenwerkingen en vertrouw op interne kennis
- Stel (kritische) vragen aan verwerkers, zowel vóór het aangaan van een overeenkomst als tijdens de uitvoering ervan
- Bespreek de verwerkersovereenkomst voordat de hoofdovereenkomst wordt aangegaan
- Creëer bewustwording voor beveiligingsincidenten, met name datalekken, en (de noodzaak voor) het melden hiervan
- Ken nieuwe medewerkers autorisaties toe die bij de functie horen en niet automatisch alle autorisaties die de vorige medewerker had
- Voorzie de betrokken teams van voldoende kennis en capaciteit voor de uitvoering van specifieke eisen rondom Wpg-verwerkingen

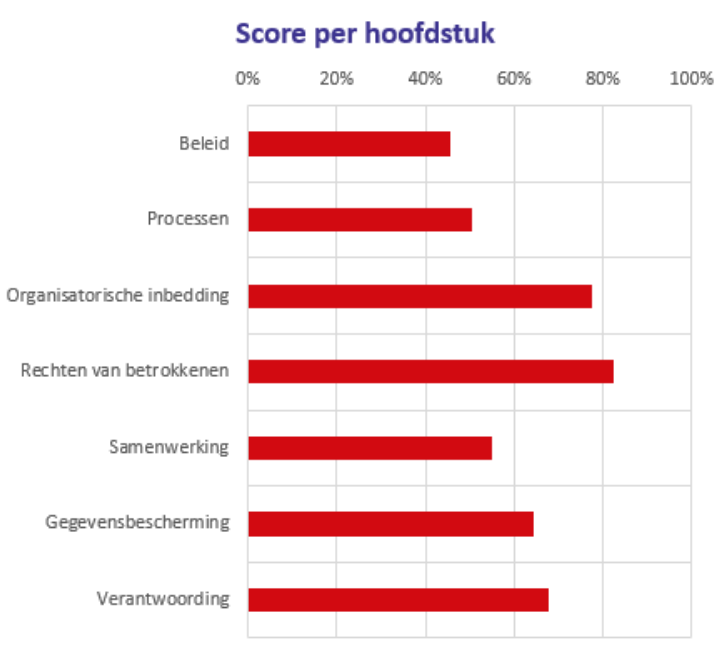
Daarnaast doe ik nog een aantal nieuwe aanbevelingen:

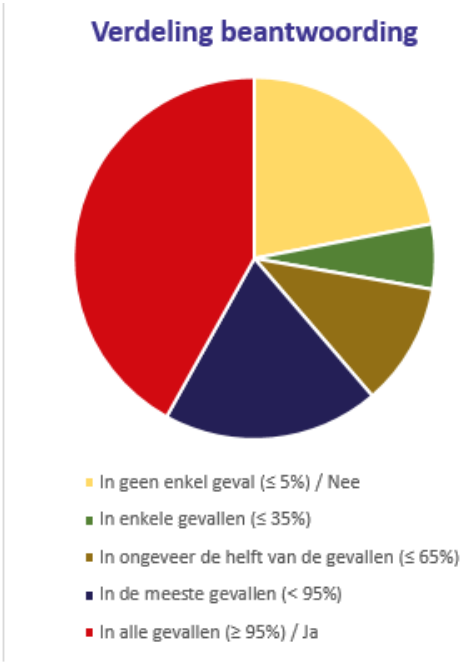
- Herzie het privacybeleid en neem hierin zaken mee rondom verantwoordelijkheden en zorg waar nodig voor een domeinspecifieke uitwerking
- Stel de e-learning rondom privacy en informatiebeveiliging verplicht
  Betrek PIN bij de communicatie over het aanbod en de noodzaak hiervan
- Inventariseer lopende samenwerkingsverbanden en controleer gemaakte afspraken
- Stel een Functionaris Gegevensbescherming aan voor de Wet politiegegevens

Alle aanbevelingen dragen bij aan het (meer) in control zijn van de bestuursorganen als verwerkingsverantwoordelijken, maar zorgen er ook voor dat medewerkers privacy makkelijker onderdeel kunnen maken van hun dagelijkse werkzaamheden. Dit vergroot de bereidheid tot en kwaliteit van de bescherming van persoonsgegevens.

