VIJFHEERENLANDEN

JAARRAPPORTAGE 2021 GEGEVENSBESCHERMING

Opgesteld door de Functionaris Gegevensbescherming

Inleiding

Als gemeente werken we met persoonsgegevens van inwoners en het is onze (wettelijke) taak hier zorgvuldig mee om te gaan en alles te doen wat in onze macht ligt om te voorkomen dat deze gegevens in verkeerde handen komen. De Algemene Verordening Gegevensbescherming (AVG) is in 2018 in werking getreden en stelt voorwaarden voor de verwerking van persoonsgegevens binnen de gemeente. Deze voorwaarden bestaan bijvoorbeeld uit kwaliteitseisen, facilitering van inzagemogelijkheden voor betrokkenen en verplichtingen rondom transparantie.

De bestuursorganen van de gemeente zijn verantwoordelijk voor de verwerkingen van persoonsgegevens in onze gemeente. Voor het merendeel gaat het om het college van Burgemeester en Wethouders. 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 en gerelateerde wetgeving en beleid. De FG adviseert gevraagd en ongevraagd gemeentebreed en brengt verslag uit aan het college en de gemeenteraad. Dit verslag draagt bij aan de uitvoering van hun taak als eindverantwoordelijken voor de gegevensverwerkingen.

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 voor de AVG 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 privacybeheerder.

In dit verslag wordt teruggekeken op 2021 en worden een aantal aanbevelingen gedaan. Daarna wordt kort vooruitgekeken naar 2022. Vanwege de verkiezingen is ervoor gekozen dit verslag aan te houden en aan het nieuwe college (en vervolgens de gemeenteraad) aan te bieden. Hierdoor is het voor de nieuwe collegeleden direct inzichtelijk waar de gemeente op dit moment staat en kunnen zij zelf keuzes maken voor de toekomst.

Terugblik 2021

Het afgelopen jaar was bijzonder voor het (sub)team 'Privacy en Informatieveiligheid' (PIN). Voor het eerst sinds de fusie zijn we het hele jaar volledig op sterkte geweest met een FG, CISO (Chief Information Security Officer) en privacybeheerder. We hebben hierdoor een aantal goede stappen gezet. Tegelijk is duidelijk geworden dat ook met een volledige bezetting niet alle zaken op het gebied van privacy goed kunnen worden uitgevoerd. Aan de hand van onderstaande ontwikkelingen wordt dit nader toegelicht.

Bewustwording

Digitaal is vooruitgang geboekt met de bewustwordingscampagne '5 voor veilig'. Op intranet zijn regelmatig themaposters met een toelichting geplaatst. Speciale aandacht is gegeven aan beveiligingsincidenten, waaronder datalekken, en het melden hiervan. Waar gewerkt wordt, worden nou eenmaal fouten gemaakt. In plaats van mensen af te rekenen op fouten wordt daarom een bedankje voor het melden, in de vorm van een chocoladereep, toegestuurd. Ons belang is het met elkaar bespreken om, waar mogelijk, stappen te ondernemen om (vergelijkbare) fouten in de toekomst te voorkomen. Dit levert veel positieve reacties (en meer meldingen!) op.

Collega's weten PIN steeds beter te vinden, zodat we vaker aan de voorkant van een proces worden aangehaakt. Het gebeurt helaas ook nog dat we pas worden betrokken als een voorstel voor het college in routing wordt gebracht. Altijd wordt geprobeerd mee te denken en collega's niet in hun werk te hinderen, maar op een productieve manier te ondersteunen. Collega's geven ook aan de geboden ondersteuning te waarderen. Op het gebied van bewustwording is nog veel te winnen rondom de vraag van wie privacy nu eigenlijk is. Privacy is namelijk niet iets van PIN, maar een integraal onderdeel van de vakinhoud (net zoals andere relevante wetgeving).

