Verslag Functionaris Gegevensbescherming over periode juli 2023 - oktober 2024

Algemeen	
Aan	MT, DB, AB
Van	Mw. mr. Sascha Boedhoe
Datum	11 december 2024
Verspreiden	Nee
Kenmerk	DOC-24008491

Samenvatting

Dit is het zesde verslag van de Functionaris Gegevensbescherming (FG) aan het Dagelijks Bestuur. Het verslag beslaat de periode juli 2023 tot en met oktober 2024.

Belangrijke gebeurtenissen op het gebied van privacy in het afgelopen verslagjaar betreffen:
- de daadwerkelijke start met overgang naar het nieuwe werken in de cloud met een Saas-oplossing (Software as a service);
- het aanwijzen van een portefeuillehouder voor ICT, data en privacy in het dagelijks bestuur;
- het vertrek van de FG per 1 december 2023, het waarnemen van de plaatsvervangend FG van 1 december 2023 tot 27 mei 2024 en de tijdelijke invulling door een externe FG vanaf 27 mei 2024 t/m 31 december 2024; en

Er zijn in het verslagjaar op privacygebied de volgende zaken gerealiseerd:
- Er zijn verbeterplannen opgesteld naar aanleiding van de eerste externe audit Wet politiegegevens. Deze verbeteringen zijn voor een groot gedeelte doorgevoerd.
- Er is een plan van aanpak gemaakt om de e-learning digitale weerbaarheid opnieuw vorm te geven.
- Er zijn enkele risicoanalyses uitgevoerd op verwerkingen van persoonsgegevens met een hoog risico, waaronder een tweetal Data Protection Impact Assessments (DPIA's) door een externe privacy officer.
- Alle organisatieonderdelen krijgen in 2025 een eigen privacyverklaring.
- Binnen de Regio wordt op dit moment gewerkt aan een eenduidige aanpak voor alle organisatieonderdelen hoe verzoeken in het kader van rechten van betrokkenen worden afgehandeld.
- Er zijn dit verslagjaar zesentwintig informatieveiligheidsincidenten gemeld. Dit is één incident minder dan in het verslagjaar hiervoor. In drieëntwintig gevallen bleek het daadwerkelijk om een datalek te gaan. Dat zijn acht datalekken meer dan het jaar ervoor. In elf gevallen was sprake van een risico voor betrokkenen waardoor gemeld moest worden aan de Autoriteit Persoonsgegevens (hierna: AP) en in negen gevallen is ook melding aan betrokkenen gemaakt.

Daarnaast kunnen de volgende belangrijke aandachtspunten worden benoemd:
- Noodzakelijke DPIA's bij nieuwe regiotaken zijn nog niet goed geborgd.
- Er moet bewustwording worden gecreëerd voor het weggooien of archiveren van informatie in mail en netwerkschijven als deze niet meer nodig is.
- Het strategisch informatieoverleg, waar wijzigingen in informatietoepassingen vanuit meerdere disciplines wordt besproken, ligt vanwege uitval van collega's momenteel stil.
- Organisatieonderdelen zullen meer aandacht moeten besteden aan het (juist) afsluiten van verwerkersovereenkomsten met partijen die als verwerker kwalificeren.

- Het uitvoering geven aan de AVG-rolverdeling tussen Regio Gooi en Vechtstreek (hierna: de Regio) en regiogemeenten is een belangrijk en beladen onderwerp.
- Het is van belang de informatieveiligheidsmaatregelen op een hoger plan te brengen en deze te documenteren.
- De FG doet een FG een aanbeveling om de gevraagde capaciteit voor een tweede privacy officer resp. een fulltime privacy officer voor uitvoerende privacywerkzaamheden.
- Tot slot geeft het onderstaande schema een overzicht van de onderdelen waarop ten opzichte van het vorige verslagjaar een stijgende lijn zichtbaar is, evenals de punten waarop nog verbeteringen nodig zijn. In de verschillende hoofdstukken wordt hier dieper op ingegaan.

Onderwerp	**Juli 2023 – oktober 2024**	**Juli 2022- juni 2023**
Organisatorische inbedding		
Kennis en kunde privacy		
Advisering, informatieverstrekking en voorlichting		
Toezicht op toepassing en naleving AVG		
Wet politiegegevens		
Bewustwording		
Register van gegevensverwerkingen		
Processen privacyproof		
Eenduidige registratie voor verantwoordingsplicht		
Relaties met derde partijen		
Privacybeleid		
Informatieplicht verwerkingen algemeen en websites		
Verzoeken i.h.k.v. rechten van betrokkenen		
Datalekken		
Informatieveiligheid		

Inhoudsopgave

1 Inleiding

Dit is het zesde verslag van de functionaris gegevensbescherming (hierna: Fg) aan het Dagelijks Bestuur (hierna: DB). In de Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet politiegegevens (hierna: Wpg) is geregeld dat de Fg verslag uitbrengt over haar werkzaamheden, bevindingen en aanbevelingen aan de verwerkingsverantwoordelijke, te weten bij de Regio het DB. Om deze reden wordt dit verslag aangeboden aan het MT, het DB en aan het Algemeen Bestuur als controlerend orgaan. Normaliter verschijnt een dergelijk verslag rond de zomervakantie. Vanwege de personele wisselingen op de Fg-rol heeft dit verslag echter langer op zich laten wachten en beschrijft dit verslag de periode juli 2023 t/m oktober 2024. In het jaarverslag staat aan de hand van belangrijke privacythema's beschreven welke acties en maatregelen de Regio in het afgelopen verslagjaar heeft genomen om de doelstellingen en beginselen uit de AVG en Wpg te behalen en te waarborgen. Bij elk thema staat met een kleur aangegeven in hoeverre de Regio in control is, namelijk geheel (groen), gedeeltelijk (oranje) of niet (rood). Waar van toepassing wordt aangegeven welke zaken al op de planning staan voor het nieuwe verslagjaar. Ook bevat dit document de bevindingen van de Fg en aandachtspunten voor het nieuwe verslagjaar. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers. Ten slotte is er per 1 juni jl. voor 16 uur per week een privacy officer aangesteld en is er voor 12 uur per week een (externe) Fg gestart. Daarmee is er een scheiding tussen uitvoering en toezicht gerealiseerd.

2 Organisatorische inbedding

Context
Het DB is verantwoordelijk voor goede gegevensbescherming binnen de Regio. Managers en medewerkers hebben een hiervan afgeleide verantwoordelijkheid. De Fg houdt toezicht op een goede omgang met persoonsgegevens volgens de AVG en Wpg.
Alle managers hebben aandachtsfunctionarissen privacy benoemd om hen te ondersteunen in hun privacytaken. De aandachtsfunctionaris is het eerste aanspreekpunt voor privacy voor zijn of haar eigen organisatieonderdeel en voor de Fg. Zij signaleren wijzigingen in de verwerkingen van persoonsgegevens. Ook coördineren zij voor hun organisatieonderdeel de afhandeling van de organisatiebrede verzoeken (zoals verzoeken om inzage) die inwoners en medewerkers vanuit de AVG en Wpg bij de Regio kunnen indienen. Dit verslagjaar heeft de Fg afzonderlijk met de verschillende aandachtsfunctionarissen gesproken. Daarnaast is het de bedoeling eens per jaar een gesprek met de organisatieonderdeel-managers te plannen.

