Rapport ‘Stand van zaken gegevensbescherming 2023’

Regionale Sociale Dienst

KROMME RIJN HEUVELRUG

Regionale Sociale Dienst
KROMME RIJN HEUVELRUG

Inhoudsopgave

Voorwoord

Met het rapport 'Stand van zaken Gegevensbescherming' leg ik gelijktijdig verantwoording af en documenteer ik welke werkzaamheden de RDWI het afgelopen jaar heeft uitgevoerd om te voldoen aan de privacywetgeving. De verantwoording, zoals in dit rapport is verwoord, gaat in op het algemene beeld van de compliance ten aanzien van de AVG en Wpg, de uitgevoerde activiteiten en opgeleverde producten, de bevindingen over het jaar 2023 en de aandachtspunten voor 2024.

Privacy heeft een vaste plek binnen de organisatie gekregen. Dat is een mooie ontwikkeling. Maar even zo is er nog veel winst te behalen op diverse vlakken waarbij continue aandacht voor het onderwerp een vereiste is om te blijven groeien. Privacy, en alles wat daar bij komt kijken om aan de privacywetgeving te voldoen, wordt nog vaak gezien als 'dat is van de privacy-professionals'. Maar privacy is van ons allemaal en iedereen in de organisatie heeft hierin een taak en verantwoordelijkheid. 'Hoe maak je privacy van ons allemaal?' wordt voor mij het komend jaar een centraal steeds terugkerend thema.

Het rapport 'Stand van zaken Gegevensbescherming 2023' wordt aangeboden aan het dagelijks bestuur van de RDWI als eindverantwoordelijke voor de verwerking van persoonsgegevens binnen de RDWI. Ik vraag het dagelijks bestuur kennis te nemen van het rapport en de hierin opgenomen aanbevelingen voor 2024.

Zeist, 6 maart 2024,

Functionaris Gegevensbescherming

Managementsamenvatting

De RDWI verwerkt bij de uitvoering van haar taken persoonsgegevens van inwoners. De Algemene verordening gegevensbescherming (AVG) en de Wet politiegegevens (Wpg) stellen de kaders voor een zorgvuldige omgang met deze persoonsgegevens en bepalen onder andere dat organisaties niet meer gegevens verzamelen dan strikt noodzakelijk is voor het doel waarvoor deze zijn verzameld. Daarnaast legt de AVG en de Wpg aan organisaties de verplichting op om de zorgvuldige omgang met persoonsgegevens aantoonbaar te maken. Dit rapport beschrijft waar de RDWI staat op het gebied van privacy, waar de grootste risico's liggen en wat er moet gebeuren om deze risico's te beperken.

In het eerste deel van dit rapport worden de diverse verplichtingen uit de AVG behandeld. Hier wordt uitgelegd wat de verplichting inhoudt, in hoeverre de RDWI voldoet aan de verplichting, welke werkzaamheden op dit vlak zijn uitgevoerd in 2023 en worden aanbevelingen gedaan op punten waar de organisatie nog niet of niet volledig aan voldoet. Om alvast een beeld te geven van de risico's en aanbevelingen die volgen in het rapport, zijn deze als volgt samengevat:

- Het huidige privacybeleid 2022-2024 moet worden geupdatet en vastgesteld voor de komende periode 2025-2027 waarbij als aandachtpunt geldt het beschrijven van de verschillende taken, rollen en verantwoordelijkheden binnen de privacyorganisatie.
- Om aantoonbaar compliant te zijn aan de AVG, stelt de AVG een aantal verplichte instrumenten voor. De status van deze instrumenten worden jaarlijks beoordeeld (in deze rapportage). Een van deze instrumenten is het bijhouden van een register van verwerkingen met tot doel zicht te krijgen op de (risicovolle) verwerkingen die plaatsvinden binnen de organisatie. Kennis over nut en noodzaak van het register van verwerkingen is nog niet breed aanwezig en behoeft aandacht voor het komende jaar.
- Een ander verplicht instrument is het uitvoeren van een DPIA, een data protection impact assessment. Een DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen zodat de organisatie maatregelen kan nemen om deze risico's te verkleinen. In 2023 is geconstateerd dat er een achterstand is in de uitvoering van DPIA's. Deze achterstand is nog niet ingehaald. Dit bekent dat ook in 2024 een hernieuwde prioritering in uit te voeren DPIA's door het managementteam moet worden vastgesteld. Prioritering is nodig vanuit de wetenschap dat het uitvoeren van een DPIA een zware stempel drukt op de bedrijfsvoering en te veel gelijktijdig lopende DPIA's niet haalbaar is.
- In 2023 is de aanbeveling opgenomen om te komen tot het instellen van een risicoregister. Inmiddels zijn gesprekken gevoerd op welke wijze risicomanagement ook over geconstateerde privacy risico's kan worden uitgerold. Dit zal in 2024 een vervolg krijgen.
- Er is op sommige plekken binnen de organisatie onvoldoende bekendheid over diverse privacy procedures binnen de organisatie. Het is van belang dat medewerkers zich bewust zijn van bestaand beleid, procedures en werkwijzen. Dit vergt aandacht voor het komende jaar.