Voor vrijwel alle teams zijn in 2021 privacy-ambassadeurs aangewezen waardoor we nieuws en tips snel bij de teams kunnen krijgen. Gebleken is wel dat zij, net als andere collega's, weinig privacykennis hebben en ook te weinig tijd om zich hier echt in te verdiepen.

Door corona konden geplande fysieke organisatiebrede bewustwordingsbijeenkomsten, zoals bijvoorbeeld een privacy-escaperoom, nog niet plaatsvinden. Dit betekent dat we in 2021 voornamelijk bezig zijn geweest met het verzenden van informatie over privacy en niet toegekomen zijn aan een meer interactieve bewustwordingscampagne.

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

Vertrouwen

Ondanks alle goede stappen die we hebben gezet, zijn er ook verbeterpunten. Als gemeente werken we veel samen met diverse partijen in de regio. We horen soms van collega's dat ons advies in zo'n geval niet nodig is, omdat er al mensen naar de stukken hebben gekeken. Meermaals is echter gebleken dat bijvoorbeeld in het geheel niet vanuit een privacy oogpunt naar een voorstel is gekeken. Het kan echter ook zijn dat ons advies anders luidt. Ik zou willen oproepen om vertrouwen te hebben in het interne advies en niet blindelings op externe advisering te vertrouwen. Niet alleen is het interne advies vaak juist gebleken, het helpt ook om (kritische) vragen te stellen en op die manier alle risico's te bekijken en waar nodig het college een juiste belangenafweging te laten maken.

We moeten niet vergeten dat het college de verantwoordelijke is en op zaken wordt aangesproken en mogelijk ook afgerekend. De opmerking dat men het in de regio op een bepaalde manier doet gaat geen redding brengen als de AP een verwerking onderzoekt en zich afvraagt waarom de gemeente de wet overtreedt. Vertrouw op de kennis binnen de organisatie en het feit dat wij er zijn om er gezamenlijk voor te zorgen dat de organisatie op de best mogelijke manier met onze (persoons)gegevens omgaat en dat het college waar nodig een zorgvuldig besluit, met inachtneming van alle informatie en risico's, kan nemen.

Conclusie/aanbeveling
Betrek PIN (vroegtijdig) bij regionale samenwerkingen en vertrouw op interne kennis.

Verwerkers

In het contact met collega's is mij opgevallen dat men vaak terughoudend is met het stellen van vragen aan leveranciers die voor ons persoonsgegevens gaan verwerken, de zogenoemde verwerkers. Wij zijn opdrachtgever en (verwerkings)verantwoordelijk, dus we moeten er voor zorgen dat we vooraf een duidelijk beeld hebben van wat de leverancier met door ons verstrekte (persoons)gegevens gaat doen en ook doorvragen als dit niet duidelijk is. Uiteraard is een prettige werkrelatie van belang, maar een leverancier die betaald krijgt voor een opdracht moet deze ook uitvoeren en voldoen aan de vooraf afgesproken voorwaarden. We moeten ons dan ook minder afhankelijk opstellen van leveranciers en ons recht uitoefenen om vragen en voorwaarden te stellen.

Een voorbeeld is het afsluiten van een verwerkersovereenkomst. Als deze nodig is, dan is dit een wettelijke verplichting. De gemeente heeft als verwerkingsverantwoordelijke een model dat wij hanteren voor al onze verwerkers. Dit is niet optioneel, al kan uiteraard op detailniveau worden gesproken over de invulling. Een belangrijk punt is de beveiliging van persoonsgegevens. Het is dan ook noodzakelijk om de leverancier te vragen naar hun beveiliging van de gegevens die ze van ons gaan ontvangen. Zonder deze informatie kunnen wij de verwerking niet goed beoordelen en de overeenkomst niet ondertekenen. Het zou vanzelfsprekend moeten zijn dat wij zorgvuldig omgaan met onze (persoons) gegevens en dus ook dat wij leveranciers onderzoeken en duidelijke afspraken maken, voordat wij gegevens aan hen gaan verstrekken. Nu zien we regelmatig dat het vragen stellen aan leveranciers als lastig wordt ervaren.