Naleving AVG

De Informatiebeveiligingsdienst (IBD) heeft een AVG Borgingsproduct ontwikkeld.[1] Hiermee kunnen we toetsen in hoeverre we als organisatie in staat zijn om de naleving van de AVG te waarborgen. Het product bestaat uit diverse vragen over uiteenlopende onderwerpen, van beleid tot beveiliging, die deels te beantwoorden zijn met ja of nee en deels met een classificatie van in hoeveel procent van de gevallen dit van toepassing is. Op dit moment halen we een totaalscore van 63%. In de linker grafiek hieronder is uitgewerkt wat de totaalscore is per onderdeel. In de rechter grafiek is te zien hoe de classificatievragen zijn beantwoord.





De IBD heeft geen registratie van gemeenten die het product gebruiken en welke score zij behalen. Navraag bij regiogemeenten en op het landelijke forum van de Vereniging Nederlandse Gemeenten (VNG) heeft geen data van andere gemeenten opgeleverd. We kunnen onze score dus niet vergelijken, maar kunnen wel zelf conclusies trekken over onze ontwikkeling binnen de genoemde gebieden. Hierna zal ik toelichten hoe de scores per onderdeel tot stand zijn gekomen, wat de ontwikkeling is geweest en aanbevelingen doen om de scores verder te verbeteren.

[1] Zie https://www.informatiebeveiligingsdienst.nl/product/avg-borgingsproduct-3-0-toetsingskader/

Beleid

Op dit onderdeel scoren we 46% en dat komt met name door het in 2018 vastgestelde en gepubliceerde privacybeleid. Dit beleid moet namelijk periodiek worden herzien. Daarnaast is destijds een vrij algemeen beleid opgesteld dat op hoofdlijnen weergeeft hoe wij als organisatie met persoonsgegevens en data omgaan. Hierin staan bijvoorbeeld nog niet de rollen, taken en verantwoordelijkheden van alle betrokken personen en er is ook niet in opgenomen dat het management verantwoordelijk is voor het realiseren van de doelstellingen van het privacybeleid en advies moet inwinnen bij een privacyspecialist voor een nieuwe verwerking van persoonsgegevens. Daarnaast dient te worden geïnventariseerd voor welke domeinen specifiekere uitwerking van het privacybeleid nodig is. Denk hierbij ook aan het opstellen van een intern privacybeleid voor de omgang met gegevens van medewerkers.

Conclusie/aanbeveling
Herzie het privacybeleid en neem hierin zaken mee rondom verantwoordelijkheden en zorg waar nodig voor een domeinspecifieke uitwerking

Processen

Binnen dit onderdeel gaat het niet alleen om de inbedding van privacy in werkprocessen, maar ook om het hebben van een actueel register van verwerkingen, het verzorgen van Data Protection Impact Assessments (DPIA's) en het toepassen van een bewaar- en vernietigingsbeleid. Gemiddeld scoren we op dit onderdeel 51%.

In mijn vorige verslag heb ik voor dit onderdeel een tweetal aanbevelingen gedaan:

- *Controleer alle gegevens in het register van verwerkingen op compleetheid en juistheid.*

In 2022 is gestart met de update van het register van verwerkingen. Alle teams worden benaderd en het register wordt door de Privacy Officer persoonlijk doorgenomen met de proceseigenaren. De update zal in 2023 worden afgerond. Vervolgens kan ik een inhoudelijke controle doen van alle facetten rondom een verwerking, zoals de juiste grondslag, gegevensdeling met derden en gemaakte afspraken met leveranciers. Waar nodig kan vervolgens actie worden ondernomen, bijvoorbeeld het aanpassen van de verwerking of het maken van (aanvullende) afspraken, zoals verwerkersovereenkomsten.

Wel is al geconstateerd dat het in-, door- en uitstroomproces van medewerkers niet altijd goed loopt. Als een nieuwe medewerker binnenkomt, of een bestaande medewerker wijzigt van functie, dan worden bepaalde rechten aangevraagd. Vaak wordt gevraagd om de rechten van degene die hiervóór de betreffende functie uitvoerde, maar het is maar de vraag of dit de juiste rechten zijn voor de functie. Het kan bijvoorbeeld zijn dat deze persoon andere rollen of taken had waarvoor andere of aanvullende rechten zijn toegekend die voor de nieuwe medewerker niet aan de orde zijn. Ook wordt vaak gevraagd om een ruime toekenning van rechten die wellicht nu niet allemaal nodig zijn, maar om te voorkomen dat iemand in de toekomst tegen problemen aanloopt. Voor een zorgvuldige omgang met (privacygevoelige) data is het van belang een goede autorisatiestructuur te hebben waarin rechten zijn gekoppeld aan functies. Hierdoor is het aanvragen en toekennen van de juiste rechten niet alleen eenvoudiger, maar ook beter te controleren en kunnen we daardoor aantonen dat we voldoen aan de wet- en regelgeving op dit gebied. Diverse teams zijn hiermee bezig (geweest), dus komend jaar zal ik de ontwikkelingen op dit gebied monitoren. Zie ook onder 'Gegevensbescherming'.