In het tweede deel wordt ingegaan op de verwerking van persoonsgegevens voor opsporing en vervolging van strafbare feiten. Binnen de RDWI is de sociaal rechercheur, de bijzonder opsporingsambtenaar (boa), belast met de opsporing van uitkeringsfraude. De boa mag in zijn taakuitoefening specifieke

opsporingsbevoegdheden inzetten. Dit maakt dat de Wpg van toepassing is. De Wpg kent een auditverplichting. In het kader van deze auditverplichting is geconstateerd dat de RDWI niet voldoet aan de vereisten uit deze wet (auditrapport van augustus 2022). Het in 2023 gestarte verbetertraject is voor een (groot) deel uitgevoerd maar medio 2023 gepauzeerd aangezien de bij de RDWI werkzame boa uit dienst is getreden. Het niet in dienst hebben van een boa betekent dat er geen opsporingsbevoegdheden kunnen worden ingezet, hetgeen betekent dat de Wpg niet van toepassing is. Deze (tijdelijke) situatie maakt dat op dit moment ook geen FG toezicht kan worden uitgevoerd.

Inleiding

De Regionale Dienst Werk en Inkomen (RDWI) verwerkt persoonsgegevens van inwoners uit de gemeenten Zeist, De Bilt, Bunnik, Utrechtse Heuvelrug en Wijk bij Duurstede bij de uitvoering van haar taken. Daarnaast verwerkt zij persoonsgegevens van medewerkers, zakenrelaties, leveranciers en dergelijken. Het verwerken van deze persoonsgegevens moet plaatsvinden volgens de regels van de Algemene verordening gegevensbescherming (AVG), en voor zover het strafrechtelijke gegevens betreft, de Wet politiegegevens (Wpg). Beide wetten bieden waarborgen voor het beschermen van deze gegevens. Dit is belangrijk omdat de gevolgen van onjuist en onzorgvuldig gebruik van persoonsgegevens grote impact kan voor betrokkenen.

De verwerking van persoonsgegevens door bijzondere opsporingsambtenaren (boa's) valt sinds de inwerkingtreding van de AVG onder de Wpg. De opsporing van strafbare feiten door boa's valt daarmee buiten het bereik van de AVG. Verwerking van persoonsgegevens op strafrechtelijke grond moet voldoen aan de vereisten van de Wpg. Werkgevers van boa's hebben daarmee bij de verwerking van persoonsgegevens bij handhavingstaken te maken met zowel de AVG als de Wpg. Dit betekent dat binnen de bedrijfsvoering rekening moeten houden met voorschriften en verplichtingen uit beide wettelijke regimes.

De AVG en de Wpg gaan uit van een zogenaamd accountability–principe hetgeen inhoudt dat iedere organisatie die persoonsgegevens verwerkt, moet kunnen aantonen dat

(1) zij persoonsgegevens verwerkt volgens de AVG- en/of Wpg-richtlijnen en;
(2) zij daartoe de juiste technische en organisatorische maatregelen treft om de persoonsgegevens te beveiligen.

Vanuit dit principe zijn er in beide wetten diverse verplichtingen opgenomen, denk hierbij onder meer aan het verplicht aanstellen van een functionaris gegevensbescherming, het bijhouden van een register van gegevensverwerkingen, het bijhouden van een register met datalekken en het uitvoeren van DPIA's (data protection impact assesment[1]).

De functionaris gegevensbescherming (FG) van de RDWI informeert en adviseert de organisatie over de uitvoering van de AVG en de Wpg vanuit een toezichthoudende rol. Dit houdt in dat de FG erop toeziet dat de RDWI voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens en hierover rapporteert. Dit rapport bevat de bevindingen over het jaar 2023.

Leeswijzer

Dit rapport bestaat uit twee delen. Het eerste deel beschrijft de stand van zaken en bevindingen gericht op de AVG. Het tweede deel richt zich op de Wpg. Het rapport is onderverdeeld in thema's[2] die - zo nodig - afsluiten met aanbevelingen voor het komende jaar.

[1] Een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen.
[2] Hierbij wordt het template van de Informatie Beveiligings Dienst (IBD), onderdeel van de VNG, gevolgd.

Deel 1 Stand van zaken en bevindingen AVG

Sinds de komst van de AVG is het de plicht aan organisaties om persoonsgegevens goed te beschermen. De AVG dwingt organisaties om veilig en zorgvuldig om te gaan met de persoonsgegevens die worden verwerkt. En dit moet aantoonbaar zijn, de zogenaamde verantwoordingsplicht uit de AVG.

