VIJFHEERENLANDEN

JAARRAPPORTAGE 2023 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

mevrouw mr. L. de Keijzer-Krens CIPP/E CIPM, april 2024

Inhoudsopgave

Inleiding

Als gemeente werken we met persoonsgegevens van inwoners. Het is belangrijk dat we hier goed mee omgaan en alles doen om te voorkomen dat deze gegevens in verkeerde handen komen. De wetgever heeft hiervoor regels opgenomen in de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Denk bijvoorbeeld aan eisen aan de kwaliteit, zorgen voor inzagemogelijkheden voor betrokkenen en regels rondom openheid.

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) controleert in Nederland of organisaties zich houden aan de privacyregels. De Functionaris Gegevensbescherming (FG) controleert intern of de gemeente zich houdt aan de regels uit de AVG, Wpg en andere privacywetgeving en beleid. Onder de interne controle vallen niet alleen gegevensverwerkingen binnen de gemeente, maar ook verwerkingen door partijen die taken uitvoeren voor de gemeente. Behalve als het gaat om delegatie blijft het college namelijk eindverantwoordelijk en aansprakelijk als betrokkenen problemen hebben door gegevensverwerkingen binnen samenwerkingen e.d.

Het college moet erop toezien dat de FG goed en op tijd wordt betrokken bij alle zaken die te maken hebben met de bescherming van persoonsgegevens. Daarnaast moet de FG worden geholpen door haar toegang te geven tot persoonsgegevens en verwerkingen daarvan. En door haar de middelen te geven voor het uitvoeren van de taak en het in stand houden 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 in 2023 is omgegaan met privacygevoelige data en de eerdere aanbevelingen voor een zo goed mogelijke omgang met persoonsgegevens. Ook wordt kort vooruitgekeken naar 2024.

Samenvatting

Mijn conclusie over 2023 is dat de organisatie veel stappen in de goede richting heeft gezet en dat we ondanks beperkte capaciteit met elkaar goede stappen hebben gezet in de bescherming van persoonsgegevens en het voldoen aan de regelgeving. Dit geldt vooral voor de AVG, de Wpg blijft hierin nog wat achter. Dit zal de komende tijd verder moeten worden opgepakt.

Wel krijgen we regelmatig signalen dat mensen privacy en informatiebeveiliging los zien van hun vakinhoudelijke werk. Het is alleen zo dat alle regelgeving op dit gebied onderdeel is, of zou moeten zijn, van de vakinhoud. Natuurlijk verschilt het voor iedere medewerker hoeveel dit is, maar het borgen van privacy en informatiebeveiliging binnen de organisatie is een taak van iedereen. Mijn doel voor 2024 is dat mensen niet alleen zeggen dat ze het belangrijk vinden, maar dat ze dit ook in daden laten zien en waar nodig voorrang geven.

Natuurlijk zie ik ook dat op verschillende fronten veranderingen gaande zijn. Dit zijn meer organisatorische zaken, zoals de komst van een nieuwe gemeentesecretaris en het onderzoek naar de zelforganisatie (de manier waarop de organisatie sinds de fusie in 2019 werkt). Ondanks dat dit niet direct te maken heeft met de bescherming van persoonsgegevens, kan het wel gevolgen hebben voor de manier waarop de organisatie werkt en daardoor voor medewerkers. Dit alles kan een positief resultaat hebben in de uitvoering van de (eerder) gedane aanbevelingen.

Met elkaar moeten we aandacht houden voor privacy en informatiebeveiliging en niet uit het oog verliezen dat we werken met data, zoals persoonsgegevens, van inwoners. Niet alleen zijn wij wettelijk verplicht hier verstandig mee om te gaan, maar dit raakt ook de kern van waar onze organisatie voor staat.

Ik adviseer om verder uitvoering te geven aan de eerder gedane aanbevelingen:

- Herzie het privacybeleid en neem hierin zaken mee rondom verantwoordelijkheden en zorg waar nodig voor een domeinspecifieke uitwerking.
- Inventariseer lopende samenwerkingsverbanden en controleer gemaakte afspraken.