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

Overeenkomsten

Een verwerkersovereenkomst verwijst altijd naar een hoofdovereenkomst waarin wordt geregeld wat de leverancier ons gaat bieden. De verwerkersovereenkomst gaat er van uit dat in de hoofdovereenkomst is geregeld hoe we na beëindiging omgaan met de geleverde persoonsgegevens. Worden ze bijvoorbeeld vernietigd of teruggegeven? Het is verbazend te zien dat er hoofdovereenkomsten bestaan zonder duidelijke afspraken en consequenties. Denk aan een akkoord op een mail met een globale offerte zonder randvoorwaarden. De vraag is of deze juridisch zijn aan te raden, maar vanuit privacy oogpunt is het advies in ieder geval om de hoofdovereenkomst niet te ondertekenen, voordat de verwerkersovereenkomst is besproken. Dit zodat we eventuele vragen kunnen stellen en waar nodig afspraken kunnen maken. Wij zullen hierbij vanuit PIN ondersteunen door dit mee te nemen in het bewustwordingstraject.

Conclusie/aanbeveling
Bespreek de verwerkersovereenkomst voordat de hoofdovereenkomst wordt aangegaan.

Processen

De verwerkingen van persoonsgegevens van de gemeente dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Alle verwerkingen van persoonsgegevens staan in het register van verwerkingen. In 2021 is gewerkt aan het updaten van het register met daarbij een controle van alle facetten rondom een verwerking, zoals de juiste grondslag, gegevensdeling met derden en gemaakte afspraken met leveranciers.

Daarnaast kan de gemeente verplicht zijn een gegevensbeschermingseffectbeoordeling, oftewel een Data Protection Impact Assessment (DPIA), uit te voeren. Indien nieuwe werkprocessen worden opgenomen in het Zaaksysteem wordt hiervoor een eenvoudige variant van een DPIA uitgevoerd. Dit wordt via het desbetreffende zaaktype in Zaaksysteem opgevoerd door de proceseigenaar. Vervolgens controleert de FG of de verwerking voldoet aan de bovengenoemde beginselen en/of het proces een uitgebreidere DPIA nodig heeft. In 2021 is een verkorte DPIA afgerond voor de VHL Academie en is een verkorte DPIA gestart voor de zogenaamde Peutermonitor. Deze zal in 2022 worden afgerond. Daarnaast is gewerkt aan de uitgebreide DPIA voor het PGAx-systeem. Dergelijke DPIA's vragen behoorlijk wat kennis en tijd van het betrokken team. Door gebrek hieraan komt een (te) groot deel bij de privacybeheerder te liggen.

In het register staan ook verwerkingen met een hoger risico die al langere tijd plaatsvinden, maar waarvoor nooit een DPIA is uitgevoerd. Tevens moeten uitgevoerde DPIA's regelmatig worden herzien. Het zou dan ook goed zijn om een planning te maken van de verwerkingen waarvoor een DPIA (opnieuw) moet worden uitgevoerd.

Conclusie/aanbeveling
Controleer alle gegevens in het register van verwerkingen op compleetheid en juistheid.
Maak een planning voor de uitvoering van nieuwe DPIA's en DPIA's die moeten worden herzien.

Rechten van betrokkenen

De gemeente dient degene van wie zij de persoonsgegevens verwerkt (de 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 door een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. Op de website van de gemeente is een privacyverklaring opgenomen. In deze verklaring staat hoe de gemeente omgaat met persoonsgegevens en hoe betrokkenen hun rechten kunnen uitvoeren. Daarnaast is bij nieuwe verwerkingen via de website en bij nieuwe formulieren een tekst opgenomen waarin betrokkenen worden geïnformeerd.

