Kwartaalrapportage
Datalek en Volwassenheidsniveau
provincie Zuid-Holland
1 oktober 2024

Inhoudsopgave

Algemene inleiding

Inleiding

Voor u ligt de tweede voortgangsrapportage voor het datalek in iDMS en de privacy-volwassenheid binnen de provincie Zuid-Holland (PZH). Deze volgt op de eerste rapportage die wij u op 30 april jongsleden stuurden. U heeft daar per brief op 18 juni op gereageerd. De provincie spreekt hierbij haar dank uit voor de ontvangen constructieve feedback. We gaan in hoofdstuk 3, 'reflectie op vragen Autoriteit Persoonsgegevens (AP)', concreet in op uw gegeven feedback en/of gestelde vragen.

Achtergrond

Direct na de melding van het datalek in september 2023 hanteerden we een iteratieve en 'agile' aanpak om inzicht te krijgen in de aard en omvang van het datalek. Aanvullend onderzochten we in de structuur van de applicatie waar zich mogelijk persoonsgegevens bevonden. Het onderzoek leverde onvoldoende concrete resultaten op. Dit kwam door de omvang van de dataset, de beperkingen van de zoekfunctie in de applicatie en de data- en logging-kwaliteit. Waar mogelijk namen wij echter beheersmaatregelen, zoals het aanscherpen van toegangsrechten. Gegeven de teleurstellende resultaten van het oorspronkelijke onderzoek pasten we onze aanpak aan. Enerzijds besloten we tot de inzet van moderne analysehulpmiddelen. Anderzijds betrokken we de data- en proceseigenaren meer bij de analyse. Daarmee kregen de analyse en het dichten van het datalek een noodzakelijke, nieuwe impuls. De aangescherpte aanpak staat in het plan van aanpak.

In de afgelopen 2 jaar investeerde de provincie Zuid-Holland aanzienlijk in het versterken van de privacy-organisatie en privacy-uitvoering. Dit omdat in de periode 2018-2022 onvoldoende groei in privacy-volwassenheid was bereikt. In 2022 voerde de Eenheid Audit en Advies van de provincie een onderzoek naar de privacy-volwassenheid uit. Daarbij hanteerde zij de volwassenheidsmatrix van het CIP. Hieruit bleek dat PZH een volwassenheidsniveau 1 scoorde (waarbij enkele onderdelen iets hoger scoorden), op een schaal van 1 tot 5 (waarbij 1 het laagste niveau is). De directie sprak destijds uit te streven naar een volwassenheidsniveau van 3, uiterlijk op 31-12-2025.

Als gevolg van de achterblijvende volwassenheid op het gebied van privacy, het datalek en de wijze waarop de organisatie om gaat met de (adviezen van de) Functionaris voor Gegevensbescherming, stelde de AP de provincie onder verscherpt toezicht. We startten een programma dat uit 2 onderdelen bestaat: de afhandeling van het datalek (programmalijn 1) en het verhogen van het volwassenheidsniveau van de organisatie (programmalijn 2). Deze programmalijnen vormen tevens de basis voor deze rapportage.

De toewijding aan het verbeteren van onze privacy-volwassenheid en het oplossen van het datalek, weerspiegelt ons streven naar een organisatie die haar verantwoordelijkheden op het gebied van privacy serieus neemt en zich inzet voor het opbouwen van vertrouwen bij alle belanghebbenden.

Uitgangspunten bij onze aanpak

Beheersing volgens gestructureerd risicomanagement: hoog risico eerst

We zetten mensen en middelen in op basis van risicomanagement: daar waar ze de risico's bij het beschermen van persoonsgegevens het meest verminderen. Risicomanagement stelt de provincie Zuid-Holland in staat gestructureerd en verantwoord om te gaan met dreigingen, kansen en risico's voor het oplossen van het datalek, en te groeien naar het volwassenheidsniveau 3.

Implementatie privacy-managementsysteem

Privacy is een continu en cyclisch proces op basis van plan-do-check-act. Daarbij is het noodzakelijk om actief vanuit de opgave en vanuit het management te sturen. Een privacy-managementsysteem stelt de organisatie in staat om steeds, per kwartaal, te prioriteren in beleidsvorming en privacy-uitvoering (DPIA's, verwerkingsregister).