Het implementeren van de AVG is geen eenmalige actie, maar vraagt om continue aandacht. Om de effectiviteit te borgen en tijdig in te kunnen spelen op nieuwe ontwikkelingen en risico's, is het dus belangrijk om jaarlijks te monitoren hoe de organisatie ervoor staat op privacy-vlak én hierover te rapporteren. Vragen die hierbij aan de orde komen zijn: Waar staan we als organisatie? Maken we vorderingen? En zo ja, in de juiste richting? Of zijn er verbeteringen/aanvullende maatregelen/acties nodig?

Hierna wordt per thema de huidige stand van zaken beschreven, gevolgd door bevindingen en aanbevelingen voor de komende periode. Er worden zeven thema's onderscheiden:

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

Beleid

Inwoners die zich melden bij de RDWI moeten erop kunnen vertrouwen dat de RDWI zorgvuldig met hun persoonsgegevens omgaat. Het kader voor het verwerken van persoonsgegevens en de principes waar de RDWI zich aan houdt, zijn uitgewerkt in het privacybeleid. In dit beleid wordt onder meer de privacyorganisatie beschreven qua taken en verantwoordelijkheden.
Op de website van de RDWI, www.rsdkrh.nl, worden derden (inwoners van de deelnemende gemeenten of bezoekers van de website) uitvoerig geïnformeerd over het privacybeleid in de daar opgenomen privacyverklaring. Het privacybeleid is tevens te vinden op de intranetsite van de RDWI en daarmee beschikbaar voor medewerkers.

Het in 2022 vastgestelde privacybeleid 2022-2024 is in 2023 tussentijds gewijzigd als gevolg van de uitkomsten van de verplichte Wpg-audit. Met deze wijziging zijn de algemene uitgangspunten, rollen, taken en bevoegdheden ten aanzien van verwerkingen van politiegegevens opgenomen in het huidige privacybeleid (zie hierna deel 2 voor nadere toelichting).

In het kader van de verantwoordingsverplichting uit de AVG wordt het privacybeleid jaarlijks beoordeeld om te controleren of zij nog in voldoende mate aansluit op de realiteit en wordt het beleid tenminste een keer per drie jaar volledig herzien. Uit deze controle is gebleken dat het beleid functies beschrijft die niet zijn ingevuld of niet bestaan in de organisatie. Dit levert een risico op.

<u>Aanbeveling</u>

- Herzie het huidige privacybeleid 2022-2024 geldend voor een komende periode van 3 jaar.

Processen

Register van verwerkingen

De RDWI moet kunnen aantonen welke verwerkingen van persoonsgegevens plaatsvinden in de organisatie. Hiertoe heeft de RDWI een register van verwerkingen. Het register biedt inzicht in de processen waarbij persoonsgegevens worden verwerkt, de systemen die we hiervoor gebruiken en wie verantwoordelijk is voor de verwerking.

Het register is begin 2022 opgeleverd na een uitgebreide revisie, waarbij tevens de procedure voor het bijhouden van dit register is vastgesteld en intern gecommuniceerd. Het register is in 2023 niet tussentijds aangevuld terwijl er wel nieuwe verwerkingen zijn geïmplementeerd. Dit wijst er op dat er intern onvoldoende kennis is van de verplichting elke nieuwe tussentijdse verwerking op te nemen in het register van verwerkingen.

Eind 2023 is de jaarlijkse check op volledigheid van dit register gestart. Deze is nog niet afgerond en loopt door in 2024. Inmiddels, ten tijde van het schrijven van dit rapport, is het register voor meer dan de helft gecontroleerd en waar nodig aangepast.

Aanbeveling

- Besteed intern aandacht aan het opvolgen van de verplichting van een jaarlijkse controle, en de verplichte tussentijdse aanvullingen als gevolg van nieuwe verwerkingen, van het register van verwerkingen.

Government, Risk en Compliance: de GRC-tool

Er is in regionaal verband (samen met de ZOU-gemeenten[3]) een softwaresysteem aangeschaft voor risicobeheersing en compliance op het gebied van informatieveiligheid en privacy, de zogenaamde GRC-tool. Met de aanschaf van dit systeem wordt beoogd de kwaliteit van de processen van risicobeheersing en compliance op het gebied van informatiebeveiliging en gegevensbescherming te optimaliseren. Gezien de complexiteit van dit systeem strandde de ingebruikname in voorgaande jaren. Eind 2023 is opnieuw gestart met de implementatie van de GRC-tool. De verwachting is dat deze gedurende het jaar in delen in gebruik wordt genomen.

Data Protection Impact Assesment (DPIA)

In sommige gevallen is het verplicht om een DPIA uit te voeren: een instrument om voorafgaand aan de verwerking de risico's van de verwerking in kaart te brengen. Hierbij gaat het om het waarborgen van de privacy van de klant en de over de klant verzamelde persoonsgegevens te beschermen tegen misbruik. De AP heeft richtlijnen opgesteld om te kunnen vaststellen in welke gevallen het uitvoeren van een DPIA verplicht is. Het uitvoeren van een DPIA vergt diepgaande kennis over het proces en de systemen waarmee gewerkt wordt. Dit is ook meteen de meerwaarde van het uitvoeren van een DPIA voor de organisatie: het vergroten van de kennis over je 'eigen' proces.