In 2021 zijn vier verzoeken ingekomen voor inzage in verwerking van persoonsgegevens. Verzoekers hebben een overzicht gekregen van de persoonsgegevens die wij verwerken met alle bijbehorende informatie. Daarnaast is één verzoek ingekomen voor het verwijderen van persoonsgegevens. De betreffende gegevens dienen aantoonbaar conform de vastgestelde bewaartermijn te worden bewaard, dus dit verzoek is afgewezen.

Conclusie/aanbeveling
Het proces is afdoende ingeregeld en kan worden voortgezet.

Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, integriteitsbeginsel en vertrouwelijkheids-beginsel is het essentieel dat de gemeente passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Een belangrijk onderdeel hiervan is de controle op het verstrekken van toegang tot systemen. Daarbij wordt gekeken welke autorisatie nodig is voor de betreffende medewerker. Ook wordt gelogd wie welke informatie raadpleegt. Medewerkers kunnen via Zaaksysteem een gemotiveerd verzoek indienen tot wijziging van de verleende autorisatie. Dit verzoek wordt beoordeeld door de FG.

Aandachtspunt is dat op dit moment onvoldoende controle bestaat op de rechten van een nieuwe medewerker. Autorisaties zijn formeel gekoppeld aan een specifieke functie en later kan men via het Zaaksysteem extra autorisaties vragen. De praktijk is vaak dat een nieuwe collega automatisch de rechten krijgt van de collega die is vertrokken. Dit zijn dan echter niet altijd alleen de autorisaties die bij de betreffende functie horen.

Medewerkers kunnen via het Zaaksysteem een beveiligingsincident melden. De procedure is eenvoudig te vinden via intranet. Samen met de privacybeheerder wordt gekeken of al dan niet sprake is van een datalek en zo ja, of het moet worden gemeld aan de AP en betrokkene(n). Tevens wordt uiteraard gekeken welke maatregelen eventueel nodig zijn om het incident op te lossen en/of ervoor te zorgen dat een dergelijk incident niet nog een keer plaatsvindt.

In de bijlage is een overzicht opgenomen van de in 2021 gemelde beveiligingsincidenten, waaronder datalekken, en de afhandeling ervan. Gezien de hoeveelheid data die binnen de gemeente wordt verwerkt kunnen we niet anders dan concluderen dat er te weinig datalekken worden gemeld. Hiervoor is dus meer bewustwording nodig.

Conclusie/aanbeveling
Ken nieuwe medewerkers autorisaties toe die bij de functie horen en niet automatisch alle autorisaties die de vorige medewerker had.
Creëer bewustwording voor beveiligingsincidenten, met name datalekken, en (de noodzaak voor) het melden hiervan.

Wet politiegegevens (Wpg)

De gemeente heeft een aantal buitengewone opsporingsambtenaren (boa's) in dienst. De gegevensverwerkingen die zij doen in het kader van hun opsporingstaken vallen niet onder de AVG, maar de Wpg. De AP heeft aangegeven uit te gaan van een benoeming als FG voor de AVG én de Wpg, tenzij de gemeente een aparte FG voor de Wpg doorgeeft. Dit laatste is niet het geval en als FG voel ik mij verantwoordelijk voor het geven van advies aan de hele organisatie. De privacybeheerder is formeel ook alleen aangesteld voor de AVG, maar voelt dezelfde verantwoordelijkheid. Binnen de betrokken teams was weinig kennis aanwezig van alle specifieke eisen die werden gesteld aan bijvoorbeeld de registratie van Wpg-verwerkingen. Vandaar dat wij vanuit PIN hebben ondersteund bij het opstellen van een register van verwerkingen voor de Wpg, het inrichten van het proces voor de uitoefening van rechten van betrokken voor wat betreft Wpg-verwerkingen en vooral bij de verplichte audits die wettelijk moeten plaatsvinden.