Privacy is strategische randvoorwaarde

Beschermen van persoonsgegevens, het realiseren van maatschappelijke opgaven, en de kwaliteit van de dienstverlening moeten hand in hand gaan. Het vertrouwen van inwoners en bedrijven is hier sterk van afhankelijk. De wet- en regelgeving rondom privacy en digitale thema's nemen toe en worden steeds complexer. In de visievorming Informatiebeheer beschrijven we informatierisico's op het gebied van onder andere veiligheid en privacy. Het op orde brengen van het informatiebeheer en het vergroten van de bewustwording van de PZH-medewerkers van de eigen rol daarin, verhogen het niveau van volwassenheid op het gebied van privacy en dataveiligheid.

De winkel blijft open

De operatie mag niet onderbroken worden door maatregelen die we in iDMS uitvoeren. Zonder extra capaciteit, middelen en inspanning is het echter niet mogelijk om de doelstellingen in dit plan te behalen. We accepteren dat medewerkers in sommige gevallen (al dan niet tijdelijk) niet over alle benodigde documenten en rechten beschikken. Dat heeft gevolgen voor onze dienstverlening. We communiceren hierover zo duidelijk mogelijk en benoemen dat we keuzes maken op het spectrum; dichten van het datalek versus continuïteit van onze dienstverlening. Medewerkers in heel de organisatie merken dat we hier actief mee bezig zijn.

Leeswijzer

Voor de leesbaarheid van deze rapportage gaan wij apart in op de 2 onderdelen van onze aanpak. Dit zijn:

1. Zo snel als mogelijk dichten van het datalek;
2. Het verhogen van het volwassenheidsniveau van de organisatie rondom dataveiligheid en privacy naar niveau 3.

Onderdeel 1 behandelen we volgens onderstaande structuur:

- **Inleiding:** een beschrijving van zowel de context waarin dit rapport tot stand komt, als van het algemene doel;
- **Doelstellingen:** een overzicht van onze doelstellingen ten aanzien van dit onderdeel.
- **Stand van zaken:** de afzonderlijke acties die voortkomen uit de doelstelling. Beschrijving per actie, de voortgang, eventuele situatiebeschrijving, en evaluatie;
- **Informeren betrokkenen:** beschrijving hoe we omgegaan zijn en omgaan met het informeren van betrokkenen;
- **Nawoord:** een reflectie op het betreffende onderdeel;
- **Bijlagen:** bijlagen ter aanvulling en/of verduidelijking van bovenstaande.

Onderdeel 2 behandelen we volgens onderstaande structuur:

- **Inleiding:** een beschrijving van zowel de context waarin dit rapport tot stand komt, als van het algemene doel;
- **Doelstellingen:** een overzicht van onze doelstellingen ten aanzien van dit onderdeel.
- **Stand van zaken:** de afzonderlijke acties die voortkomen uit de doelstelling. Beschrijving per actie, de voortgang, eventuele situatiebeschrijving, en evaluatie;
- **FG-adviezen:** hoe we hiermee omgaan, wat de status van de adviezen is, en wat de situatie betekent voor de FG zelf;
- **Nawoord:** een reflectie op het betreffende onderdeel;
- **Bijlagen:** eventuele bijlagen ter aanvulling en/of verduidelijking van bovenstaande.

We sluiten de rapportage af met een totaaloverzicht van uw genoemde zorgen, voorzien van onze reactie (‘Reflectie op vragen AP’), en de reactie op onze rapportage van onze Functionaris voor Gegevensbescherming (FG).

1. Spoor 1: het dichten van het datalek

1.1 Inleiding

Voor het dichten van het datalek in iDMS (ons documentbeheersysteem) probeerden we eerder alle documenten op privacygevoelige informatie te analyseren. Dat bleek niet praktisch. Daarom voerden we een nieuwe, gerichtere aanpak in. Hierbij verdeelden we de documenten in verschillende categorieën. Elke categorie heeft specifieke eigenschappen, met mogelijkheden en beperkingen voor het dichten van het datalek. We onderscheiden de volgende categorieën:

Centraal toegankelijke documenten:

- Categorie 1: 4,3 miljoen archiefdocumenten
  Deze documenten zijn in het kader van de archiefwet op een specifieke locatie in iDMS gearchiveerd.