Voortgang in verslagjaar
Begin 2023 is er in het dagelijks bestuur een portefeuillehouder ICT, data en privacy benoemd. Daarvoor was er niemand in het bestuur die zich hier specifiek mee bezighield.
Nota bene. Voor dit verslagjaar is nog geen aandachtsfunctionaris privacy voor Beleid en Bestuur aangesteld. Hiervoor zal nog iemand moeten worden aangewezen.

Verder zijn er – zoals eerder beschreven – personele wisselingen op de Fg-rol geweest. De vorige Fg is per 1 december 2023 uit dienst getreden en de plaatsvervangend Fg heeft in de periode 1 december 2023 tot 27 mei 2024 waargenomen. Er is langdurig een vacature uitgezet voor een nieuwe Fg; dit heeft echter geen geschikte kandidaten opgeleverd.
Sinds 27 mei jl. is er vervolgens voor 12 uur per week een externe interim Fg geworven, die tot het eind van 2024 toezicht zal houden op privacyzaken binnen de Regio. Ook is sinds mei jl. een interne CISO voor 16 uur in de week aangesteld die binnen de Regio verantwoordelijk is voor de informatiebeveiliging en aanspreekpunt is over dit onderwerp. Deze functie komt binnenkort opnieuw vacant.

Vervolgens is er sinds 1 juli jl. voor 16 uur een privacy officer aangesteld voor de uitvoerende privacywerkzaamheden.

Met de komst van een aparte privacy officer en een aparte Fg zijn de toezichthoudende- en uitvoerende privacywerkzaamheden feitelijk niet meer bij een en dezelfde persoon belegd.
De uitvoerende privacy werkzaamheden zijn namelijk (in beginsel) bij de privacy officer belegd en de toezichthoudende taak ligt bij de Fg.

Het idee was om een fulltime privacy officer te werven, maar dit is niet gelukt. Nu de privacy officer slechts 16 uur per week beschikbaar is, houdt de Fg zich in sommige gevallen nog met uitvoerende werkzaamheden bezig. Om die reden zijn de rollen nog niet volledig gescheiden. De Regio zou meer moeten groeien in de volwassenheid van het toepassen van deze rollen.
De Regio is op dit punt nog niet volledig in control.

Acties komende jaar
De huidige privacy officer is slechts parttime beschikbaar, namelijk voor 16 uur per week. Het is aan te bevelen dat de Regio de benodigde formatie, te weten de capaciteit voor een fulltime privacy officer, in het nieuwe jaar beschikbaar houdt, zodat er ruimte is voor een tweede privacy officer op het moment dat er een geschikte kandidaat is.
Verder zal de huidige interim Fg per 31 december voor het laatst zijn en wordt de Fg-rol vanaf 1 januari 2025 ingevuld door twee interne senior juridische adviseurs die hun adviestaken zullen scheiden van hun Fg-taken. Beiden zullen parttime beschikbaar zijn voor de Fg-rol.

3 Kennis en kunde privacy

Context
Het is van belang dat de diverse functionarissen die zich met privacyzaken bezighouden, kennis en kunde op peil brengen en houden.

Voortgang in verslagjaar
Uit de wekelijkse en tweewekelijkse netwerkbijeenkomsten van de GGD voor de Fg's van de 25 GGD-en komen nuttige ervaringen en best practices naar voren en referentie DPIA's die ook door de Regio worden benut. Verder zijn door de functionarissen die met privacyzaken bezig zijn, diverse cursussen, webinars, seminars en congressen gevolgd. Vervolgens is de privacy officer samen met de adviseur kwaliteit, rechtmatigheid en informatiebeveiliging bezig met een project ten aanzien van de uitbreiding van de huidige e-learning. De Regio is op dit punt in control.

Acties komende jaar
Binnen de Regio zal er constant aandacht moeten worden besteed aan het op peil houden van kennis en kunde op het gebied van privacy en gegevensbescherming. De uitrol van de e-learning digitale weerbaarheid zal hier aan bijdragen. Deze wordt volledig voor alle RVE's uitgerold en het doel is dat alle medewerkers de e-learning een keer maken.
Er is nu hernieuwde aandacht voor de e-learning. Zo wordt geborgd dat ook nieuwe medewerkers worden aangehaakt. Daarnaast wordt er een uitbreiding gedaan richting security.
Het is aan te bevelen dat nieuwe medewerkers bij indiensttreding de e-learnin volgen en dat bestaande medewerkers deze jaarlijks herhalen. Ook is het advies om in 2025 opnieuw in gesprek te gaan met de privacy aandachtsfunctionarissen en hen te informeren over de taken als aandachtsfunctionaris, zodat zij weten wat van hen wordt verwacht.

4 Advisering, informatieverstrekking en voorlichting

Context
Formele adviezen aan verwerkingsverantwoordelijke (vaak organisatieonderdeel-manager) worden gegeven wanneer er risico's voor de privacy van inwoners van de Regio en/of medewerkers bestaan of als er onduidelijkheid bestaat over de uitvoering van een bepaalde gegevensverwerking.
Van de formele adviezen van de Fg kan de verwerkingsverantwoordelijke enkel gemotiveerd afwijken.

Voortgang in verslagjaar
De Fg heeft een aantal formele adviezen gegeven waarop de verwerkingsverantwoordelijke heeft gereageerd. In de tabelvorm hieronder worden deze formele adviezen kort geduid.

Onderwerp	**Advies Fg**	**Verwerkings-verantwoordelijke**	**Reactie verwerkingsverantwoordelijke**
Instemming (vanwege wettelijke verplichting feitelijke kennisneming) OR vereist bij logging en monitoring gebruikershandelingen	Het advies is om de OR te betrekken bij de verplichte logging van gebruikershandelingen	Algemeen Directeur ("aan de organisatie")	De Algemeen Directeur wil dit begin 2025 agenderen in de OR ter informatie. Ook wordt nagegaan of dit eerder met hen is besproken.
Uitvoeren tijdige DPIA bij automatiseren verrijkingsverzoeken[1] Veilig Thuis	Het advies is om de pilot-VT's te verplaatsen tot na het moment dat de DPIA is afgerond.	Algemeen Directeur ("aan de organisatie")	Overgenomen
Gebruik Whatsappgroepen i.r.t. Wpg (en AVG)	Het advies is om daar waar het gaat om het uitwisselen van persoonsgegevens/politie gegevens geen gebruik te maken van Whatsapp. Voor informele zaken (zoals een afdelingsborrel) is het prima.	Algemeen Directeur ("aan de organisatie")	Overgenomen
Risico openheid DecosJOIN (hierna: JOIN) i.c.m. gebruik aan DIV'ers	Het advies is om iets te doen aan deze openheid van JOIN en bijvoorbeeld default vertrouwelijkheden per organisatieonderdeel toe te voegen, te zorgen voor meer DIV-capaciteit om de daglijsten weer te kunnen doornemen dan wel een combinatie van deze twee.	Algemeen Directeur ("aan de organisatie")	Overgenomen
Printapparaten	Het advies is om het scannen naar mappen die voor meerdere personen toegankelijk zijn, onmogelijk te maken.	Algemeen Directeur ("aan de organisatie")	Overgenomen
DPIA-register	Het advies is om overzichtelijk te maken wanneer een DPIA voor het laatst is uitgevoerd, wanneer deze herijkt moet worden en in hoeverre maatregelen ook	Algemeen Directeur ("aan de organisatie").	Overgenomen