- *Maak een planning voor de uitvoering van nieuwe en te herziene DPIA's.*

De gemeente kan, zowel voor bestaande als nieuwe processen, verplicht zijn een gegevensbeschermingseffectbeoordeling, oftewel een Data Protection Impact Assessment (DPIA), uit te voeren.

Bij nieuwe werkprocessen en/of als processen worden opgenomen in het Zaaksysteem wordt hiervoor minimaal een eenvoudige variant van een DPIA uitgevoerd. Dit wordt via het desbetreffende zaaktype in Zaaksysteem opgevoerd door de proceseigenaar. Vervolgens controleer ik of de verwerking voldoet aan de wettelijke beginselen en/of het proces een uitgebreidere DPIA nodig heeft.

In 2022 is een verkorte DPIA gestart en/of afgerond voor de volgende verwerkingen:
- de zogenaamde Peutermonitor
  afgerond, positief advies FG met kanttekening waarover college heeft besloten
- sociale kaart (Zorg4Vijfheerenlanden)
  tot op heden niet afgerond
- gegevensdeling Avres in verband met het verstrekken van leefgeld aan Oekraïners
  afgerond, positief advies FG
- Agressieprotocol en registratie van incidenten
  afgerond, positief advies FG met voorwaarde rondom vastlegging

Daarnaast is een uitgebreide DPIA opgesteld voor de volgende verwerkingen:
- softwarepakket PGAx
  betreft meerdere verwerkingen met vergelijkbare partners, is in 2021 gestart en in 2022 afgerond, positief advies FG
- gegevensdeling Avres in verband met Inburgeringswet
  afgerond, positief advies FG
- gegevensdeling regiogemeente vanwege uitbesteed toezicht Wmo 2015 en Jeugdwet
  afgerond, positief advies FG

Zodra het register in zijn geheel is herzien zal ik een overzicht maken van verwerkingen waarvoor een DPIA moet worden uitgevoerd of waarvoor een eerder uitgevoerde DPIA moet worden herzien. Hierbij zal in eerste instantie de focus liggen op processen met gevoelige data, zoals bijvoorbeeld binnen het sociaal domein, maar ook processen die gegevens van personeel raken binnen het team HRM.

Organisatorische inbedding
De score voor dit onderdeel is 78% en dit komt met name door de aanstelling van de FG en de positionering van deze functie binnen de organisatie. Aandachtspunten binnen dit onderdeel zijn:
- de totale capaciteit aan privacyspecialisten is (te) beperkt;
- medewerkers hebben geen (aantoonbaar) bewustwordingstraject gevolgd.

Voor beide aandachtspunten heb ik in mijn vorige verslag een aanbeveling gedaan:

- *Vergroot de capaciteit van de Privacy Officer binnen team Control dan wel stel (een) privacy officer(s) binnen de teams aan.*

Eerder is al geconstateerd dat veelal te weinig privacykennis aanwezig is bij de teams. De ondersteuning die wordt gevraagd van het subteam Privacy en Informatiebeveiliging (PIN), bestaande uit de FG, de Privacy Officer en de Chief Information Security Officer (CISO), is te groot voor de aanwezige capaciteit. Naar aanleiding hiervan hebben gesprekken plaatsgevonden binnen de directie en netwerkmanagers en tussen diverse netwerkmanagers en de FG en Privacy Officer. Dit zal komend jaar voortgang moeten krijgen, want deze aanbeveling is zeker nog actueel. Daarnaast verwijs ik in dit kader alvast naar hetgeen staat onder ‘Verantwoording’. Het management is verantwoordelijk voor de privacybescherming bij de uitvoering van taken, maar zal hiervoor ondersteuning vragen aan privacyspecialisten. Deze kan nu slechts beperkt worden geboden.