Uit de wet vloeit namelijk voort dat we elk jaar een interne Wpg-audit moeten uitvoeren en ééns per 4 jaar een externe audit door een daartoe gecertificeerde toetser. Feitelijk betekende dit dat in 2021 beide audits moesten plaatsvinden. Hier is dan ook vooral in de tweede helft van het jaar veel werk voor verzet vanuit PIN en de betrokken teams. Het externe auditrapport moet worden opgestuurd naar de AP. De AP heeft hiervoor uitstel verleend tot 31 december 2022.

De interne audit (over het jaar 2021) heeft in februari 2022 plaatsgevonden. Het rapport wordt binnenkort definitief gemaakt en daarna gaan de teams aan de slag met de aanbevelingen. In de tweede helft van dit jaar zal de externe audit (eveneens over het jaar 2021) plaatsvinden. Het rapport wordt aan het college verstrekt en vervolgens toegestuurd aan de AP. Hierin nemen we uiteraard de voortgang van de gedane aanbevelingen mee.

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

Capaciteit

Het is hiervoor al een paar keer genoemd, maar afgelopen jaar is gebleken dat slechts een klein percentage van de collega's voldoende privacykennis heeft om diverse zaken na een instructie zelfstandig af te handelen. Over het algemeen is uitgebreide ondersteuning nodig en deze is niet altijd op korte termijn te geven met de beperkte capaciteit op privacygebied binnen PIN. Daarnaast heeft de Wpg in de tweede helft van het jaar veel tijd gevraagd van vooral de privacybeheerder. Dit alles is begrijpelijk, maar wel van belang om te constateren. Eerdere jaren was de beperkte capaciteit ook aan de orde, maar werd dit mede veroorzaakt door het feit dat PIN niet op volle sterkte was. Dat was in 2021 niet het geval, dus kunnen we nu daadwerkelijk constateren dat de huidige capaciteit op privacygebied onvoldoende is. Ik wil dan ook ter overweging meegeven de capaciteit van de privacybeheerder uit te breiden dan wel privacybeheerders binnen teams aan te stellen.

Conclusie/aanbeveling
Vergroot de capaciteit van de privacybeheerder binnen team Control dan wel stel (een) privacybeheerder(s) binnen de teams aan.

Samenvatting

Mijn conclusie over 2021 is dat er veel ontwikkelingen zijn geweest en dat we op de goede weg zijn in de bescherming van persoonsgegevens en de naleving van relevante wetgeving. Wel is gebleken dat sommige zaken veel tijd kosten, mede door het gebrek aan kennis binnen de organisatie. Dit levert een capaciteitsprobleem op waardoor de bescherming van persoonsgegevens in het geding komt.

De 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.

Samengevat gaat het om de volgende aanbevelingen:

Voor de hele organisatie

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

Voor de medewerkers binnen PIN

- Zet de huidige bewustwordingscampagne voort, aangevuld met een interactiever karakter zoals e-learning, phishing en/of escaperoom
- Creëer bewustwording voor beveiligingsincidenten, met name datalekken, en (de noodzaak voor) het melden hiervan

Voor de hele organisatie, maar gecoördineerd door PIN

- Controleer alle gegevens in het register van verwerkingen op compleetheid en juistheid
- Maak een planning voor de uitvoering van nieuwe DPIA's en DPIA's die moeten worden herzien

Voor het college

- Voorzie de betrokken teams van voldoende kennis en capaciteit voor de uitvoering van specifieke eisen rondom Wpg-verwerkingen
- Vergroot de capaciteit van de privacybeheerder binnen team Control dan wel stel (een) privacybeheerder(s) binnen de teams aan