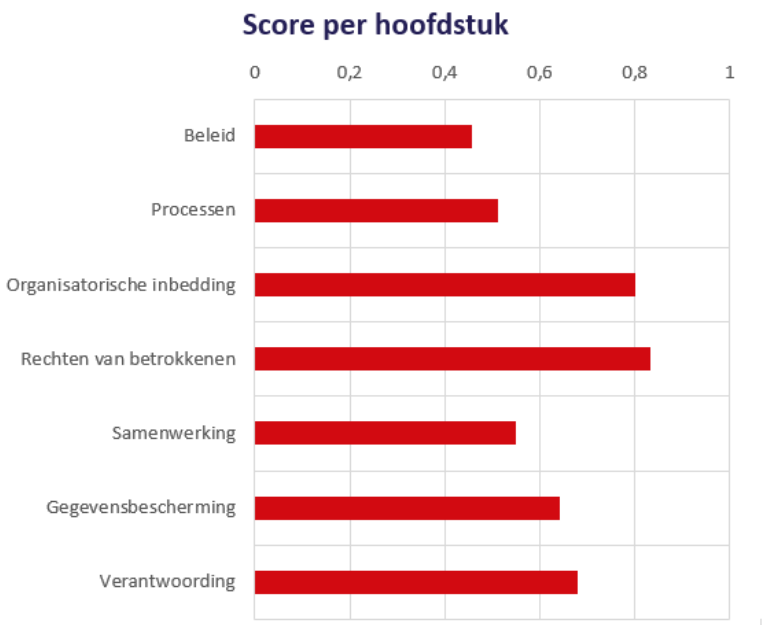
Daarnaast doe ik nog een aantal nieuwe aanbevelingen over het voldoen aan de Wet politiegegevens (Wpg):

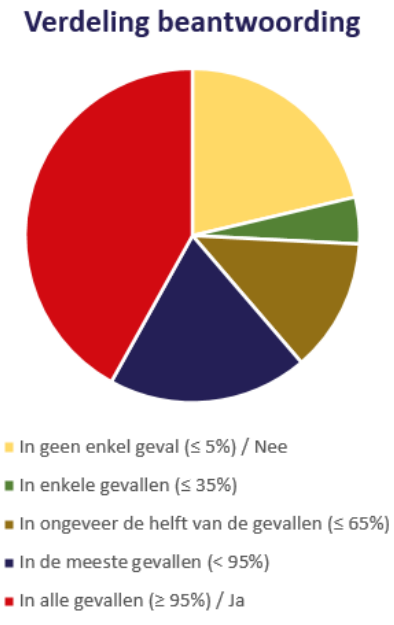
- Voer alsnog per omgaande de her-audit uit en stuur het rapport aan AP.
- Voer in 2024 een interne audit uit over zowel 2022 als 2023.

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 werk. 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 hoe we als organisatie voldoen aan de AVG. Het product bestaat uit verschillende vragen over allerlei onderwerpen, van beleid tot beveiliging, die voor een deel te beantwoorden zijn met ja of nee en voor een deel met een classificatie van in hoeveel procent van de gevallen dit geldt. Op dit moment halen we een totaalscore van 64%. Dit is een kleine stijging vergeleken met 2022 door de start van de e-learning in de tweede helft van 2023. In de linker grafiek hieronder is uitgewerkt wat de totaalscore is voor ieder onderdeel. In de rechter grafiek is te zien hoe de classificatievragen zijn beantwoord.





De IBD heeft geen lijst van gemeenten die het product gebruiken met daarbij hun scores. 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 voor ieder 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** (46%)*
Dit onderdeel is niet veranderd vergeleken met mijn vorige jaarverslag. Het gaat er vooral om dat het privacybeleid wordt vernieuwd en dat de rollen, taken en verantwoordelijkheden van alle betrokken personen worden opgenomen, naast de verantwoordelijkheid van het management voor het halen van de doelen van het privacybeleid en het aan een privacyspecialist vragen van advies voor een nieuwe verwerking van persoonsgegevens. Daarnaast moet worden uitgezocht voor welke afdelingen specifiekere uitwerking nodig is. Denk hierbij ook aan het schrijven van een intern privacybeleid voor de omgang met gegevens van medewerkers. De Privacy Officer zal de vernieuwing coördineren en de juiste teams betrekken voor de inhoud.