Door meer capaciteit te hebben aan mensen met specifieke privacykennis kunnen medewerkers ook sneller en vaker worden geholpen bij hun dagelijkse activiteiten, kan meer ondersteuning worden geboden bij zaken zoals datalekken en DPIA's, maar kunnen ook nieuwe, zowel wettelijke als organisatorische, ontwikkelingen sneller en efficiënter worden uitgewerkt en opgevolgd. Naast vergroting van de capaciteit bij de teams is het natuurlijk ook mogelijk te denken aan privacyfunctionarissen per domein. Deze zijn breder in te zetten op elk vraagstuk waar ze op dat moment nodig zijn.

Voor welke invulling ook wordt gekozen, ik wil benadrukken dat privacy niet iets is van bijvoorbeeld PIN. Alle teams zijn zelf verantwoordelijk voor hun eigen werk én hebben binnen hun werk in bepaalde mate te maken met de verwerking van persoonsgegevens. Het is dan ook noodzakelijk dat iedere medewerker op de hoogte is van de regelgeving op dit gebied en de betekenis ervan voor hun eigen werk. De AVG is hierin te vergelijken met bijvoorbeeld de Algemene wet bestuursrecht (Awb). Niet alleen Juridische Zaken houdt zich hiermee bezig, maar iedere medewerker moet een bepaalde kennis hebben. Voor de AVG is dit niet anders. Als medewerkers onvoldoende kennis hebben lopen onze inwoners een groter risico op onjuist gebruik van hun gegevens. Daarnaast loopt de organisatie een groter risico op datalekken met als gevolg financiële schade, bijvoorbeeld een boete van de AP, en imagoschade. Dit houdt ook verband met de volgende aanbeveling.

Verantwoording

Dit onderdeel scoort 68% aangezien ik jaarlijks rapporteer over mijn bevindingen en ook wordt geëvalueerd op informatiebeveiliging. De evaluatie op de naleving van de AVG kan worden verbeterd. Het gaat hier namelijk niet alleen om toezicht door de FG, maar ook om een evaluatie vanuit het management, aangezien zij de verantwoordelijkheid hebben voor de privacybescherming bij de uitvoering van taken. Hiervoor zal ondersteuning worden gevraagd van privacyspecialisten, dus ik verwijs naar mijn eerder besproken aanbeveling rondom het gebrek aan capaciteit.

- *Zet de huidige bewustwordingscampagne voort, aangevuld met een interactiever karakter zoals e-learning, phishing en/of escaperoom.*

De bewustwordingscampagne '5 voor veilig' is voortgezet door berichten op intranet en het bedanken van melders van beveiligingsincidenten, waaronder datalekken, met een chocoladereep. Het aantal meldingen gaat gestaag omhoog. Mensen vragen ook vaker of iets moet worden gemeld als datalek. In het algemeen merken we dat medewerkers meer privacy gerelateerde vragen stellen, waardoor de juiste collega's eerder in een proces worden betrokken. Privacy is namelijk zoals gezegd niet iets van PIN, maar een integraal onderdeel van de vakinhoud (net zoals andere relevante wetgeving).

Directie en management hebben besloten het bewustwordingstraject uit te breiden met onder andere een e-learning traject en een phishing campagne. Er is onderzoek gedaan naar diverse bedrijven die e-learning e.d. aanbieden en hoe een en ander is in te passen in reeds aanwezige systemen. Begin dit jaar is een aanbieder gekozen en in het derde kwartaal wordt gestart met het aanbieden van leerlijnen aan alle medewerkers. De e-learning wordt aangeboden via de interne 5HL Academie waarbij de voortgang per medewerker wordt geregistreerd. Hiermee kan dus vervolgens worden aangetoond dat alle medewerkers het specifiek voor hen geldende bewustwordingstraject hebben gevolgd.

Aandachtspunt hierbij is dat ik heb begrepen dat dit e-learning-traject geen verplicht karakter krijgt. Dit brengt als risico met zich mee dat medewerkers de e-learning niet, of niet op een serieuze wijze, volgen met als consequentie de risico's op onjuist gebruik van gegevens, financiële schade en imagoschade. Aangezien iedereen binnen zijn werk in bepaalde mate te maken heeft met regelgeving rondom privacy is het van belang dat iedereen de geboden leerlijn volgt. Een verplicht karakter maakt ook duidelijk dat het hebben van kennis op dit gebied voor iedereen noodzakelijk is en dat dit wordt onderstreept door zowel verwerkingsverantwoordelijken als management.