Vooruitblik 2022

Graag zou ik hier aangeven dat we, indien ze worden overgenomen, gaan werken aan alle genoemde aanbevelingen. Helaas is de privacybeheerder per 1 mei jl. vertrokken en wordt gezocht naar een vervanger. Dit zorgt ervoor dat de beantwoording van vragen en uitvoering van projecten langer kan duren en minder zaken kunnen worden opgepakt, zoals bijvoorbeeld de controle van het register van verwerkingen en de uitvoering van DPIA's. Enerzijds omdat we 30 uur per week missen voor advisering en ondersteuning op privacygebied en de teams dus meer zaken zelf moeten uitzoeken of langer moeten wachten tot ik als FG binnen mijn reguliere werkzaamheden tijd vrij kan maken. Anderzijds kan ik bepaalde taken als FG, vanuit mijn rol als interne toezichthouder, ook niet overnemen van de meer uitvoerende privacybeheerder. Een voorbeeld hiervan is dat ik formeel inhoudelijk niet kan meeschrijven aan een DPIA, aangezien ik die na afronding moet beoordelen en advies moet geven over de gewenste verwerking.

Uiteraard ondersteun ik de teams zoveel mogelijk, maar het feit dat we minimaal een aantal maanden niet op volledige sterkte opereren verlaagt het ambitieniveau voor dit jaar. De werkzaamheden zullen zich beperken tot lopende processen en noodzakelijke handelingen door nieuwe ontwikkelingen, zoals bijvoorbeeld de Wet Open Overheid. In ieder geval zal PIN verder gaan met het bewustwordingstraject en de aandachtspunten rondom (het melden van) beveiligingsincidenten en (verwerkers)overeenkomsten. Daarnaast zal ik werken aan de controle van het register van verwerkingen en het ondersteunen van de teams bij de uitvoering van hun werkzaamheden op privacygebied.

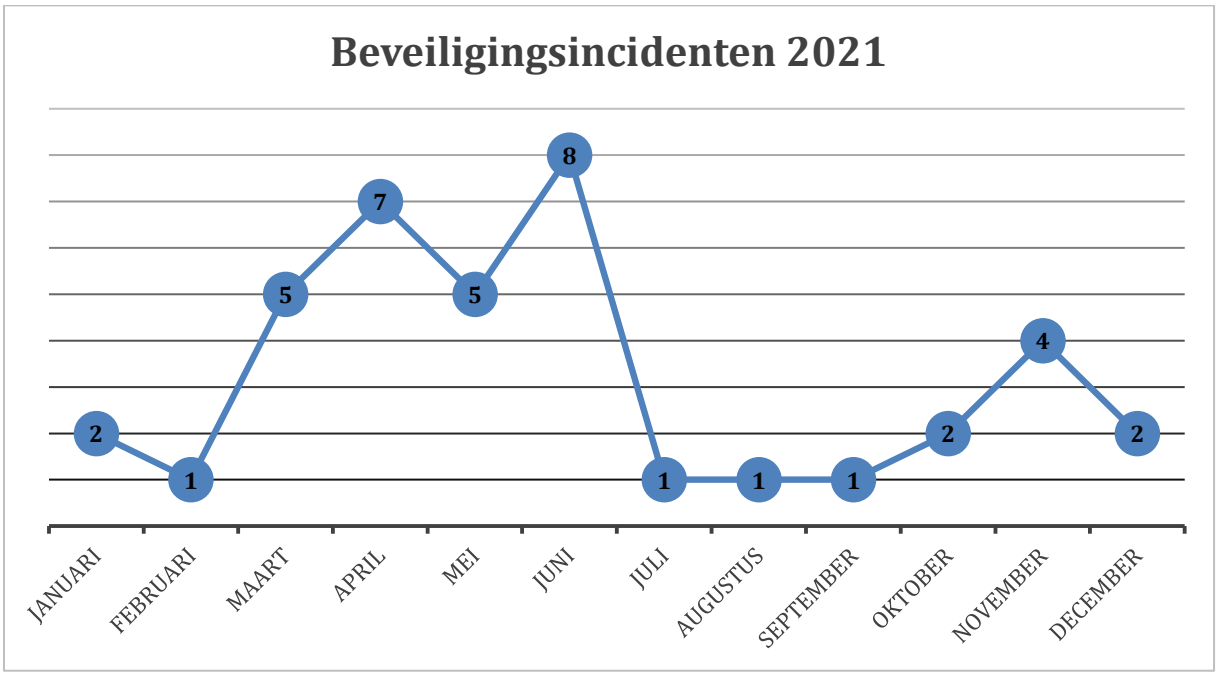
Een en ander vraagt van iedereen een grote mate van flexibiliteit en hard werken en dan is het eigenlijk nog niet genoeg. Dit zal in ieder geval de situatie zijn totdat een nieuwe privacybeheerder is aangesteld. Zoals aangegeven zal de ontwikkeling echter ook daarna beperkt blijven, tenzij wordt geïnvesteerd in meer capaciteit en kennis op privacygebied.