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

***Processen** (51%)*
Binnen dit onderdeel gaat het niet alleen om het opnemen van privacy in werkprocessen, maar ook om het hebben van een actueel register van verwerkingen, het verzorgen van Data Protection Impact Assessments en het gebruiken van een bewaar- en vernietigingsbeleid.

Eerder heb ik de aanbeveling gedaan om alle gegevens in het register te controleren op compleetheid en juistheid. In 2022 is gestart met het bijwerken van het register en hier is in 2023 verder aan gewerkt. De Privacy Officer heeft contact gehad met alle teams en legt op dit moment de laatste hand aan de aanpassing van het register en het online zetten hiervan. Daarna kan ik een controle doen van alle onderdelen rondom een verwerking en kan waar nodig actie worden ondernomen.

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 simpele vorm van een DPIA uitgevoerd. Dit wordt via het zaaktype DPIA in Zaaksysteem vastgelegd door de proceseigenaar. Daarna controleer ik of de verwerking voldoet aan de wet en/of het proces een uitgebreide DPIA nodig heeft.

In 2023 is een verkorte DPIA gestart en/of afgerond voor de volgende verwerkingen:
- de nieuwe website
  afgerond, geen sprake van verzamelen van persoonsgegevens

Daarnaast is een uitgebreide DPIA gedaan voor de volgende verwerkingen:
- gebruik bodycams
  afgerond, positief advies FG
- project sluipverkeer
  afgerond, positief advies FG

Als het register is vernieuwd zal ik een overzicht maken van verwerkingen waarvoor een DPIA moet worden uitgevoerd of waarvoor een eerder uitgevoerde DPIA moet worden vernieuwd. Hierbij zal de focus eerst 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 (80%)

De score voor dit onderdeel is licht gestegen en dit is te danken aan de uitvoering van een eerdere gedane aanbeveling om de bewustwordingscampagne '5 voor veilig' door te zetten en aan te vullen met een escaperoom, phishing test en e-learning.

De bestaande zaken zijn voortgezet, zoals berichten op intranet en het met een chocoladereep bedanken van medewerkers die een beveiligingsincident, waaronder datalekken, melden. Daarnaast is eind augustus 2023 een phishing mail verstuurd aan iedereen binnen de organisatie en hebben in september 2023 het college, directie, management en een aantal medewerkers meegedaan aan een cyber security escaperoom. Daarna is de e-learning uitgezet. Elke 5e van de maand ontvangt iedere medewerker vanuit de interne 5HL Academie een e-mail dat een nieuwe leerlijn klaarstaat. Iedere leerlijn behandelt een speciaal onderwerp over privacy en informatiebeveiliging.

We zien dat het aantal meldingen van beveiligingsincidenten gestaag omhoog gaat, zeker na bepaalde aandacht hiervoor zoals rondom de phishing test. Ook worden meer vragen gesteld. Dit is een belangrijke ontwikkeling. Privacy is namelijk niet iets van bijvoorbeeld alleen het subteam Privacy en Informatiebeveiliging (PIN), bestaande uit de FG, de Privacy Officer en de Chief Information Security Officer (CISO). Het is een integraal onderdeel van de vakinhoud (net zoals andere relevante wetgeving).

Voor nu zie ik wel het beeld ontstaan dat niet iedereen bij is met de afronding van de maandelijkse e-learning. In mijn vorige verslag heb ik aanbevolen de e-learning een verplicht karakter te geven. Aan de ene kant om ervoor te zorgen dat iedereen de kennis krijgt. Aan de andere kant om duidelijk te maken dat deze kennis voor iedereen noodzakelijk is en verwerkingsverantwoordelijken en management dit onderstrepen. Ik sta nog steeds achter deze aanbeveling. In het eerste kwartaal van 2024 is gebleken dat medewerkers aansporen ook effect heeft, bijvoorbeeld door een netwerkmanager of door een herinneringsmail vanuit PIN. We zullen op verschillende manieren collega's blijven stimuleren om de e-learning te volgen.