[1] Verzoeken waarbij men bij VT een melding kan doen van gevallen of vermoeden van huiselijk geweld en/of kindermishandeling.

	zijn opgevolgd.		
Doorgifte van persoonsgegevens naar de VS	Het advies is om geen gebruik (meer) te maken van Amerikaanse gratis internetdiensten voor o.a. het maken van formulieren, het uitvoeren van surveys/enquêtes en het versturen van nieuwsbrieven.	Algemeen Directeur (“aan de organisatie”).	Overgenomen
Het gebruik van ChatGTP binnen de organisatie	Het advies is om voor nu in beginsel geen gebruik te maken van generatieve-AI, zoals ChatGTP	Algemeen Directeur (“aan de organisatie”).	Word nog onderzocht

Daarnaast is veelvuldig een beroep op de juridisch adviseurs en de Fg gedaan voor advies bij alle aangelegenheden waarbij medewerkers binnen de organisatie te maken hadden met de verwerking van persoonsgegevens. Ook heeft de Fg adviezen geschreven op nieuwe DPIA’s, geadviseerd bij het afhandelen van datalekken en advies verstrekt bij vragen over het AVG-proof inrichten van nieuwe applicaties, systemen (zoals Microsoft 365 en Decos JOIN) en het gebruik van applicaties zoals Whatsapp en Youforce. De Regio is op dit punt in control.

5 Toezicht op toepassing en naleving AVG

Context
De Fg moet onafhankelijk toezicht houden op een goede omgang met persoonsgegevens volgens de AVG en het privacybeleid.

Voortgang in verslagjaar
Met de komst van de privacy officer heeft de Fg zich in het afgelopen verslagjaar kunnen richten op toezichthoudende taken. In die rol heeft de Fg gevraagd en ongevraagd advies kunnen geven op de naleving van de gegevensbescherming binnen de Regio. Ook heeft de Fg zich kunnen richten op het schrijven van Fg-adviezen bij DPIA’s, het beoordelen van datalekken en het schrijven van een uniform werkproces ten aanzien van de rechten van betrokkenen. In het kader van het werkproces voor de rechten van betrokkenen heeft de Fg met de verschillende aandachtsfunctionarissen gesprekken gevoerd met als doel om te inventariseren hoe op dit moment met AVG-verzoeken wordt omgaan, of het dienstonderdeel al een eigen privacyverklaring heeft en in hoeverre de aandachtsfunctionaris op de hoogte is van zijn of haar rol bij AVG-verzoeken. Tot slot heeft de Fg toezicht gehouden op het auditproces in het kader van de Wpg. Daar zal in de volgende paragraaf dieper op worden ingegaan.

Nu de Fg slechts voor 12 uur per week werkzaam is voor de Regio, heeft deze momenteel beperkt ongevraagd advies kunnen geven. De Regio is op dit punt nog niet volledig in control.

Acties komende jaar
In het komende jaar zal de Fg ook meer invulling moeten geven aan het proactieve toezicht. Per 1 januari 2025 zal de fg-rol worden vervuld door twee senior juridische adviseurs. Zoals eerder beschreven zullen de Fg-taken worden gescheiden van de adviestaken. Hoewel zij ook betrokken blijven bij advieswerkzaamheden, zal de komst van twee Fg’s zorgen voor meer capaciteit. De verwachting is dat hiervoor meer ruimte zal ontstaan voor het ongevraagd adviseren.

6 Wet politiegegevens

Context
Buitengewone opsporingsambtenaren (hierna: Boa's) hebben een speciale bevoegdheid, namelijk de taak de openbare veiligheid te bewaken, strafbare feiten op te sporen en te vervolgen. Voor deze speciale bevoegdheden zijn regels nodig. Deze regels zijn neergelegd in de Richtlijn gegevensbescherming bij rechtshandhaving (hierna: RGR) en in Nederland is deze Europese richtlijn o.a. in de Wpg geïmplementeerd. De Wpg is van toepassing op het moment dat er politiegegevens worden verwerkt. Binnen de Regio hebben zowel GAD als RBL, te maken met het verwerken van politiegegevens en om die reden dient de Regio zich ook aan de Wpg houden. Een verplichting vanuit de Wpg is een verplichte jaarlijkse interne audit en een vierjaarlijkse externe audit.

Voortgang in verslagjaar
Eind 2022 heeft de Regio een externe Wpg-audit over 2021[2] laten uitvoeren. Hieruit kwamen de nodige verbeterpunten naar voren. Om deze aan te pakken zijn verbeterplannen opgesteld door de betreffende afdelingen. Eind 2023 is een hercontrole uitgevoerd. Hieruit bleek dat op veel punten vooruitgang is geboekt, maar dat nog niet alles op orde is. Op dit moment is de adviseur kwaliteit, rechtmatigheid en informatieveiligheid bezig met het uitvoeren van de interne Wpg-audit en ondersteunt de GAD en het RBL bij de verbeteringen die nodig zijn om bij de volgende externe audit (in 2025, over de situatie in 2024) tot een optimaal resultaat te komen.

De (persoons)gegevens die Boa's als opsporingsambtenaren verwerken, vallen pas sinds 2019 onder de Wpg. De periode 2019-2021 was dan ook de eerste periode waarvoor een externe Wpg-audit moest worden uitgevoerd. Aangezien dit een nieuw proces was, heeft de vorige Fg zich samen met de adviseur kwaliteit, rechtmatigheid en informatieveiligheid gericht op de uitvoerende werkzaamheden met betrekking tot dit punt. Inmiddels liggen de uitvoerende werkzaamheden die voortvloeien uit de Wpg bij de adviseur kwaliteit, rechtmatigheid. De plaatsvervangende Fg en de huidige interim-Fg hebben zich nu volledig kunnen richten op het toezicht. Hier is dus een verbeterslag gemaakt. De Regio is op dit punt in control.

Acties komende jaar
Op dit moment dienen alle normen intern opnieuw te worden geaudit. Dit zal worden uitgevoerd met betrekking tot de opzet, het bestaan en de werking en staat gepland voor januari 2025. De vierjaarlijkse externe audit is gepland voor medio maart 2025. De processen bij zowel RBL als GAD moeten dan zodanig ingericht zijn dat de uitkomsten voldoen aan de gestelde eisen.

7 Bewustwording

Context
Bewustwording bij het bestuur, management en medewerkers over het belang van privacy en de bijbehorende regels is een essentiële voorwaarde voor duurzame naleving van de AVG.