Conclusie/aanbeveling
Stel de e learning rondom privacy en informatiebeveiliging verplicht
Betrek PIN bij de communicatie over het aanbod en de noodzaak hiervan

Rechten van betrokkenen

Een groot onderdeel van de AVG is de transparantie richting betrokkenen, oftewel de mensen van wie wij persoonsgegevens verwerken. Organisaties zijn verplicht mensen goed te informeren over wat er met hun data wordt gedaan en waarom, zowel vóór een verwerking als op verzoek van een betrokkene. In 2018 is hiervoor een privacyverklaring opgesteld en deze is meermaals aangevuld. Ook is een procedure ontwikkeld, zodat betrokkenen via DigiD eenvoudig en snel een verzoek kunnen indienen en ook op korte termijn een reactie ontvangen. In 2022 zijn er geen verzoeken ontvangen. Dit jaar al wel een aantal, dus mensen weten deze mogelijkheid zeker te vinden. Alle ontwikkelingen hebben geleid tot een gemiddelde score van 83% op dit onderdeel. Dit is zeker het noemen waard, want het geeft aan dat we goede omgang met data - en transparantie hierover - binnen onze gemeente belangrijk vinden.

Samenwerking

De gemeente werkt veelal samen met partners. Het kan hierbij gaan om grote samenwerkingen in de regio, maar ook om organisaties die wij een deel van onze taken laten uitvoeren. Op dit onderdeel scoren we nu 55%. We maken wel afspraken met deze partijen, maar hier is niet altijd iemand met privacykennis bij betrokken. Ook wordt achteraf niet getoetst of de gemaakte afspraken worden nageleefd. In mijn vorige verslag heb ik voor dit onderdeel al een aantal aanbevelingen gedaan:

- *Betrek PIN (vroegtijdig) bij regionale samenwerkingen en vertrouw op interne kennis.*

PIN heeft actief gewerkt aan eigen zichtbaarheid en het verkleinen van de afstand door het inplannen van kennismakingsafspraken en meeloopdagen, deelname aan Town Hall bijeenkomsten en het houden van een pubquiz. Dergelijke activiteiten zullen worden voortgezet.

Ook is PIN diverse malen betrokkenen bij nieuwe verwerkingen, onder andere richting Avres rondom regelingen voor vluchtelingen uit Oekraïne. Ik zie een stijgende lijn op dit gebied. Meer mensen weten PIN (vroegtijdig) te vinden en handelen naar gegeven adviezen. De continue bewustwordingscampagne zal hieraan (blijven) bijdragen. Het is natuurlijk lastig om te zeggen dat de betrokkenheid voldoende was, want ik kan niet oordelen over zaken waarbij PIN niet is betrokken en waarvan ik wellicht in het geheel niet afweet. Er is geen volledig beeld over de status van afspraken en gedane controles bij verbonden partijen en leveranciers. Dit zal dan ook een aandachtspunt zijn voor de komende jaren.

Conclusie/aanbeveling
Inventariseer lopende samenwerkingsverbanden en controleer gemaakte afspraken

- *Stel (kritische) vragen aan verwerkers, zowel vóór het aangaan van een overeenkomst als tijdens de uitvoering ervan.*

Afgelopen jaar zijn diverse verwerkersovereenkomsten gesloten en hierin liepen de contacten goed. Vragen zijn beantwoord en opmerkingen zijn overgenomen. De continue bewustwordingscampagne zal hieraan (blijven) bijdragen. Daarnaast controleer ik periodiek ingekomen stukken rondom gegevensverwerkingen in het Zaaksysteem en spreek mensen waar nodig aan op het betrekken van PIN bij dergelijke vraagstukken.

- *Bespreek de verwerkersovereenkomst voordat de hoofdovereenkomst wordt aangegaan.*

Het blijkt dat het inkoopproces rondom aanbestedingen niet voor iedereen duidelijk is. Collega's mogen veel zelf regelen en niet iedereen komt (vooraf) langs voor advies. Dit is vaak wel noodzakelijk, bijvoorbeeld voor het stellen van vragen en maken van afspraken. Zoals vorig jaar aangegeven wordt deze kwestie, en dan met name de risico's, komende tijd meegenomen in de bewustwordingscampagne.