Met directie en management is afgesproken dat we dit jaar vanuit PIN met hen en de teams in gesprek gaan. Dit om te onderzoeken wat voor kennis nodig is, voor wie de e-learning verplicht moet zijn en hoe de kennis zich verhoudt tot de beschikbaarheid van privacyspecialisten. Denk ook aan het gegeven dat het management verantwoordelijk is voor de privacybescherming bij de uitvoering van taken. Zij hebben hiervoor hulp nodig van privacyspecialisten, maar die kunnen deze hulp nu maar minimaal geven. Tijdens de gesprekken zal uiteraard ook het belang van de e-learning worden benadrukt.

Rechten van betrokkenen (83%)

Deze score is gelijk gebleven. Dit percentage laat zien dat we goede omgang met data - en openheid hierover - belangrijk vinden. Een groot onderdeel van de AVG is openheid richting betrokkenen, de mensen van wie wij persoonsgegevens verwerken. Organisaties zijn verplicht mensen goed te informeren over wat ze met hun data doen en waarom. Dit geldt vóór een verwerking en als een betrokkene hierom vraagt. Hiervoor hebben wij een algemene privacyverklaring en deze aangevuld voor een aantal specifieke verwerkingen.

Daarnaast kunnen betrokkenen via DigiD makkelijk en snel een verzoek doen. Zij ontvangen op korte termijn, en altijd binnen de wettelijke termijnen, een reactie. In 2023 hebben we van 8 betrokkenen een verzoek ontvangen. Mensen weten de gemeente hiervoor dus te vinden. In de helft van de gevallen ging het om mensen die niet in onze gemeente wonen. De app MijnGegevens van de Rijksoverheid speelde hier een rol in. Via deze app kan iedereen inloggen met DigiD en zien wie toegang heeft gehad tot hun persoonsgegevens. Als mensen van buiten onze gemeente zien dat wij hun BRP-informatie hebben opgezocht, kunnen ze bij ons een verzoek doen voor uitleg hierover.

Samenwerking *(55%)*

De gemeente werkt veel samen met partners. Het kan hierbij gaan om grote samenwerkingen in de regio. Maar denk ook aan organisaties die wij een deel van onze taken laten uitvoeren. Voor dit onderdeel zijn nog geen wijzigingen sinds mijn vorige jaarverslag. Het gaat er vooral om dat er geen compleet beeld is over de afspraken en uitgevoerde controles bij verbonden partijen en leveranciers. Dit zal dan ook een aandachtspunt zijn voor de volgende jaren. De Privacy Officer zal de inventarisatie coördineren en de juiste teams betrekken voor de inhoud.

Conclusie/aanbeveling ***(herhaling)***
Inventariseer lopende samenwerkingsverbanden en controleer gemaakte afspraken.

Gegevensbescherming *(64%)*

De beveiliging van persoonsgegevens raakt natuurlijk de algemene beveiliging van data van de gemeente. Een beveiligingsincident waarbij direct persoonsgegevens zijn betrokken kan een datalek zijn. Ook andere incidenten kunnen leiden tot een inbreuk op de persoonsgegevens waarvoor wij verantwoordelijk zijn. Een voorbeeld is het open staan van een buitendeur. Medewerkers kunnen incidenten melden via het Zaaksysteem. PIN kijkt daarna of er een datalek is en wat voor acties nodig zijn. Bijvoorbeeld het melden van een datalek bij de Autoriteit Persoonsgegevens of de betrokkene(n).