Voortgang in verslagjaar
De uitrol van de e-learning privacy met als doel het vergroten van de digitale weerbaarheid van de Regio en haar medewerkers, is het afgelopen jaar opnieuw leven ingeblazen.
Vragen over privacy en de afwikkeling van datalekken worden aangewend om de privacybewustwording bij management en medewerkers te bevorderen. De gesprekken met aandachtsfunctionarissen privacy en managers worden benut om onder andere aandacht te vragen voor het belang van blijvend privacybewustzijn binnen de organisatieonderdelen. De vorige Fg hield jaarlijks sessies ter bevordering van privacybewustzijn.

[2] De eerste externe audit Wpg voor boa-werkgevers ging over de periode 2019-2021 maar hoefde, vanwege het feit dat deze audit voor hen nieuw is, pas in kalenderjaar 2022 te worden uitgevoerd.

Vanwege beperkte capaciteit is er echter het afgelopen jaar echter weinig aandacht besteed aan fysieke bewustzijnssessies. De Regio is op dit punt dus niet volledig in control.

Acties komende jaar
In het komende jaar zal de e-learning verder worden voortgezet. Ook ten aanzien van informatieveiligheid zal in de e-learning meer aandacht worden besteed aan de basisvaardigheden van medewerkers. Een bewustwordingscampagne, onder andere gericht op de toenemende dreiging van phisingmails zal hier een belangrijk onderdeel van zijn.
Daarnaast zal er, in het kader van privacybewustwording, opnieuw een rondgang langs de aandachtsfunctionarissen moeten worden georganiseerd. Ook kan overwogen worden om fysieke bewustzijnsessies voor medewerkers te organiseren en berichten te plaatsen op de Binnenband, bijvoorbeeld op 28 januari op de 'Dag van de privacy' en de zomergroet van de Fg.

8 Register van verwerkingsactiviteiten

Context
Op grond van de AVG is een verwerkingsverantwoordelijke verplicht een register van verwerkingsactiviteiten bij te houden, ook wel het verwerkersregister genoemd. Dit register is een van de belangrijkste verantwoordingsinstrumenten voor een zorgvuldige omgang met persoonsgegevens. Het verwerkersregister legt alle verwerkingen van persoonsgegevens binnen de Regio vast.
Het bevat onder andere informatie over de rechtmatige grondslag voor de verwerkingen, de ontvangers van de gegevens en de bewaartermijnen van de gegevens.
Het register is een document dat continue onderhouden moet worden. Nieuwe verwerkingen worden toegevoegd, processen kunnen veranderen en in de praktijk komt het vaak voor dat zaken anders verlopen dan oorspronkelijk beschreven.

Voortgang in verslagjaar
De Regio heeft een register van verwerkingsactiviteiten ingericht en voldoet daarmee aan de verplichting om een verwerkersregister te hebben. Het register is momenteel in Excel gevoerd en 40 procent van het register is ook in de applicatie Decos JOIN geplaatst. Het doel is om het gehele register in deze applicatie onder te brengen, zodat de Fg en de aandachtsfunctionarissen hier gezamenlijk efficiënt mee kunnen werken. Dit verslagjaar heeft de Fg met de RVE manager van Veilig Thuis (hierna: VT) het VT deel van het verwerkersregister doorgenomen met het oog op actualisatie. De privacy officer zal de benodigde aanpassingen in het register doorvoeren. Daarnaast zal de Fg dit verslagjaar samen met de RVE managers van GAD en RBL naar de verwerkingen van deze RVE's kijken, zodat deze waar nodig geactualiseerd kunnen worden.

Nu de Regio een verwerkersregister heeft, is de Regio op dit punt in control.

Acties komende jaar
Voor het komende jaar is de ambitie om het verwerkersregister volledig over te zetten naar JOIN, waarin speciaal voor deze doeleinden functionaliteiten zijn ontwikkeld. Op dit moment is er echter onvoldoende capaciteit voor deze overzetting. Het is wenselijk dat deze taak wordt belegd bij de privacy officer die echter ook vele andere verantwoordelijkheden heeft. Verder zal in 2025 aandacht besteed moeten worden aan het actualiseren van het resterende deel van het verwerkersregister, en is het aan te bevelen om afspraken te maken met de aandachtsfunctionarissen over het doorlopend onderhouden en actualiseren van het register.

9 Processen privacyproof

Context
Het is van belang dat de verwerkingen van de Regio zoals deze in het register van gegevensverwerkingen staan, volgens de privacyregels plaatsvinden.

Dit houdt in dat de werkprocessen die persoonsgegevens bevatten, getoetst en ingericht moeten worden volgens de beginselen behoorlijkheid, transparantie, doelbinding (persoonsgegevens mogen alleen worden verzameld met een gerechtvaardigd doel dat specifiek en vooraf uitdrukkelijk is omschreven), dataminimalisatie (niet meer verwerken dan noodzakelijk), opslagbeperking (persoonsgegevens mogen niet langer dan noodzakelijk worden bewaard), juistheid, integriteit en vertrouwelijkheid.
Voor verwerkingen met een hoog risico voor inwoners en medewerkers is de Regio verplicht een gegevensbeschermingseffectbeoordeling (hierna: DPIA) uit te voeren. Volgens de AVG moet een DPIA voorafgaand aan een verwerking worden uitgevoerd. In de praktijk is dit echter vaak lastig. Ook is het wenselijk dat alle disciplines aan de voorkant van het DPIA-proces betrokken worden, hetgeen voor een goede DPIA van belang is.

Door het uitvoeren van een DPIA worden de risico's in kaart gebracht en de maatregelen geformuleerd die deze risico's kunnen beperken. De Regio werkt met een DPIA-kalender waarop jaarlijks de vooraf geplande DPIA's voor dat kalenderjaar zijn opgenomen. Daarnaast werken de 25 GGD-en landelijk samen aan DPIA's op het terrein van de publieke gezondheid. Ook is er op advies van de huidige Fg sinds dit verslagjaar een DPIA-register ingesteld. In dit register zijn onder andere opgenomen wanneer de DPIA is uitgevoerd en wanneer deze, volgens richtlijnen van de AP, herijkt zou moeten worden.

Voortgang in verslagjaar
Van 2023 t/m maart 2024 is een externe privacy officer ingehuurd die zich heeft gericht op het uitvoeren van een tweetal DPIA's, te weten de DPIA op de Pilot Veilig Thuis Project Verrijkingsverzoeken en de DPIA op Consultatiebureau consulten van 0 tot 12 jaar. Beide DPIA's zullen moeten worden aangevuld en zodra dit is gedaan, zal op beide DPIA's een Fg-advies geschreven worden.

Ook is een start gemaakt met een DPIA voor de HR-processen die worden ondersteund door Youforce. Helaas ligt deze DPIA door capaciteitsgebrek nu tijdelijk stil. De DPIA cameratoezicht geniet - als gevolg van het plaatsen van camera's aan de buitenzijde van het pand aan de Burgemeester de Bordesstraat - prioriteit om aangepast te worden. Door capaciteitsgebrek ligt ook deze DPIA tijdelijk stil.