Gegevensbescherming

De beveiliging van persoonsgegevens raakt natuurlijk de algemene beveiliging van data van de gemeente. Als er een beveiligingsincident is waarbij direct persoonsgegevens zijn betrokken kan sprake zijn van een datalek. Maar ook andere incidenten, bijvoorbeeld een buitendeur die openstaat, kan leiden tot een inbreuk op de persoonsgegevens waarvoor wij verantwoordelijk zijn. We hebben daarom een procedure ontwikkeld voor het melden van alle incidenten en vervolgens wordt vanuit PIN gekeken of sprake is van een datalek en welke acties nodig zijn, bijvoorbeeld beveiliging aanpassen of datalek melden bij de Autoriteit Persoonsgegevens of de betrokkene(n). Medewerkers kunnen deze meldingen doen via het Zaaksysteem. In de bijlage is een overzicht opgenomen van de in 2022 gemelde beveiligingsincidenten (31 zaken), waaronder datalekken (15 zaken), en de afhandeling ervan. Met name dankzij deze procedure scoren we op dit onderdeel 64%.

Gezien de hoeveelheid data die binnen de gemeente wordt verwerkt kan ik niet anders dan concluderen dat nog steeds te weinig datalekken worden gemeld. In mijn vorige verslag heb ik hiervoor al een aanbeveling gedaan:

- *Creëer bewustwording voor beveiligingsincidenten, met name datalekken, en (de noodzaak voor) het melden hiervan.*

Deze is nog steeds actueel en hiervoor is dus blijvende aandacht noodzakelijk. Dit wordt meegenomen in de bewustwordingscampagne en meer specifiek in het e-learning aanbod. Hiervoor geldt ook hetgeen ik hierboven aangeef over het al dan niet verplichte karakter van e-learning en de risico's hierbij.

Naast de omgang met incidenten valt onder dit onderdeel ook het hebben van inzicht in de risico's van de verwerking van persoonsgegevens en hoe hiermee om wordt gegaan. Op dit moment is het afhankelijk van de professionaliteit van de functioneel beheerder dan wel applicatiebeheerder, en in hoeverre hun advies wordt opgevolgd binnen een team, hoe met data in systemen wordt omgegaan. Denk bijvoorbeeld aan het toekennen van autorisaties, in mijn vorige verslag heb ik hiervoor een aanbeveling opgenomen:

- *Ken nieuwe medewerkers autorisaties toe die bij de functie horen en niet automatisch alle autorisaties die de vorige medewerker had.*

In 2022 is een begin gemaakt met het opstellen van beheerplannen voor applicaties. De organisatie neemt hiermee stappen in de juiste richting. Men realiseert zich dat de gemeente veel groter is geworden en dat professionalisering nodig is. Het werk wordt wel uitgevoerd, maar op een omslachtige manier. Als een medewerker in- of doorstroomt moeten op diverse plaatsen autorisaties worden aangevraagd, beoordeeld en doorgevoerd. Risico hierbij is dat medewerkers te weinig of teveel autorisaties krijgen. Met te weinig autorisaties kunnen mensen hun werk niet (goed) doen, waardoor nieuwe aanvragen nodig zijn en alle processen weer gaan lopen. Teveel autorisaties kunnen zorgen voor verkeerd gebruik van data en overtreding van wetgeving. De ontwikkeling die gaande is, waaronder duidelijk beleid en een goed ingericht proces, zorgt voor minder risico's, kortere lijnen en snellere controles.

Tijdens het opstellen van de beheerplannen is duidelijk geworden dat niet alleen het functioneel beheer van applicaties een aandachtspunt is, maar dat er aandachtspunten zijn binnen de gehele informatiehuidhouding (teams Documentaire Informatievoorziening, Informatisering en Automatisering). De rollen van de verschillende teams ten opzichte van elkaar zijn onvoldoende duidelijk waardoor projecten soms naast in plaats van met elkaar plaatsvinden. Hierbij lopen we het risico dat zaken op tegenstrijdige manieren worden ingeregeld of dat zaken in het geheel over het hoofd worden gezien. Dit is al onderkend binnen de organisatie en er komt een Programmamanager om de teams hierbij te ondersteunen.

Verantwoording

Dit onderdeel scoort 68% aangezien ik jaarlijks rapporteer over mijn bevindingen en ook wordt geëvalueerd op informatiebeveiliging. De evaluatie op de naleving van de AVG kan worden verbeterd. Het gaat hier namelijk niet alleen om toezicht door de FG, maar ook om een evaluatie vanuit het management, aangezien zij de verantwoordelijkheid hebben voor de privacybescherming bij de uitvoering van taken. Hiervoor zal ondersteuning worden gevraagd van privacyspecialisten, dus ik verwijs naar mijn eerder besproken aanbeveling rondom het gebrek aan capaciteit.