In 2023 is geconstateerd dat er een achterstand is in de uitvoering van DPIA's. Deze achterstand is nog niet ingehaald. Dit bekent dat ook in 2024 een hernieuwde prioritering in uit te voeren DPIA's door het managementteam moet worden

[3] Gemeenten in de regio Zuidoost Utrecht

vastgesteld. Prioritering is nodig vanuit de wetenschap dat het uitvoeren van een DPIA een zware stempel drukt op de bedrijfsvoering en te veel gelijktijdig lopende DPIA's niet haalbaar is.

Het wel of niet uitvoeren van een DPIA is geen keuze maar een wettelijke verplichting waarop de AP actief toezicht houdt. Dit blijkt onder meer uit de recente opgelegde boete aan ICS voor het achterwege laten van een risicoanalyse[4]. De AP benadrukt in dit besluit nogmaals dat het voorafgaand aan de werking uitvoeren van de DPIA ertoe leidt dat van tevoren maatregelen kunnen worden genomen om de privacy van betrokkenen te beschermen.

Cijfers over 2023

- In 2023 zijn twee DPIA's afgerond.
- Tevens zijn er 4 DPIA's gestart die nog niet zijn afgerond
- In 2023 zijn twee DPIA's in een vroeg stadium gepauzeerd welke in 2024 zullen worden herstart.

<u>Aanbevelingen</u>

- De huidige procedure voor het uitvoeren van een DPIA dateert uit 2022 en zal komend jaar opnieuw moeten worden beoordeeld op juistheid en werkbaarheid.
- Het is van belang dat ondanks dat het uitvoeren van DPIA's een zware stempel drukt op de organisatie, dit proces geborgd wordt in de standaard bedrijfsvoering en een automatisme gaat worden bij het implementeren van een nieuw proces of nieuwe verwerking.
- Stel een prioritering vast in uit te voeren DPIA's.

Adviezen

In 2023 zijn er FG-adviezen en/of signalen verstrekt aan het managementteam/de organisatie. Een greep uit de onderwerpen van deze adviezen/signalen:

- Een algoritmeregister: De regering wil dat de overheid algoritmes verantwoord gebruikt. Verantwoord inzetten van algoritmes betekent dat ten minste voldaan moet worden aan wet- en regelgeving en dat de inzet in lijn is met publieke waarden en ethische principes (denk hierbij aan menselijke controle, rechtvaardigheid, privacy en non-discriminatie). In 2023 is gestart met een inventarisatie van eventueel gebruik van algoritmes binnen de dienstverlening. Met een dergelijke inventarisatie kan een afweging worden gemaakt of de RDWI een eigen publiek algoritmeregister gaat implementeren of aansluit bij het Algoritmeregister van de Nederlandse overheid.
- Nieuwsberichten: een overzicht van recente ontwikkelingen op het gebied van de toezichthoudende rol van de AP en welke lessen hieruit te trekken zijn voor de organisatie.
- Advies over opvolging brief van de AP inzake bevragingen Inlichtingenbureau.
- Het signaal over het ontbreken van een verplichte terugmeldvoorziening bij gebruik van de Basisregistratie personen (BRP).
- Signaal naar aanleiding van boetebesluit van de AP aan de SVB om het eigen proces 'telefonisch identiteitscontrole' onder de loep te nemen.

<u>Aanbevelingen</u>

[4] https://autoriteitpersoonsgegevens.nl/actueel/boete-voor-creditcardbedrijf-ics-na-ontbrekende-risicoanalyse

- Hoe en of FG-adviezen worden opgevolgd is aan de verwerkingsverantwoordelijke, het managementteam. Het kan voorkomen dat adviezen op de plank blijven liggen door bijvoorbeeld tijdsgebrek of andere prioriteiten. Om het zicht op deze adviezen, en de (mogelijk) geconstateerde risico's, niet te verliezen, is in 2023 aanbevolen een privacy risicoregister in gebruik te nemen en deze periodiek op de agenda van het managementteam te plaatsen. Deze werkwijze is (nog) niet geïmplementeerd waardoor er geen volledig zicht is op geconstateerde risico's en de opvolging hiervan. Het verdient aanbeveling het onderzoek naar de wijze waarop risicomanagement kan worden toegepast op geconstateerde privacy risico's af te ronden met implementatie van een voor de organisatie geschikte werkwijze. Doel hiervan is het behouden van zicht op onbehandelde risico's en het verstrekken van inzicht in waar en bij wie dit risico is belegd. Immers: het niet hebben van een risico-eigenaar is een risico op zich voor de organisatie.
- De inventarisatie van het gebruik van algoritmes is stil gevallen. Het verdient aanbeveling deze weer op te pakken.