Verder zijn dit verslagjaar de volgende DPIA's uitgevoerd en vastgesteld.
- De DPIA Gezondheidsmonitor Jeugd 2023;
- De DPIA iHPV;
- De DPIA Digitaal Leefplein;
- De DPIA Gezondheidsmonitor Jong Volwassenen;
- De DPIA Gezondheidsmonitor Volwassen en ouderen;
- De DPIA Nu Niet Zwanger; en
- De DPIA Zorg en Veiligheidshuizen.

Op deze DPIA's moet – met uitzondering van de DPIA Gezondheidsmonitor JV en de DPIA Nu Niet Zwanger - nog een Fg-advies komen.

In totaal zijn dit verslagjaar negen DPIA's uitgevoerd. Dit is ondanks de beperkte capaciteit relatief veel en heeft deels te maken met een samenloop van DPIA's die dit verslagjaar zijn opgeleverd.

De AP stelt dat bij veranderingen in de gegevensverwerking, de risico's van de verwerking of de context van de verwerking, een nieuwe DPIA noodzakelijk is. Ook als de gegevensverwerking niet is veranderd, wordt aangeraden om periodiek een DPIA uit te voeren, bijvoorbeeld eens per 3 jaar. Op advies van de huidige Fg is er dit verslagjaar een DPIA-register ingericht met als doel om bovenstaande zaken inzichtelijk te maken. In het DPIA-register wordt o.a. in kaart gebracht wanneer welke DPIA is uitgevoerd en wanneer deze toe is aan herijking.

Nota bene. In de praktijk is het zo dat er bij een hoog risico verwerking ieder jaar wordt bekeken of er iets is veranderd in de gegevensverwerking. Indien dit het geval is, leidt dit tot herijking van de DPIA die op deze verwerking is gedaan.

Gelet op het hebben van een DPIA-kalender, het DPIA-register én de hoeveelheid DPIA's die dit verslagjaar zijn uitgevoerd, kan gezegd worden dat de Regio op dit punt in control is.

Acties komende jaar
Er dient blijvend aandacht te worden besteed aan het structureel uitvoeren van DPIA's volgens de DPIA-kalender. Ook moet doorlopend worden beoordeeld of een DPIA aan herijking toe is.

Daarnaast moet het register van verwerkingsactiviteiten zorgvuldig worden bijgehouden, zodat de verwerkingen in het register actueel blijven en kan worden nagegaan of er nieuwe DPIA's moeten worden uitgevoerd.

Verder is het wenselijk om voorafgaand aan de DPIA een pre-DPIA uit te voeren. Aan de hand van een pre-DPIA kan worden beoordeeld of er sprake is van een hoog risico bij de verwerking, waardoor de organisatie verplicht is om een DPIA uit te voeren. Een pre-DPIA is een effectief instrument om - in het kader van de verantwoordingsplicht - aan te kunnen tonen dat de verwerking grondig is geëvalueerd. Ook zorgt de pre-DPIA ervoor dat de scope van de DPIA vooraf bekend is, zodat hiermee in de planning rekening kan worden gehouden.
Vanaf juli jl. is er een interne privacy officer aangesteld die zich o.a. bezighoudt met het uitvoeren van DPIA's. De privacy officer is echter slechts 16 uur per week beschikbaar voor de Regio.
De realiteit is dat het gezien de huidige arbeidsmarkt, lastig is om dit soort functies in te vullen. In het bijzonder voor het uitvoeren van noodzakelijke DPIA's met betrekking tot nieuwe Regiotaken die niet in de jaarkalender zijn opgenomen, zou het een overweging kunnen zijn om een externe privacy officer in te schakelen om deze taken uit te voeren.

De Regio zal vervolgens verder moeten gaan met het opschonen van persoonsgegeven die niet (meer) relevant zijn, om te kunnen voldoen aan de beginselen van dataminimalisatie en opslagbeperking. Hoewel de migratie naar de cloud heeft geleid tot het opschonen van oude mappen zonder duidelijke eigenaar die langere tijd ongebruikt waren - wat een positieve ontwikkeling is - moet ook aandacht worden besteed aan het verwijderen van informatie die is opgeslagen op zowel netwerkschijven als in de mailboxen. Het is belangrijk dat de Regio hier actief aandacht aan besteedt en medewerkers hiervan bewust maakt, bijvoorbeeld door een bericht hierover te plaatsen op de Binnenband.

10 Eenduidige registratie voor verantwoordingsplicht

Context
De in de AVG voorgeschreven verantwoordingsplicht houdt in dat je kunt aantonen dat je als organisatie aan de AVG voldoet. Hiervoor is een eenduidige registratie van privacyrelevante gebeurtenissen van belang. Zo is er naast het register van gegevensverwerkingen en het datalekken- en incidentenregister, een registratie van de afgesloten verwerkersovereenkomsten, de ontvangen verzoeken in het kader van rechten van betrokkenen (zoals inzageverzoeken), de pre-DPIA checklist waar mee kan worden aangetoond of de organisatie al dan niet verplicht is om een DPIA uit te voeren, het DPIA-register en de door de Fg gegeven adviezen en reacties daarop door betreffende organisatieonderdeel-manager.

Voortgang in verslagjaar
AVG-verzoeken die bij de Regio binnenkomen, worden in JOIN geregistreerd. Dossiers in JOIN worden nu - in plaats van op jaarbasis - per verzoek in JOIN gehangen. Er wordt nu per verzoek een dossier aangemaakt, waarin het binnenkomende verzoek, het besluit (inclusief begeleidende brief) en het proces-verbaal zit. Op dit punt is de Regio dan ook in control.

Nota bene: Er zijn dit verslagjaar nog geen AVG-verzoeken geweest. Dit is mede te verklaren door het feit dat veel inzage- en verwijderingsverzoeken op een andere grondslag worden gebaseerd (bij GGD en Jeugd en Gezin bijvoorbeeld op grond van de Wet geneeskundige behandelovereenkomst; bij Veilig Thuis op grond van de Wet maatschappelijke ondersteuning 2015).

Acties komende jaar
Doorgaan met structureel registeren van de verschillende registraties. Ook in het nieuwe verslagjaar is deze taak belegd bij de privacy officer.

11 Relaties met derde partijen

Context
De Regio werkt met verschillende partijen samen. Deze samenwerking kan ook veel verschillende vormen aannemen. Het goed duiden van de rollen (zelfstandig verwerkingsverantwoordelijke[3], gezamenlijk verwerkingsverantwoordelijken[4] en verwerker) en hier met betrokken partijen een gezamenlijk standpunt over in nemen, is één van de lastigste uitdagingen van de AVG. Zeker nu de feitelijke situatie hierin altijd doorslaggevend is.

Op het moment dat er sprake is van een verwerkingsverantwoordelijke en een verwerker dan worden de afspraken rondom privacy neergelegd in een 'verwerkersovereenkomst'. De organisatieonderdelen hebben zelf de verantwoordelijkheid dat verwerkersovereenkomsten op een juiste wijze worden afgesloten, namelijk volgens het meest recente model van de VNG[5]). De Fg en juridisch adviseurs zijn beschikbaar voor het beoordelen van de inhoud van de overeenkomst.
Bij gezamenlijke verwerkingsverantwoordelijkheid moeten afspraken in een 'onderlinge regeling' worden vastgelegd.