De bijlage bevat een overzicht van de in 2023 gemelde incidenten en de afhandeling ervan. Het gaat om 49 incidenten, waarvan er 22 een datalek zijn. Dit is een duidelijke stijging vergeleken met 2022. Toen zijn er 31 incidenten gemeld, waarvan er 15 een datalek waren. We zien soms ook een piek in het aantal meldingen. Bijvoorbeeld op de momenten van het sturen van een phishing mail en het starten met de e-learning. In 2022 was ook een piek te zien na aandacht voor het melden van datalekken. Een voorzichtige conclusie is dan ook dat het kweken van bewustwording zijn vruchten afwerpt. Als we kijken naar de inhoud van de incidenten, dan gaat het voornamelijk om zaken waarbij een menselijke fout een rol speelt. De e-learning helpt mensen om meer kennis te krijgen en meer alert te zijn, waardoor de kans op dit soort fouten wordt verkleind. Aandacht blijft dan ook noodzakelijk, zowel via de e-learning als via berichten op intranet en trainingen zoals bijvoorbeeld de escaperoom.

Kleine opmerking bij het aantal gemelde incidenten gaat over de hiervoor genoemde phishing mail. Een aantal mensen heeft deze mail aangemeld als beveiligingsincident en die meldingen staan in deze rapportage. Sommige mensen hebben de mail gemeld bij de Helpdesk of gezien als spam en verwijderd. Dit is onderkend door de CISO. Eerder dit jaar is daarom aandacht besteed aan een uniforme manier van melden van (mogelijke) phishing/spam mails. Via de bewustwordingscampagne zal dit blijvend aandacht krijgen.

Het gaat bij dit onderdeel ook om besef van de risico's van de verwerking van persoonsgegevens en hoe we hiermee omgaan. De situatie vergeleken met vorig jaar is bijna hetzelfde. Hoe we met data in systemen omgaan hangt aan de ene kant af van de professionaliteit van de functioneel beheerder of applicatiebeheerder. En aan de andere kant van het door het team volgen van hun advies.

In 2022 is gestart met het schrijven van beheerplannen voor applicaties. De organisatie nam hiermee stappen in de goede richting. Tijdens het schrijven werd duidelijk dat er aandachtspunten zijn binnen de hele informatiehuidhouding (teams Documentaire Informatievoorziening, Informatisering en Automatisering). Dit is onderkend en om deze aan te pakken is eind 2023 een Programmamanager aangesteld. Deze teams ontwikkelen zich op dit moment. Deze ontwikkeling zal, evenals het schrijven van beheerplannen, verder vervolg moeten krijgen.

***Verantwoording** (68%)*

Als FG breng ik elk jaar verslag uit over mijn bevindingen. Daarnaast evalueren we op het gebied van informatiebeveiliging. Het onderzoek of we voldoen aan de AVG kan worden verbeterd. Het gaat hier namelijk niet alleen om controle door de FG, maar ook om een onderzoek door het management. Zij zijn namelijk verantwoordelijk voor de privacybescherming bij de uitvoering van taken. Hiervoor zullen zij hulp vragen van privacyspecialisten. Dit moeten we dus meenemen in de gesprekken zoals aangegeven onder 'Organisatorische inbedding'.

Wet politiegegevens (Wpg)

Het borgingsproduct is gemaakt voor het onderzoeken van de naleving van de AVG. Ik werkte ook als FG van de Wpg. Officieel was ik hiervoor niet aangesteld. Vorig jaar heb ik de aanbeveling gedaan om een FG aan te stellen voor de Wpg. Deze aanbeveling is overgenomen en uitgevoerd. Ik ben in 2023 officieel aangesteld als FG voor de Wpg.

Audits

De Wpg verplicht tot het elk jaar uitvoeren van een interne Wpg-audit. Daarnaast moet een gecertificeerde toetser ééns in de vier jaar een externe audit uitvoeren. De interne audit over het jaar 2021 (en daarvoor) is in februari 2022 uitgevoerd. De externe audit over dezelfde periode in december 2022. Het auditrapport is aan het college gegeven en, samen met het verbeterplan, aan de Autoriteit Persoonsgegevens (AP) gestuurd.

In 2023 moest de wettelijk verplichte her-audit plaatsvinden. Dit door de aangegeven verbeterpunten bij de externe audit. Ook moest een nieuwe interne audit worden uitgevoerd (over 2022). Het rapport van de her-audit moest ook weer worden gestuurd aan de AP. Zij hebben aangegeven dit vóór 1 maart 2024 te willen ontvangen.