Organisatorische inbedding

De informatieveiligheid en privacyorganisatie

Voor een goede en juiste uitvoering van de AVG is het van belang dat eenieder binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en het creëren van (informatieveiligheid en) privacy-bewustzijn.

De RDWI heeft hiertoe begin 2023 een (hernieuwde) blauwdruk[5] vastgesteld voor de informatieveiligheid- en privacyorganisatie (IV&P). Wijzigingen betroffen met name de ter beschikking gestelde fte voor de verschillende rollen in de IV&P-organisatie. Bij vaststelling van deze blauwdruk werd al gesignaleerd dat het risico bestond dat invulling van de benodigde fte, gezien de huidige arbeidsmarkt, moeizaam zou kunnen verlopen. Dit is ook zo gebleken hetgeen direct gevolgen heeft voor het borgen van de taken op het gebied van informatieveiligheid en privacy.

Inmiddels is voor de functie van privacy-officer gekozen voor het opzetten van een intern opleidingstraject onder begeleiding van een extern ingehuurde privacy professional. Voor de structurele invulling van rollen op het terrein van informatieveiligheid wordt in de regio op dit moment onderzoek gedaan naar mogelijke samenwerking (tussen de ZOU-gemeenten) om zo de krapte op de arbeidsmarkt het hoofd te bieden.

<u>Aanbevelingen</u>

- Het document Blauwdruk IV&P-organisatie v2.0 is een levend document welk jaarlijks tegen het licht moet worden om te beoordelen of de daarin genoemde randvoorwaarden zijn ingevuld.
- Het document Blauwdruk IV&P-organisatie v2.0 bevat nog 'lege plekken' die moeten worden aangevuld. Dit betreft mede het opstellen van (een deel van de) functiebeschrijvingen van de bij de IV&P-organisatie betrokken functies.

[5] Blauwdruk IV&P-organisatie v2.0 vastgesteld op 16 maart 2023 door het DB

Bewustwording
In 2023 is de RDWI gestart met een nieuwe bewustwordingsprogramma voor de medewerkers 'Bewust in control'. De methode van 'Bewust in control' is geënt op het periodiek aandacht vragen voor het onderwerp informatieveiligheid en privacy waardoor medewerkers continu getriggerd worden om hier even over na te denken zonder dat het hen veel tijd kost.

'Bewust in control' bevat de volgende instrumenten: trainingen voor nieuwe medewerkers (deze is bij aanvang van het programma voor alle medewerkers verplicht is gesteld), nano-learning (frequent aanbieden van kort stukjes lesstof in per mail verstuurde vragen), per kwartaal een korte training over een specifiek onderwerp en een halfjaarlijkse phishingmailaktie.

Vanuit het management is het volgen van dit programma verplicht gesteld om een maximale deelnamebereidheid te bereiken. Periodiek wordt gerapporteerd over de deelnamegraad aan de unitmanagers die hierop sturen. Met dit programma heeft de RDWI een gedegen bewustwordingsprogramma in huis gehaald.

Vanuit de IV&P-organisatie worden voorts regelmatig berichten op het intranet geplaatst om het onderwerp informatieveiligheid en privacy levend te houden.

Inkoop
In 2023 heeft privacy en informatiebeveiliging een vaste plek in het inkoopproces gekregen zodat dit onderwerp aan het begin van het inkooptraject direct wordt meegenomen. Hiermee borgt de RDWI de zorgplicht (artikel 25 AVG) om aan de voorkant van het inkoopproces na te denken over passende technische en organisatorische maatregelen en eisen en zorg te dragen dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk.

Reglement functionaris voor de gegevensbescherming (FG-reglement)
In 2023 is het FG-reglement vastgesteld. Hiermee legt de RDWI vast op welke wijze zij de FG heeft gepositioneerd als ook welke taken en verantwoordelijkheden de FG heeft en hoe de organisatie de FG faciliteert in een goede uitvoering hiervan.

<u>Aanbevelingen</u>
- Er is nog onvoldoende bekendheid bij de medewerkers betrokken bij het inkoopproces over waar welke verantwoordelijkheden voor privacy en informatiebeveiliging liggen waardoor het gevaar bestaat dat deze onderwerpen tussen wal en schip geraken. Duidelijkheid creëren over wie waarvoor aan de lat staat, is essentieel voor het borgen van privacy en informatieveiligheid in het inkoopproces. Plan gesprekken hierover in.

Rechten van betrokkenen
De RDWI dient degene van wie zij de persoonsgegevens verwerkt (de betrokkene) zowel actief als passief te informeren over deze verwerking, de wijze van het verwerken, de grondslag en de maatregelen die zij neemt om onrechtmatige toegang en onrechtmatige verwerking te voorkomen. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. Op de website informeert de RDWI betrokkenen hierover.

In 2023 zijn in totaal zes (6) AVG-verzoeken, waarvan vier (4) inzageverzoeken en een (1) verwijderingsverzoek, en een (1) AVG-gerelateerde klacht ontvangen.