Op het moment dat organisatieonderdelen nieuwe gegevensuitwisselingen met derde partijen hebben, worden zij gevraagd dit altijd voor te leggen aan de betreffende juridisch adviseur.
Bij de verwerking van persoonsgegevens maakt de Regio in sommige gevallen gebruik van (digitale) diensten van externe partijen. Er wordt bij verschillende (digitale) werkprocessen gebruik gemaakt van andere organisaties die een opdracht krijgen tot verwerking van persoonsgegevens. Bij verwerking van persoonsgegevens door een derde partij die handelt ten behoeve van de Regio (als verwerkingsverantwoordelijke) en waarbij gegevensverwerking de primaire opdracht is, is de derde aan te merken als verwerker en moeten afspraken worden gemaakt in een verwerkersovereenkomst.

Overigens is niet voor elke uitbesteding van werk een verwerkersovereenkomst nodig. Als de derde partij zelf bepaalt waarvoor ze persoonsgegevens verwerkt en welke gegevens dat zijn dan is die partij waarschijnlijk zelf verwerkingsverantwoordelijke en is een verwerkersovereenkomst dus niet op zijn plaats.

In relatie tot de regiogemeenten het volgende. Voor taken die via een dienstverleningsovereenkomst bij de Regio zijn belegd is de Gemeenschappelijke Regeling Regio Gooi en Vechtstreek (hierna: de gemeenschappelijke regeling) uitgegaan van gezamenlijke verwerkingsverantwoordelijkheid met gemeenten. Voor taken die op andere wijze bij de Regio zijn belegd, te denken valt aan mandaat of machtiging, wordt aan de hand van de feitelijke situatie – indien nodig op basis van extern advies - beoordeeld waar de verwerkingsverantwoordelijkheid ligt.

Voortgang in verslagjaar
Met betrekking tot de relatie tussen de Regio en haar leveranciers is gebleken dat er in het verleden geen verwerkersovereenkomsten met (software)leveranciers van de Regio waren afgesloten. De Regio neemt hierin nu een meer leidende rol, waardoor de situatie inmiddels is verbeterd. De vorige Fg heeft in het kader van kwaliteitsbewaking gekeken naar de verwerkersovereenkomsten in JOIN. De uitkomst hiervan is dat verwerkersovereenkomsten nu standaard bij aanbestedingen worden meegestuurd en

[3] Een verwerkingsverantwoordelijke stelt het doel en de middelen van de verwerking vast, dat wil zeggen het 'hoe en waarom' van de verwerking.
[4] Van gezamenlijke verwerkingsverantwoordelijkheid is sprake bij een gezamenlijke deelname van twee of meer entiteiten aan de vaststelling van het doel en de middelen van een verwerkingsactiviteit.
[5] https://www.informatiebeveiligingsdienst.nl/product/handreiking-standaard-verwerkersovereenkomst-gemeenten/#download

afgesloten, waarbij gebruik wordt gemaakt van standaard verwerkersovereenkomst van de VNG. Op dit punt is de Regio in control.

Ten aanzien van de AVG-rolverdeling tussen de Regio en de regiogemeenten geldt – zoals hierboven beschreven - dat de gemeenschappelijke regeling per 1 mei jl. op dit punt is aangepast. In de regeling wordt nu uitgegaan van gezamenlijke verwerkingsverantwoordelijkheid tussen de Regio en de regiogemeenten.
Verder loopt er op dit moment een rechtszaak tussen een inwoner en de Regio waarvan de uitkomst mogelijk meer duidelijkheid over deze rolverdeling zal geven.

Daarnaast is gebleken dat in het afgelopen verslagjaar bij het beleggen van taken bij de Regio de bevoegdheid om persoonsgegevens te verwerken nog steeds niet altijd duidelijk is vastgelegd. Er zijn hier in het afgelopen verslagjaar geen acties op ondernomen. De Regio is op dit punt dus nog niet volledig in control.

Acties komende jaar
Om op het punt van de AVG-rolverdeling tussen Regio en regiogemeenten meer in control te komen, blijven de volgende acties van belang:
- Proberen te komen tot eenduidigheid over de AVG-rolverdeling tussen partijen en de bijbehorende afspraken.
- Een inventarisatie uitvoeren van de noodzaak om verwerkersovereenkomsten en overeenkomsten voor gezamenlijke verwerkingsverantwoordelijkheid af te sluiten tussen de Regio en de regiogemeenten voor de huidige taakuitvoeringen.
- Daadwerkelijk afsluiten van de overeenkomsten en dit goed registreren.
- In de tekst van de gemeenschappelijke regeling bij de verschillende vormen van overdracht van taken en bevoegdheden aangeven wat de meest aangewezen AVG-rolverdeling van partijen is.

12 Privacybeleid

Context
Wanneer een organisatie op grote schaal bijzondere persoonsgegevens verwerkt, dient zij een privacybeleid op te stellen en te hanteren. Binnen de Regio verwerken een aantal onderdelen op grote schaal bijzondere persoonsgegevens, voornamelijk gezondheidsgegevens. Daarom is het hebben van een privacybeleid voor de Regio een verplichting en dit beleid is er sinds 2021. Het privacybeleid is van toepassing op de gehele organisatie, inclusief alle processen, onderdelen, objecten en zowel geautomatiseerde als handmatige verwerkingen van persoonsgegevens door de Regio.
Het privacybeleid is een belangrijk instrument om vast te leggen hoe de Regio met persoonsgegevens omgaat. Het is een intern document en fungeert als een richtlijn voor medewerkers omtrent het verwerken van persoonsgegevens.

Voortgang in verslagjaar
Vorig verslagjaar heeft de Fg een begin gemaakt met het updaten van het privacybeleid, Aandachtsfunctionarissen privacy zijn meegenomen in het privacybeleid en enkele organisatieonderdelen hebben dit beleid naar het eigen organisatieonderdeel vertaald. Dit verslagjaar is dit onderdeel niet verder opgepakt. De Regio is op dit punt nog niet volledig in control.

Acties komende jaar
Onderstaande acties blijven ook dit verslagjaar van belang.
- Komend jaar is het belangrijk het privacybeleid bij de verschillende organisatieonderdelen beter bekend te maken. Hiervoor zal het beleid verder geconcretiseerd moeten worden per organisatieonderdeel, zodat het beter herkenbaar is voor de uitvoering. Dit kan door het maken van een versimpelde weergave van het beleid met organisatieonderdeel-specifieke aandachtspunten en door dit vervolgens met interactieve sessies bij de organisatieonderdelen te laten landen.
- Aanbevolen wordt om het bijhouden van het privacybeleid en het concretiseren naar de organisatieonderdelen te laten coördineren door een privacy officer in samenwerking met de

aandachtsfunctionarissen. De AP heeft specifiek voor het vormgeven van privacybeleid[6] aangegeven dat die taak niet bij de Fg mag liggen vanwege onverenigbaarheid met haar toezichthoudende rol.