Leerdam, mei 2022

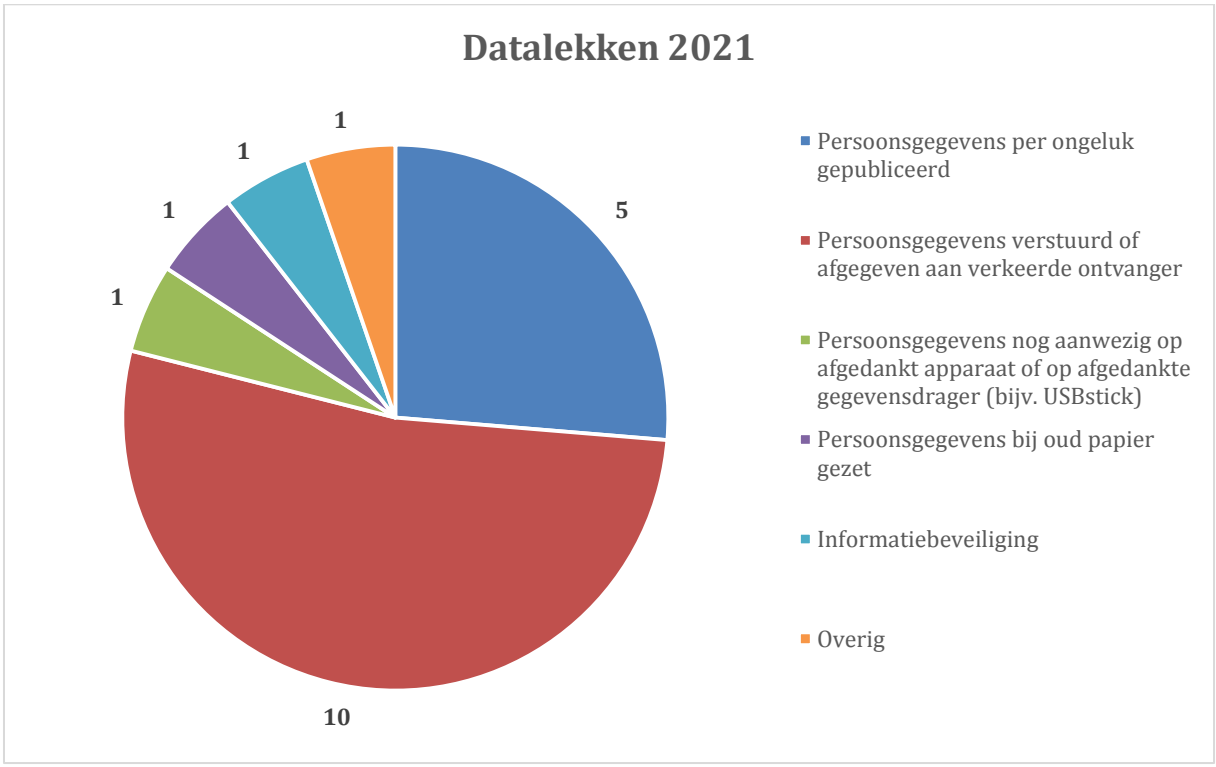
mevrouw mr. L. de Keijzer-Krens CIPP/E CIPM

Bijlage - beveiligingsincidenten 2021

In 2021 zijn er 39 beveiligingsincidenten gemeld. Het is goed te zien dat er een piek ontstaat in het aantal meldingen op de momenten dat in het bewustwordingstraject specifieke aandacht is besteed aan dit onderwerp.