Alle inzageverzoeken zijn toegekend. Het verwijderingsverzoek is, na uitleg over de van toepassing zijnde regels omtrent bewaartermijnen, ingetrokken. Een toegekend verwijderingsverzoek uit 2022 is in 2023 uitgevoerd na implementatie van benodigde software. De AVG-gerelateerde klacht is behandeld waarbij klager uitleg is gegeven.

In 2023 is gestart met de bouw van een specifiek voor dit proces ingericht werkproces in het zaaksysteem zodat registratie en archivering van en verantwoording over het proces volledig is geborgd. Dit wordt afgerond in 2024.

Samenwerking

De RDWI werkt op meerdere terreinen, in verschillende functies, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In die gevallen dat er sprake is van een verwerking van persoonsgegevens tussen de partijen, het ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens, is de AVG van toepassing. Iedere partij blijft er primair zelf verantwoordelijk voor dat persoonsgegevens goed beschermd zijn. In aanvulling hierop worden verplicht afspraken gemaakt over de omgang met de persoonsgegevens. Dit kan bijvoorbeeld in een gegevensdelingsovereenkomst of een verwerkersovereenkomst. Welke van toepassing is, is afhankelijk van de rol en positie van betrokken partijen.

Verantwoordelijkheid voor het opmaken van deze overeenkomsten ligt bij de verantwoordelijke unitmanager of teamcoördinator. Het opstellen van deze overeenkomsten wordt als lastig ervaren. In het geval er gebruik wordt gemaakt van een verwerker, geldt het principe dat er geen gegevens mogen worden gedeeld zolang de verwerkersovereenkomst niet is getekend door beide partijen. Dit wordt niet altijd opgevolgd. Voor dit principe is aandacht nodig. De RDWI maakt gebruik van een instructiedocument voor de interne medewerker én voor de externe verwerker ter ondersteuning bij het invullen van een verwerkersovereenkomst.

Juridisch kader voor gegevensdeling

In 2023 is gestart met een onderzoek[6] naar de mogelijkheden van het delen van (persoons)gegevens tussen de RDWI en de deelnemende gemeenten. Dit naar aanleiding van gebleken behoefte aan duidelijkheid over de vraag wanneer persoonsgegevens nu wel en wanneer deze niet mogen worden gedeeld met de gemeenten. Het omvangrijke onderzoek heeft niet geleid tot een duidelijk standpunt, handzaam kader, welk gebruikt kan worden voor een standaardisering in de beoordeling van verzoeken tot gegevensdeling. Dit betekent dat elk verzoek tot het delen van persoonsgegevens op zijn merites moet worden beoordeeld. In 2023 zijn er geen formele verzoeken tot het delen van persoonsgegevens van de deelnemende gemeenten ontvangen.

<u>Aanbeveling</u>:

- Het proces rondom de totstandkoming van de verwerkersovereenkomst is nog niet geheel duidelijk bij alle betrokkenen. Dit vergt aandacht.

Beveiliging

De AVG legt de verantwoordelijkheid om aan te tonen dat aan de privacyregels wordt voldaan uitdrukkelijk bij de organisatie zelf. Eén van de maatregelen om aan de verantwoordingsplicht te voldoen is de verplichting tot het bijhouden van alle

[6] Het onderzoek is uitgevoerd door een student van de Juridische Hogeschool Avans-Fontys

inbreuken in verband met persoonsgegevens, ofwel het bijhouden van een datalekregister[7]. De AP kan dit register opvragen ter controle. Het doel van deze documentatieverplichting is te stimuleren dat organisaties intern leren van eerdere inbreuken en maatregelen nemen om de kans op nieuwe inbreuken te verminderen. Het managementteam wordt periodiek geïnformeerd over de incidenten die hebben plaatsgevonden.

Wat leren we van de incidenten in 2023?
In het afgelopen jaar zijn er **28** incidenten gemeld. **5** incidenten bleken na onderzoek geen datalek te zijn. Dit leidt tot een **23**-tal datalekken in 2023. Al deze datalekken hebben betrekking op de AVG.

AVG-rubriek	2023	2022	2021
Gebruik onjuist (email)adres	20	20	25
Verloren gegevensdragers	1	1	0
Gemeld incident na onderzoek geen datalek	5	3	2
Applicaties verkeerd gebruikt/ingericht	2	4	2
Overig	0	4	2
Totaal aantal incidenten	**28**	**32**	**31**
Totaal aantal datalekken	**23**	**29**	**29**

Nadere toelichting van de rubrieken:

AVG-rubriek	Uitleg
Gebruik onjuist (email)adres	- Onjuist e-mailadres (9) - Onjuist postadres (11)
Verloren gegevensdragers	Laptop in trein laten liggen (1)
Gemeld incident na onderzoek geen datalek	- Betrof onjuiste instelling in functionaliteit van een van de gebruikte programma's waar geen gebruik van is gemaakt (1) - Datalek ontstond bij externe partij, ten onrechte geregistreerd als datalek(2) - Na onderzoek oordeel geen datalek (2)
Applicaties verkeerd gebruikt/ingericht	Teveel rechten toegekend waardoor iemand te veel kan/ziet (2)
Overig	-