Wet politiegegevens (Wpg)

Het borgingsproduct is opgesteld voor het evalueren van de naleving van de AVG. Aangezien ik echter, bij het gebrek aan een voor de Wpg aangestelde FG, vorig jaar ook heb opgetreden als FG van de Wpg heb ik destijds ook een aanbeveling gedaan:

- *Voorzie de betrokken teams van voldoende kennis en capaciteit voor de uitvoering van specifieke eisen rondom Wpg-verwerkingen.*

In 2022 is in company een training aangeboden aan alle boa's en enkele andere betrokkenen bij de Wpg. Gezien het verloop zou op termijn een herhaling wenselijk zijn.

Audits

Vanuit de Wpg hebben we de verplichting om elk jaar een interne Wpg-audit uit te voeren en ééns per vier jaar een externe audit te laten doen door een daartoe gecertificeerde toetser. De interne audit over het jaar 2021 (en daarvoor) heeft in februari 2022 plaatsgevonden. De externe audit over dezelfde periode in december 2022. Het auditrapport is aan het college verstrekt en, samen met het hieruit voortvloeiende verbeterplan, toegestuurd aan de Autoriteit Persoonsgegevens.

Gebleken is dat we op vrijwel geen enkel punt voldoen aan de wet- en regelgeving. Dit was in zoverre ook geen verrassing, maar het is nu wel van belang om hiermee voortvarend aan de slag te gaan. Komend jaar moet een (wettelijk verplichte) her-audit plaatsvinden in verband met de geconstateerde verbeterpunten bij de externe audit. Tevens dient een nieuwe interne audit plaats te vinden.

Aangezien we als organisatie zorgvuldig met persoonsgegevens van inwoners om moeten (én willen) gaan, is het van belang de verbeterpunten voortvarend op te pakken. Dit zodat we komend jaar bij de her-audit kunnen aantonen dat in ieder geval stappen zijn gezet. Overigens kijkt de Autoriteit Persoonsgegevens ook mee, want zowel de resultaten van de externe audit als die van de her-audit worden toegestuurd.

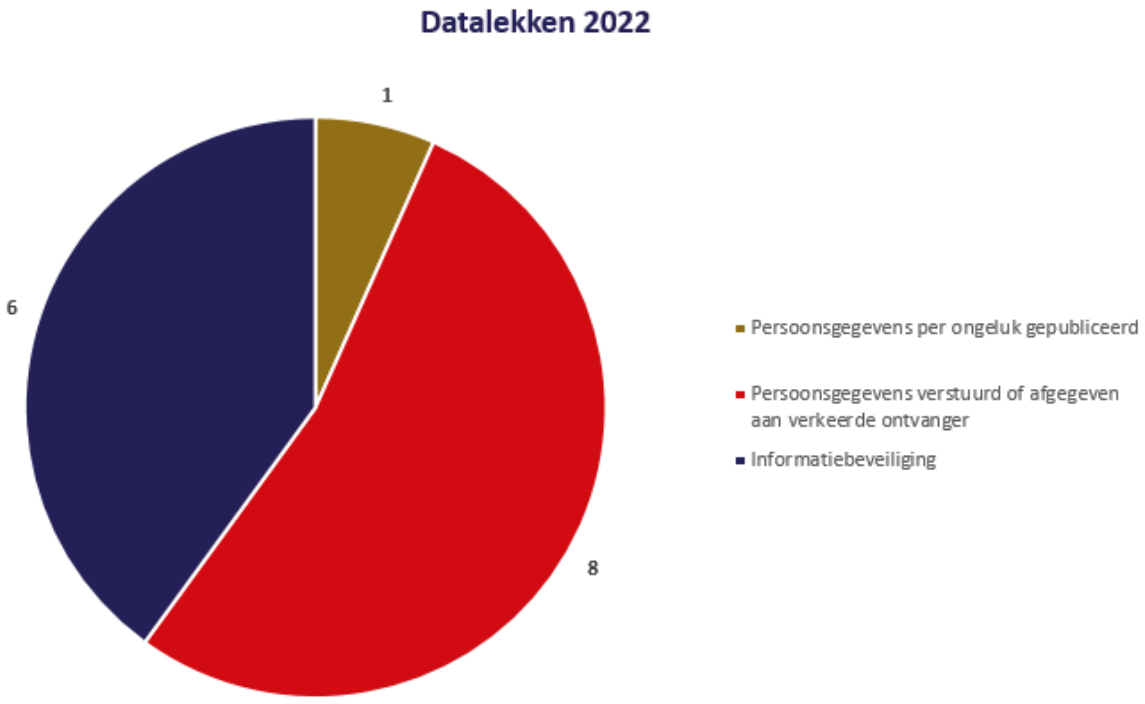
Begin dit jaar is een werkgroep gestart om de verbeterpunten uit te (laten) voeren. Er zat weinig voortgang in, dus dit heeft al de nodige aandacht gehad. Inmiddels worden er stappen gezet en dit zal komend jaar in ieder geval mijn aandacht houden. Overigens ben ik formeel niet aangesteld als FG voor de Wpg, maar alleen voor de AVG. Wel heb ik vooralsnog als zodanig opgetreden en zal dit komend jaar ook blijven doen, maar er dient formeel alsnog een FG voor de Wpg moeten worden aangesteld.