Van deze 39 meldingen zijn er 19 gekwalificeerd als een datalek, hieronder gespecificeerd naar de meest voorkomende categorieën.



Het gaat om de volgende zaken:

Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger (10)
- Brief / formulier aan verkeerde, maar betrouwbare, ontvanger verstuurd. Datalek niet gemeld aangezien betrouwbare ontvanger de stukken direct heeft vernietigd.
- Brief / e-mail / stukken aan verkeerde ontvanger verstuurd. Gezien inhoud en geringe impact geen melding gedaan bij AP en betrokkene.
- Gegevens van aanvrager verstuurd aan gemachtigde. Op dat moment niet juist, maar gemachtigde ingehuurd door aanvrager en daarmee al op de hoogte van gegevens. Niet gemeld aan AP.
- Uittreksel aan verkeerde ontvanger verstuurd. Bevatte geen gevoelige informatie. Ontvanger uittreksel teruggestuurd. Niet gemeld aan AP, wel aan betrokkene.
- E-mail met afspraakbevestiging aan verkeerde ontvanger verstuurd. Bevatte beperkte informatie. Niet gemeld aan AP, wel aan betrokkene.
- Salaris- en gezondheidsgegevens aan verkeerde medewerker verstuurd. Datalek gemeld aan AP en betrokkene.
- Brief omtrent gevoelige informatie aan verkeerde ontvanger verstuurd. Gemeld bij AP. Later bleek genoemde persoon niet te bestaan, dus achteraf gezien geen datalek.

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

Persoonsgegevens per ongeluk gepubliceerd (5)
- Ingekomen raadsstuk (2x) met persoonsgegevens per ongeluk openbaar gepubliceerd. Datalek gemeld aan AP en betrokkene.
- Lijst met gegevens (2x) bevatte per abuis enkele persoonsgegevens. Datalek niet gemeld aangezien lijst is verstuurd aan een betrouwbare ontvanger en direct door deze ontvanger is vernietigd.
- Foto’s met namen van medewerkers tijdens interne bijeenkomst gepubliceerd op social media. Niet gemeld aan AP, wel via intranet aan betrokkenen.

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

Persoonsgegevens nog aanwezig op afgedankt apparaat of gegevensdrager (1)
- Mobiele telefoon verstrekt aan nieuwe collega, maar hier bleken contactgegevens op te staan van vorige gebruiker. Datalek niet gemeld aan AP en betrokkenen aangezien gegevens in handen waren van betrouwbare ontvanger en direct zijn verwijderd. Proces doorgenomen met betrokken medewerkers en aangescherpt.

Persoonsgegevens bij oud papier gezet (1)
- In de gemeentehuizen staan speciale afgesloten papiercontainers waarmee informatie veilig wordt afgevoerd en vernietigd. Een aantal papiercontainers heeft korte tijd opengestaan waardoor in theorie een datalek kon ontstaan. Het proces is aangepast, maar er is gezien de geringe impact geen melding gedaan bij AP dan wel eventuele betrokkenen.

Informatiebeveiliging (1)
- Prints komen terecht in account van andere collega. Probleem opgelost door leverancier. Niet gemeld aan AP en betrokkene aangezien het hier een collega van dezelfde afdeling met vergelijkbare autorisaties betrof.

Overig (1)
- Ingenomen waardedocument niet direct opgeborgen in kluis. Gevonden door collega en alsnog opgeborgen. Collega formeel niet bevoegd, maar document ook niet ingezien. Datalek niet gemeld aan AP en betrokkene.