Een incident waarbij persoonsgegevens zijn betrokken wordt altijd gemeld bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor betrokkene. Indien het risico van mogelijke impact op de rechten en vrijheden van de betrokkene(n) hoog wordt ingeschat, zijn wij ook verplicht de betrokkene op de hoogte te stellen van het incident. Het aanmerken van een inbreuk als een 'hoog risico'-inbreuk is een inschatting die telkens opnieuw wordt gemaakt. De uitkomst hiervan is afhankelijk van de specifieke omstandigheden van de inbreuk, met inbegrip van de ernst van het potentiële effect en de waarschijnlijkheid dat dit zich voordoet. In 9 gevallen zijn de betrokkenen benaderd en is uitleg gegeven wat er met hun persoonsgegevens is gebeurd.

[7] Dit volgt uit artikel 33 lid 5 van de AVG.

Cybercriminaliteit in 2023
In 2023 zijn er 12 meldingen van phishing gedaan (e-mails ontvangen door medewerkers met het verzoek om gevoelige informatie te verstrekken middels het doorklikken op een meegestuurde link). Al deze meldingen zijn gedeeld met de RID waarbij in geen van de gevallen een beveiligingsincident is geconstateerd (er is geen kwaadaardige software achtergelaten).

Binnen de RDWI wordt gestimuleerd om alert te zijn op datalekken en phishingacties en indien deze zich voordoen, ze te melden. Meldingsbereidheid is een teken dat medewerkers weten wat een datalek of phishing is, dit herkennen en weten wat ze moeten doen. Door de meldingen wordt inzicht verkregen in waar risico's liggen en kan hierop worden geacteerd.

Aanbeveling:

- Cybercriminaliteit wordt steeds vaker gezien als een groot risico. Elke nieuwe technologietrend creëert nieuwe mogelijkheden voor cybercriminelen. Technologische ontwikkeling zoals bijvoorbeeld kunstmatige intelligentie heeft invloed op het steeds geavanceerder worden van gebruikte middelen. Aandacht hiervoor middels bewustwording van medewerkers blijft daarom een continue proces.

Verantwoording

De AVG dwingt organisaties om veilig en zorgvuldig om te gaan met de persoonsgegevens die worden verwerkt. Als verwerker van persoonsgegevens moet de organisatie kunnen aantonen dat aan alle regels van de AVG (artikel 5) wordt voldaan, de zogenaamde verantwoordingsplicht. Dit vindt plaats in diverse administratieve verplichtingen en documenten waaronder het privacybeleid, de privacyverklaring, het uitvoeren van DPIA's, het bijhouden van een datalekregister en het register van verwerkingen. Genoemde documenten zijn hiervoor reeds uitvoerig behandeld en is uiteengezet hoe deze er aan toe zijn bij de RDWI.

Deel 2 Stand van zaken en bevindingen Wpg

De RDWI heeft - tot halverwege 2023 - voor toezicht, handhaving en opsporing een buitengewoon opsporingsambtenaar (boa) in dienst. De verwerking van persoonsgegevens door een boa in het kader van opsporing valt sinds de inwerkingtreding van de AVG onder de Wet politiegegevens (Wpg). De boa heeft daarmee bij de verwerking van persoonsgegevens te maken met zowel de AVG als de Wpg. Dit betekent dat binnen de bedrijfsvoering rekening moeten worden houden met voorschriften en verplichtingen uit beide wettelijke regimes.

Verplichtingen uit de Wpg

De Wpg bevat strenge eisen over de wijze waarop de verwerking van gegevens mag plaatsvinden. Die moet plaatsvinden in afzonderlijke systemen en door specifiek daartoe aangewezen medewerkers. De reden voor deze strenge eisen ligt in de aard van de bevoegdheden. Bij het uitvoeren van een wettelijke opsporingstaak zijn dit namelijk bevoegdheden uit het Wetboek van Strafvordering en de Wet op de economische delicten. Hiermee kan diep op de privacy van burgers worden ingegrepen en dit vraagt om strenge regels om de privacy van burgers te beschermen.

Voor de verwerking van politiegegevens stelt de Wpg, net als de AVG, een aantal algemene criteria. Dit betreft criteria over noodzakelijkheid, rechtmatigheid, juistheid, proportionaliteit, subsidiariteit en volledigheid. Daarnaast moet de verwerkingsverantwoordelijke een aantal technische en organisatorische maatregelen nemen. Dit betreft onder meer het zorgdragen voor juiste beveiligingsmaatregelen, het uitvoeren van DPIA's, het inrichten van een proces voor het uitoefenen van de rechten van burgers, het melden van datalekken bij de AP en het bijhouden van een datalekregister, het bijhouden van een register van verwerkingen en het hebben van een 'Wpg-proof' ICT-systeem (denk hierbij aan een autorisatiestelsel, termijnbewaking van gegevens, onderscheid kunnen maken tussen soorten politiegegevens (gegevens verdachten, slachtoffers, getuigen of contactpersonen) en de mogelijkheid tot logging).