- Het privacybeleid dient regelmatig geëvalueerd te worden en zo nodig aangepast. In 2021 is het privacybeleid vastgesteld. Er zijn wijzigingen in het privacybeleid voorbereid, maar deze moeten nog ter vaststelling aan het DB worden voorgelegd. Dit is in het afgelopen verslagperiode niet gebeurd. Dit blijft dan ook als actiepunt staan. Aan de wijziging van het beleid zullen acties gekoppeld worden die geprioriteerd zijn. Met de aanstelling van de privacy officer zou dat in het nieuwe verslagjaar kunnen worden bewerkstelligd.

13 Informatieplicht verwerkingen algemeen en websites

Context
Het is van belang dat de verwerkingsverantwoordelijke de personen waarvan zij persoonsgegevens verwerkt (voornamelijk inwoners en medewerkers) informeert over de verwerking en de rechten die zij hierbij kunnen uitoefenen. Een privacyverklaring op de website is hiervoor het meest logische middel.

Voortgang in verslagjaar
Ter invulling van het recht van inwoners om transparante informatie over de verwerking van persoonsgegevens te ontvangen, is er een algemene privacyverklaring voor alle verwerkingen van de Regio. Om te voldoen aan de informatieplicht uit de AVG is echter specifiekere informatie (toegespitst op de verwerking/set van verwerkingen) nodig. Daarom is er een sjabloon gemaakt voor drie soorten privacyverklaringen voor drie verschillende websites (organisatieonderdeel, thema en campagne). Vorig verslagjaar is hier al met een aantal organisatieonderdelen al een slag mee geslagen. Enkele privacyverklaringen zijn inmiddels volgens deze sjablonen opgesteld en in gebruik. Zo heeft het Zorg- en Veiligheidshuis inmiddels een privacyverklaring op het eigen deel van de landelijke website.[7] Ook RBL, Jeugd en Gezin en Veilig Thuis hebben inmiddels een actuele privacyverklaring op het eigen deel van de regionale website staan, zo bleek uit de inventarisatie die de Fg dit verslagjaar heeft gedaan. De overige organisatieonderdelen verwijzen nog naar de algemene website van de Regio. De privacyverklaringen zullen echter volledig op het organisatieonderdeel worden afgestemd op het moment dat het uniforme werkproces voor rechten van betrokkenen volledig geactualiseerd is. Op dit moment is de Regio op dit punt nog niet volledig in control.

Acties komende jaar
Het advies voor komend jaar is nog steeds om voor alle organisatieonderdelen die een website hebben een specifieke privacyverklaring op te stellen, omdat inwoners de verschillende organisatieonderdelen als losse organisaties ervaren, aparte verklaringen per organisatie beter toegankelijk zijn en deze beter aansluiten bij de verwachting en het referentiekader van de bezoekers. Een dergelijke aanpak sluit beter aan bij het uitgangspunt van de AVG van adequate informatievoorziening. Zoals hierboven eerder genoemd, wordt er gewerkt aan een uniform werkproces voor de rechten van betrokkenen. Vanwege de capaciteitstekorten is dit jaar de afweging gemaakt dat de Fg en aandachtsfunctionarissen privacy (ondersteund door de betreffende juridisch adviseur) hiervoor samen optrekken. Nu dit een taak is die in beginsel beter bij de privacy officer past, is het aan te bevelen dat de privacy officer in het nieuwe verslagjaar voldoende ruimte krijgt voor de privacyverklaringen.

Daarnaast is dit verslagjaar een privacyregeling voor medewerkers opgesteld, die de verwerkingen van persoonsgegevens op het werk beschrijft. De afspraak is gemaakt dat deze regeling in een privacyverklaring voor medewerkers wordt gegoten.

[6] AP treedt op tegen dubbelrol (binnenlandsbestuur.nl)
[7] https://www.zorgenveiligheidshuizen.nl/veiligheidshuizen/veiligheidshuis_gooienvechtstreek/privacyverklaring

14 Verzoeken i.h.k.v. rechten van betrokkenen

Context
Iedere persoon van wie persoonsgegevens worden verwerkt, heeft een aantal rechten met betrekking tot deze verwerking. Deze worden de rechten van betrokkenen genoemd. Deze rechten staan in de AVG, maar enkele komen ook (soms net iets anders) voor in de materiewetgeving die op bepaalde organisatieonderdelen van toepassing is.[8] De bekendste rechten betreffen het recht om een verzoek tot inzage, een verzoek tot rectificatie of een verzoek tot verwijdering of vernietiging in te dienen. Voor de afhandeling van de rechten van betrokkenen gelden wettelijk eisen die geborgd moeten worden in een proces.

Voortgang in verslagjaar
Er zijn in deze periode geen AVG-verzoeken door betrokkenen ingediend.
Verder is er dit verslagjaar een begin gemaakt met een uniform werkproces voor de rechten van betrokkenen voor alle organisatieonderdelen. De verwachting is dat het proces voor het einde van dit jaar zal staan waardoor de Regio op dit punt in control is.

Acties komende jaar
Binnen de Regio wordt gewerkt aan een eenduidige aanpak hoe verzoeken in het kader van de AVG-rechten van betrokkenen worden afgehandeld.
Het huidige werkproces inzageverzoeken en overige verzoeken op grond van artikelen 15 t/m18 AVG kan hiervoor als uitgangspunt dienen. Zoals hierboven beschreven, is voor dit jaar de afweging gemaakt dat de Fg deze taak – in samenspraak met de aandachtsfunctionarissen – op zich neemt. Deze taak hoort in beginsel meer tot het takenpakket van de privacy officer. Het wordt aanbevolen dat de privacy officer in het nieuwe verslagjaar de privacyverklaringen die worden afgestemd op het werkproces, oppakt.

15 Datalekken

Context
Op de werkvloer kunnen fouten worden gemaakt. Wanneer deze fouten betrekking hebben op de veiligheid van informatie, spreken we van een informatieveiligheidsincident. Een informatieveiligheidsincident wordt aangemerkt als een datalek wanneer er sprake is van toegang tot, vernietiging, wijziging of onbedoeld vrijkomen van persoonsgegevens.
De organisatie stimuleert het intern melden van mogelijke datalekken bij het Team Privacyincidenten. Het op de juiste manier afhandelen van meldingen draagt bij aan een voortdurende verbetering van de organisatie.
Indien er sprake is van een risico voor inwoners of medewerkers, moet het datalek worden gemeld bij de AP. Wanneer dit risico als hoog wordt ingeschat moet het datalek ook worden gemeld aan de betrokkenen van wie de persoonsgegevens zijn geraakt.

Voortgang in verslagjaar
De Regio kent een Team Privacyincidenten. Dit team bestaat uit de Fg, de privacy officer, een van de juridische adviseurs, de bestuurssecretaris en – in geval van meldingen die te maken hebben met informatiebeveiliging – de CISO. Er is een verdeling gemaakt waarbij een ieder zich op een dag van de week bezighoudt met de beoordeling en afhandeling van mogelijke datalekken die via de postbus worden gemeld. De voorgestelde maatregelen worden altijd in overleg met het gehele team afgestemd.