De organisatie is aan de slag gegaan met de aangegeven verbeterpunten. Zoals in mijn vorige jaarverslag staat heeft het gebrek aan voortgang begin 2023 de nodige aandacht gehad. Rond de helft van het jaar zijn stappen gezet, maar helaas heeft dit tot weinig verbeteringen geleid. Ik heb verschillende keren gevraagd naar de situatie van de her-audit. Uiteindelijk bleek maart 2024 dat niet binnen de wettelijke termijn een her-audit is uitgevoerd (en ook geen interne audit). Hierdoor is dus ook geen rapport aan de AP gestuurd. Ik beveel dan ook aan om alsnog te voldoen aan de auditplicht en de AP te informeren over het resultaat.

Conclusie

- De gemeente heeft de wettelijk verplichte her audit in verband met de geconstateerde verbeterpunten bij de externe audit over 2021 (en daarvoor) niet binnen de wettelijke termijn uitgevoerd;
- De gemeente heeft daardoor niet binnen de door de AP gestelde termijn het rapport bij de AP aangeleverd;
- De gemeente heeft de interne audit over 2022 niet uitgevoerd.

Aanbeveling

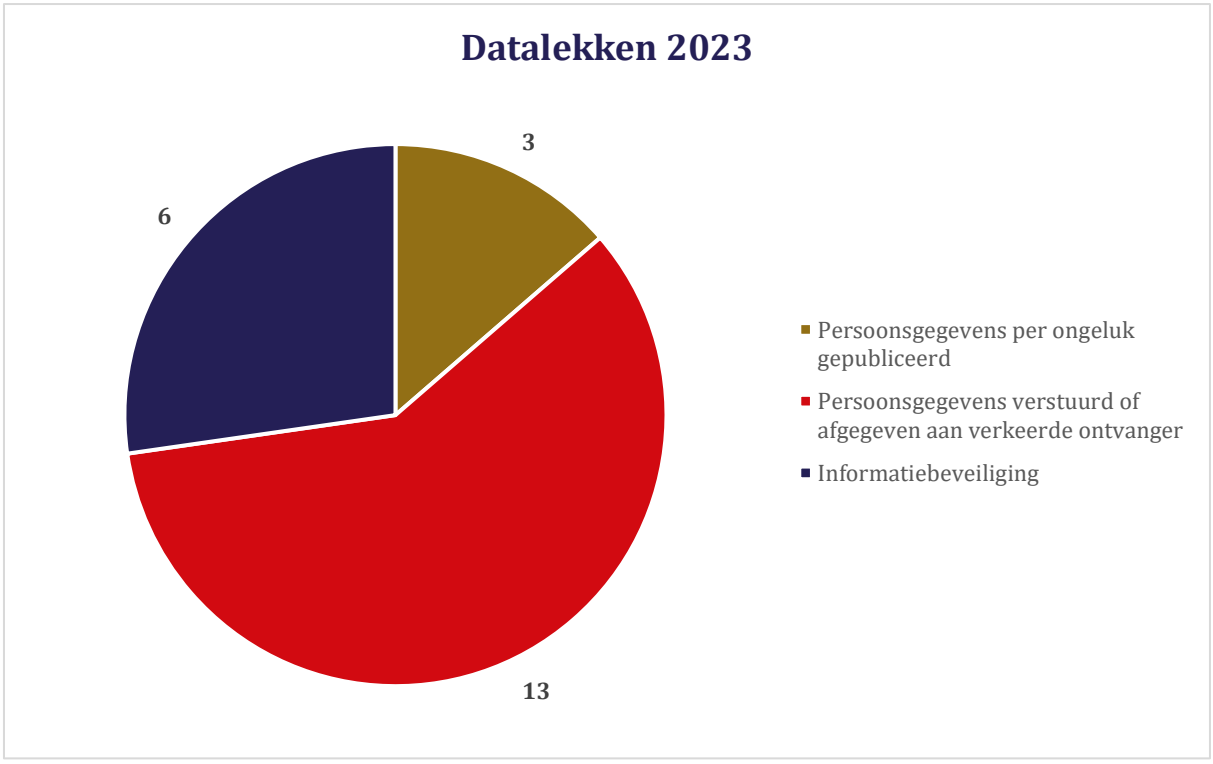
- Voer alsnog per omgaande de her audit uit en stuur het rapport aan de AP;
- Voer in 2024 een interne audit uit over zowel 2022 als 2023.