Auditverplichting, uitkomsten en verbeterplan

De Wpg kent een auditverplichting. De AP houdt toezicht op het daadwerkelijk uitvoeren van deze auditverplichting en monitort de uitkomsten hiervan (er is een toezendplicht van het auditrapport aan de AP). Eind 2022 zijn de bevindingen van de eerste uitgevoerde externe audit opgeleverd. De vele bevindingen hebben geleid tot het opstellen van een verbeterplan met tot doel zorgdragen dat binnen de RDWI conform de Wpg wordt gewerkt.

Het beterplan is, voor zo ver mogelijk, uitgevoerd met het opstellen van beleid, werkinstructies en procedures, maar is uiteindelijk 'gestrand' op de uitdiensttreding van de boa in augustus 2023. Geen boa in dienst betekent dat er geen opsporingsbevoegdheden kunnen worden ingezet en er dientengevolge geen politiegegevens worden verwerkt. Dit betekent ook dat het voor de Wpg vereiste ICT systeem niet in gebruik kan worden genomen. Immers, alleen een voor de organisatie geregistreerde boa[8] mag toegang tot dit systeem.

[8] Dit vindt plaats door het aanvragen van een akte van opsporingsbevoegdheid door de werkgever bij het ministerie van Justitie en Veiligheid.

In overleg met de betrokken auditor is besloten tot het stilleggen van verdere uitvoering van het verbeterplan tot na indiensttreding van een boa. De AP is hierover geïnformeerd (in haar rol van toezichthouder op de Wpg) en heeft ingestemd met het tijdelijk pauzeren van de verdere implementatie van de Wpg. Als gevolg hiervan is ook het FG-toezicht op de Wpg op dit moment niet verder uitgewerkt. Zodra de organisatie een boa in dienst neemt, herleeft de auditverplichting en wordt het FG-toezicht herpakt.

Opvolging aanbevelingen uit het rapport 2022

In onderstaand overzicht zijn de aanbevelingen uit het rapport 'Stand van zaken gegevensbescherming 2022' opgenomen. In de laatste kolom is de status van opvolging eind 2023 weergegeven. De niet opgevolgde dan wel nog niet afgehandelde aanbevelingen komen terug in onderhavige rapportage.

Thema	*Aanbeveling*	*Update eind 2023*
Beleid	Zorg dat kennis over het eigen privacybeleid meegenomen wordt in de komende bewustwordingsinstrumenten.	Gereed.
Beleid	Het bestaande privacybeleid moet worden aangevuld met de Wet politiegegevens.	Gereed.
Processen	Voer de jaarlijkse controle op het register van verwerkingen.	Nog niet afgerond.
Processen	Onderzoek het stopzetten van de implementatie de GRC-tool.	Herstart in projectvorm regionaal.
Processen	Zorg dat DPIA's worden uitgevoerd.	Uitvoering van DPIA's blijft een continue aandachtspunt.
Organisatorische inbedding	Leg de taken en verantwoordelijkheden van de rollen en functies in het IV&P-team vast in rol-/functiebeschrijvingen.	Nog niet afgerond.
Organisatorische inbedding	Implementeer een nieuw bewustwordingsprogramma.	Gereed.
Organisatorische inbedding	Geef privacy en informatiebeveiliging een vaste plek in het inkoopproces van de organisatie.	Gereed. Kennis hierover en wetenschap wat dit met zich meebrengt voor de betrokken medewerkers moet alsnog worden verdiept.
Rechten van betrokkenen	Implementeer anonimiseringssoftware.	Gereed.
Rechten van betrokkenen	Train medewerkers actief op de wijze waarop wordt gerapporteerd met het oog op dataminimalisatie	Niet gestart. Geagendeerd voor 2024.
Samenwerking	Besteed aandacht aan het onderwerp 'verwerkersovereenkomsten'.	Lopend. Kennis hierover en wetenschap wat dit met zich meebrengt voor de betrokken medewerkers moet alsnog worden verdiept.
Samenwerking	Onderzoek het kader waarbinnen de RDWI gegevens met derden mag delen.	Onderzoek is afgerond maar heeft niet geleid tot een bruikbaar kader.
Beveiliging	Voortdurende aandacht voor de onderwerpen 'beveiligd mailen' en 'phishingmails'.	Gereed.
Beveiliging	Stel een crisisplan	Lopend.

	informatiebeveiligingsincidenten op.	
Verantwoording	Vul het borgingsproduct van de VNG in voor komend jaar	Niet gestart. Geagendeerd voor 2024.