- Categorie 2: 7 miljoen ‘oude documenten’
  Deze documenten zijn vanaf 1 augustus 2021 niet meer gewijzigd.

- Categorie 3: 19 miljoen ‘actuele documenten’
  Deze documenten zijn vanaf 1 augustus 2021 nog wel gewijzigd en actueel in gebruik.

Niet-centraal toegankelijke documenten:

- Categorie 4: 20 miljoen ‘documenten in persoonlijke mappen’.
  Deze documenten staan in persoonlijke mappen. Dat betekent dat deze mappen alleen voor de betreffende ‘mapeigenaar’ zichtbaar zijn. Tenzij de betreffende medewerker toegang tot de persoonlijke map heeft verleend aan anderen. Autorisaties op deze mappen en documenten kunnen we alleen met een zorgvuldige, geautomatiseerde analyse interpreteren, en zo mogelijk herzien.

Aan de hand van deze categorieën hebben we een gerichtere aanpak opgesteld. We starten waar het risico het hoogst is. Daarnaast kunnen we beter de balans houden tussen aan de ene kant het zo snel mogelijk dichten van het datalek, en aan de andere kant het beheersbaar houden van de gevolgen van onze aanpak op het functioneren van de organisatie.

1.2 Doelstelling

Op spoor 1 – het dichten van het datalek – zijn onze doelstellingen onveranderd:

1. Het uiterlijk op 31-12-2024 dichten van het datalek in het centraal toegankelijke deel van het iDMS.
2. Het collectief – en waar mogelijk persoonlijk – informeren van betrokkenen.

1.3 Aanpak datalek: stand van zaken en geplande acties

We hebben een belangrijke stap gezet in het dichten van het datalek. Naast het intrekken van algemene toegangsrechten, implementeerden we een analysetool. Deze stelt ons in staat om

het iDMS te doorzoeken op documenten met privacygevoelige informatie. Met deze analyse kunnen we bepalen wie toegang mag hebben tot welke documenten. Zo kunnen we tijdelijk een extra laag toegangsrechten toevoegen aan documenten met privacygevoelige gegevens.

1.3.1 IAM

Parallel aan deze aanpak, voeren we met Identity Access Management (IAM) een duurzame oplossing door. Dit is een lopend project binnen de provincie die we met urgentie naar voren hebben gehaald. Het heeft als doel een geautomatiseerd systeem op te zetten voor het toekennen en intrekken van rechten op basis van rollen.

Hiervoor is het nodig dat het iDMS ingericht wordt naar de onze nieuwe organisatiestructuur 'OGO' (opgavegericht organiseren). Deze aanpassing vraagt om herziening van bestaande structuren. Dit is ingewikkeld en tijdrovend. Bovendien hebben we hiervoor de expertise en samenwerking van meerdere van onze disciplines nodig, waaronder Informatiebeheer, HR, ambtelijk opdrachtgevers en Technisch- en Functioneel beheer. We zetten alles op alles om dit zo snel als mogelijk ingericht te hebben. Dit zal alleen nog niet in 2024 ingevoerd zijn.

1.3.2 Informatietransitie

Het programma Informatietransitie speelt ook een belangrijke rol. Dit meerjarige programma startte in januari 2023. Het heeft als doel het informatiebeheer van de provincie Zuid-Holland te verbeteren en is essentieel bij het dichten van het datalek in iDMS. Het programma verhoogt de betrouwbaarheid van onze systemen en zorgt dat we informatie op een veilige en efficiënte manier kunnen beheren.

Omdat we het dichten van datalek als grote prioriteit zien, pakten we de analyse en verbetering van de toegankelijkheid van iDMS eerder dan gepland op. Om diezelfde reden prioriteerden we ook de aanschaf en invoering van een analysetool.