Bijlage - beveiligingsincidenten 2023

In 2023 zijn 49 beveiligingsincidenten gemeld.

Interessant om een piek te zien in het aantal meldingen op het moment van het sturen van een phishing mail en het starten met de e-learning. Vorig jaar was ook een piek te zien na aandacht voor het melden van datalekken. Een voorzichtige conclusie is dat het kweken van bewustwording zijn vruchten afwerpt.

Van de 49 meldingen zijn 22 een datalek, hieronder verdeeld in de meest voorkomende soorten.



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

Het gaat om de volgende zaken:

Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger (13)
- Document aan verkeerde ontvanger verstuurd. Gemeld aan betrokkene, niet aan Autoriteit Persoonsgegevens. *(3x)*
- Formulier met persoonsgegevens voor controle aan inwoner en partner gestuurd. Betrokkene aangekaart, gezien kleine impact niet gemeld aan Autoriteit Persoonsgegevens.
- E-mail aan verkeerde ontvanger verstuurd. Gezien geen gevoelige informatie geen melding gedaan bij betrokkenen en Autoriteit Persoonsgegevens. *(3x)*
- Documenten aan verkeerde ontvanger verstuurd. Gemeld aan betrokkene en, gezien gevoelige informatie, ook aan Autoriteit Persoonsgegevens.
- E-mail aan verkeerde ontvanger verstuurd. Gezien betrouwbare ontvanger en direct verwijderen van mail geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens. *(4x)*
- Document opgeslagen in verkeerde dossier. Gezien kleine impact geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.

Persoonsgegevens per ongeluk gepubliceerd (3)
- Achternaam indiener document voor gemeenteraad heeft korte tijd online gestaan. Gezien kleine impact geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens. *(2x)*
- Persoonsgegevens zijn gedeeld met leverancier bij vraag over werking van het softwarepakket, terwijl dit niet nodig was voor de afhandeling ervan. Gezien kleine impact geen melding gedaan bij betrokkene en Autoriteit Persoonsgegevens.

Informatiebeveiliging (6)
- Brief aan inwoner met daarin gevoelige informatie lag zonder enveloppe in bakje met te verzenden post. Gezien kleine impact niet gemeld aan betrokkene en Autoriteit Persoonsgegevens.
- Na de verkiezingen zijn niet door alle stembureaus de registers van ongeldig verklaarde stempassen (ROS) direct bij het gemeentelijk stembureau ingeleverd. Deze zijn in de afgesloten stembussen gedaan, die beveiligd zijn opgeslagen. De inhoud daarvan is volgens de Kieswet beveiligd vernietigd, echter de ROS drie maanden te laat. Gezien kleine impact niet gemeld aan betrokkenen en Autoriteit Persoonsgegevens.
- Bij aanmelden zaak in softwarepakket zijn mogelijk gegevens te zien die niet van toepassing zijn op dit zaaktype. Gezien kleine impact niet gemeld aan betrokkene en Autoriteit Persoonsgegevens.
- Op scherm in vergaderkamer was door verkeerde instellingen vertrouwelijk onderwerp van afspraak te zien. Gezien kleine impact niet gemeld aan betrokkene en Autoriteit Persoonsgegevens.
- Stukken over interne sollicitaties achtergebleven op vergadertafel. Gezien kleine impact niet gemeld aan betrokkenen en Autoriteit Persoonsgegevens.
- Vertrouwelijke map niet afgesloten voor medewerkers team. Gezien kleine impact niet gemeld aan betrokkenen en Autoriteit Persoonsgegevens.

In alle zaken is het proces besproken met de betrokken medewerker(s). Waar nodig zijn aanpassingen aan de software of het proces gedaan.