Conclusie/aanbeveling
Stel een Functionaris Gegevensbescherming aan voor de Wet politiegegevens

Bijlage - beveiligingsincidenten 2022

In 2022 zijn er 31 beveiligingsincidenten gemeld.

Van deze 31 meldingen zijn er 15 gekwalificeerd als een datalek, hieronder gespecificeerd naar de meest voorkomende categorieën.



Hier is goed te zien dat het bij datalekken met name gaat om zogenaamde menselijke fouten. Het blijft dus zaak om mensen bewust om te laten gaan met persoonsgegevens.

Het gaat om de volgende zaken:

Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger (8)

- Brief aan verkeerde ontvanger verstuurd. Gezien reeds bekende gegevens en geringe impact betrokkene datalek niet gemeld aan betrokkene en Autoriteit Persoonsgegevens.
- E-mail aan verkeerde ontvanger verstuurd. Gezien reeds openbare inhoud geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.
- Stukken met gevoelige informatie aan verkeerde ontvanger verstuurd. Gemeld aan betrokkene, niet aan Autoriteit Persoonsgegevens.
- E-mail aan verkeerde ontvanger verstuurd. Gezien geen gevoelige informatie en direct verwijderen van mail geen melding gedaan bij betrokkenen en Autoriteit Persoonsgegevens.
- E-mail aan verkeerde ontvanger verstuurd. Gemeld aan betrokkene, niet aan Autoriteit Persoonsgegevens.
- Foutieve bijlage meegestuurd bij brief. Gezien openbaarheid van gegevens geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.
- E-mail aan verkeerde ontvanger verstuurd. Gezien geen gevoelige informatie en direct verwijderen van mail geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.
- Stukken met gevoelige informatie aan verkeerde ontvanger verstuurd. Gezien betrouwbare ontvanger en direct verwijderen van mail geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.

Persoonsgegevens per ongeluk gepubliceerd (1)

- Brief onjuist geanonimiseerd waardoor naam korte tijd online heeft gestaan. Gezien geringe impact geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.

Informatiebeveiliging (6)

- Stukken over verstrekte subsidies achtergebleven op vergadertafel. Gezien geen gevoelige en vooral zakelijke inhoud geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.
- Fout in softwarepakket waardoor men na inloggen mogelijk persoonsgegevens van anderen kon inzien. Leverancier heeft dit na constatering direct opgelost. Gezien de geringe impact geen melding gedaan bij betrokkenen, maar gezien het brede gebruik van de software wel gemeld bij Autoriteit Persoonsgegevens.
- Oude dossiers lagen in kasten op een afdeling in plaats van in het centrale archief. Gezien geringe impact niet gemeld aan betrokkene en Autoriteit Persoonsgegevens.
- Medewerker onterecht toegang verkregen tot gezamenlijke mailbox vanwege niet volgen van juiste procedure. Gezien geringe impact niet gemeld aan betrokkenen en Autoriteit Persoonsgegevens.
- Het bevragen van persoonsgegevens vanuit een specifiek softwarepakket was zeer breed binnen de organisatie mogelijk. Dit is niet per se een datalek, maar zou het mogelijk kunnen veroorzaken. Aangezien het uitgangspunt binnen de organisatie is om beperkte autorisaties te hanteren is dit na constatering direct aangepast. Gezien geringe impact niet gemeld aan betrokkenen en Autoriteit Persoonsgegevens.

In alle zaken is het proces besproken met de betrokken medewerker(s) en zijn waar nodig aanpassingen gedaan.