[8] Grofweg komt het erop neer dat betrokkenen bij een beroep op de AVG hun rechten kunnen laten gelden t.a.v. losse persoonsgegevens, terwijl bij een beroep op de Wet op de geneeskundige behandelovereenkomst (Wgbo), Jeugdwet of Wmo 2015 de rechten gelden t.a.v. het document/dossier zelf.

In het afgelopen verslagjaar zijn intern zesentwintig informatieveiligheidsincidenten gemeld. Dit is één incident minder dan in het verslagjaar hiervoor. Van de meldingen bleek het in drieëntwintig gevallen daadwerkelijk om een datalek te gaan. De meeste datalekken deden zich voor bij Veilig Thuis en Jeugd en Gezin. Van deze drieëntwintig datalekken was in elf gevallen sprake van een risico voor betrokkenen waardoor gemeld moest worden aan de Autoriteit Persoonsgegevens. Van deze drieëntwintig gevallen is in negen gevallen ook melding aan betrokkenen gemaakt, eenmaal uit zorgvuldigheid, vijf keer omdat er werkelijk een hoog risico was. Hieronder is in tabelvorm aangegeven wat de cijfers zijn van de andere verslagjaren sinds het van toepassing zijn van de AVG.

Verslagjaren	**'18-'19**	**'19-'20**	**'20-'21**	**'21-'22**	**'22-'23**	**23-'24**
Gemelde informatieveiligheidsincidenten	21	21	48	39	27	26
Datalekken	12	10	25	20	15	23
Gemeld aan AP	7	0	9	12	5	11
Gemeld aan betrokkene	6	0	5	7	5	9

De meest voorkomende datalekken vielen in de categorieën 'toegankelijkheid van persoonsgegevens voor niet-bevoegde persoon' op ruime afstand gevolgd door 'versturen van persoonsgegevens aan verkeerde ontvanger'. De Regio is op dit punt (nagenoeg) in control.

Acties komende jaar
Er zal blijvend aandacht moeten worden gevraagd voor het vergroten van bewustwording bij medewerkers. Het is aan te bevelen om gedurende het komende verslagjaar regelmatig berichten op de Binnenband te plaatsen om medewerkers te informeren over datalekken en hen te stimuleren deze te melden. Hierbij zal benadrukt moeten worden dat het melden van een datalek een positieve en waardevolle actie is. Daarnaast zou overwogen kunnen worden om een kleine beloning, zoals een reep chocolade, te verstrekken aan medewerkers die een datalek melden, als blijk van waardering.

Verder is het aan te bevelen om medewerkers jaarlijks een e-learning module te laten volgen om hun kennis op het gebied van gegevensbescherming en bewustwording te vergroten.

16 Informatieveiligheid

Context
Een goede inrichting van informatieveiligheid is belangrijk voor een optimale bescherming van persoonsgegevens.

Voortgang in verslagjaar
In mei van dit jaar is er een CISO aangesteld. Deze bepaalt het strategisch beleid rondom alle informatiebeveiliging en zorgt dat dit beleid wordt gecommuniceerd, uitgerold en organisatie breed wordt gedragen.

Inmiddels is bekend geworden dat de CISO de Regio per 1 januari 2025 zal verlaten. Er is nog geen structurele vervanging voor deze functie gevonden.

Acties komende jaar
In 2025 zal een start worden gemaakt met het certificeringstraject van NEN 7510; de norm voor informatiebeveiliging in de zorg. Dit is een tijdrovend proces en om die reden worden er momenteel externe specialisten ingehuurd ter ondersteuning.

Als onderdeel van dit traject zal het strategisch informatieveiligheidsbeleid tactisch moeten worden uitgewerkt. Dit omvat onder andere het verder ontwikkelen en naar een hoger niveau tillen van de informatieveiligheidsmaatregelen. Zo ook het opstellen van een duidelijke beschrijving hiervan. In dit verslagjaar zijn daar nog geen stappen in gezet. Veel van de noodzakelijke maatregelen worden wel al

in meer of mindere mate toegepast, maar dat is niet aantoonbaar en die aantoonbaarheid is voor de NEN 7510 wel vereist.

17 Oordeel over afgelopen jaar en aanbeveling

De Regio scoort groen op de volgende onderdelen: organisatorische inbedding, kennis en kunde, advisering, informatieverstrekking en inlichting, eenduidige registratie voor verantwoordingsplicht en voor datalekken.
Op enkele punten scoort de Regio echter oranje, wat aangeeft dat de Regio daar nog een verbeterslag moet maken. Nota bene: de onderdelen waarop de Regio groen scoort, dienen doorlopend onderhouden te worden om deze status te behouden.

Met de aanstelling van een aparte privacy officer is er dit verslagjaar een belangrijke verbetering gerealiseerd op het onderdeel organisatorische inbedding.

De scheiding van taken heeft ervoor gezorgd dat de privacy officer zich volledig heeft kunnen richten op de uitvoering van de meest urgente privacytaken, terwijl de Fg toezicht kon houden op de naleving. Het is echter zo dat ook de Fg soms nog in de uitvoering betrokken is, aangezien de privacy officer slechts beperkt beschikbaar is, wat geen wenselijke situatie is. De Regio zou in deze rolverdeling nog in volwassenheid moeten groeien.

De AP heeft zich herhaaldelijk uitgesproken over de noodzaak om uitvoerende en toezichthoudende privacytaken duidelijk te onderscheiden. Dit is des te belangrijker in een organisatie die veel gevoelige persoonsgegevens verwerkt.

Hoewel de scheiding van taken tussen de privacy officer en de Fg een verbetering is, zitten we dit verslagjaar – per saldo - op een lagere capaciteit dan vorig jaar. Dit komt door de huidige krapte op de arbeidsmarkt, waardoor het lastig is geschikte kandidaten te vinden. Voor het nieuwe verslagjaar blijft dit een aandachtspunt.

Het is aan te bevelen om de gestelde formatie in elk geval beschikbaar te houden, zodat als zich in de toekomst een geschikte kandidaat aandient, daar direct op kan worden ingegaan. Ook kan worden overwogen om tijdelijk externe capaciteit in te huren, bijvoorbeeld in de vorm van een tweede privacy officer die bij specifieke projecten kan ondersteunen.

Het volledig beschikbaar stellen van een medewerker voor uitvoerende privacytaken helpt de organisatie om de onafhankelijke adviezen van de Fg in een werkbare oplossing te gieten.
Bovendien komt de Fg op deze manier meer toe aan de proactieve toezichthoudende taak, zowel voor de AVG als de Wpg.

Als er voor wordt gekozen om de benodigde capaciteit niet beschikbaar te houden, is de consequentie dat de Regio niet duurzaam kan voldoen aan de AVG. De bescherming van persoonsgegevens van zowel inwoners als medewerkers kan dan niet optimaal worden verwezenlijkt. Daarmee kan de Regio kwetsbaar zijn voor handhavende maatregelen van de AP en mogelijke aansprakelijkstellingen door inwoners.