1.3.3 Aanpak categorie 1 en 2: 'archiefdocumenten' en 'oude documenten'

Van deze categorieën ontnamen we de concern-brede toegangsrechten. Daardoor zijn deze items (samen 11,3 miljoen) niet meer toegankelijk voor alle PZH-medewerkers.

In individuele gevallen herstelden we op verzoek - en na autorisatie door de verantwoordelijke manager - de toegang tot benodigde documenten: uitsluitend wanneer de betrokken medewerker de documenten nodig heeft voor het uitvoeren van diens werkzaamheden.

Met het wegnemen van de brede toegangsrechten is het risico op onrechtmatige raadpleging van deze documenten aanzienlijk verkleind. Bestaande specifieke rechten van bestaande groepen medewerkers zijn nog wel actief. Daarom starten we met het geautomatiseerd analyseren van deze documenten, zodra de analyse van de documenten in categorie 3 en 4 is afgerond.

1.3.4 Aanpak categorie 3: 'actuele documenten'

Het intrekken van alle concern-brede toegangsrechten voor deze documenten zorgt voor grote en moeilijk voorspelbare risico's voor de voortzetting van onze primaire processen. Daarom brengen we eerst geautomatiseerd de privacy-gevoeligheid en de toegekende autorisaties van deze documenten geanalyseerd en gedetailleerd in kaart.

Als eerste stap voerden we in september een Proof of Concept (PoC) uit op 2 miljoen van de 19 miljoen documenten. De PoC kon pas starten na implementatie van de analysetool. We

hebben hiertoe een zorgvuldig traject doorlopen waar een aanbesteding en het volgen van een DPIA onderdeel van waren. De resultaten van deze PoC helpen ons niet alleen om de toegangsrechten voor deze documenten aan te passen, maar geven ook inzicht in wat we kunnen verwachten voor de resterende 17 miljoen documenten. Waar nodig zullen we aanvullende acties uitwerken en invoeren. De PoC is daarnaast bedoeld om ervaring op te doen en verbeteringen door te voeren.

Op basis van de PoC-resultaten analyseren we de overige 17 miljoen documenten in batches van ongeveer 4 miljoen items, met een doorlooptijd van 3 tot 4 weken per batch.

De analyseresultaten van de PoC en de analyse van de vervolgbatches geven verder inzicht in de samenhang en classificatie van documenten. Op basis van deze resultaten en classificatie nemen we verdere maatregelen om de risico's te verminderen. In dit kader voegen we een aanvullende autorisatieschil aan het huidige iDMS toe. Daarmee kunnen we rechten toekennen op specifieke documenten. Dit gaat bijvoorbeeld om maatregelen op het gebied van: het verwijderen van toegangsrechten, het beperken van de toegankelijkheid, of het verwijderen van privacygevoelige informatie uit documenten die bewaard moeten blijven (vanwege de Archiefwet en Woo).

Het herstellen van de toegang tot bepaalde documenten voor individuele medewerkers of groepen medewerkers, vraagt veel inzet van ons functioneel beheer. We werken daarom aan een 'menukaart' die bestaat uit specifieke autorisatiegroepen. Een groep heeft toegang tot bepaalde documenten, dossiers en mappen. Met het autoriseren voegen we een medewerker toe aan 1 of meer groepen. Daarmee wordt het niet alleen overzichtelijker aan wie we welke toegangsrechten toekennen, maar kunnen we bij doorstroom de toegang ook beter beheren. Begin kwartaal 4 van 2024 introduceren we de menukaart.

We verwachten voor deze categorie het datalek van 19 miljoen documenten eind 2024 volledig te dichten.

1.3.5 Aanpak categorie 4: 'documenten in persoonlijke mappen'

Voor deze categorie documenten analyseren we geautomatiseerd de privacy-gevoeligheid van de inhoud en de verleende autorisaties. Uit de analyse volgen aanbevelingen voor het herzien van autorisaties. Deze categorie vraagt ook om maatwerk in het aanpassen van de autorisaties. Dit omdat de autorisaties persoonlijk verleend zijn (en geen concern-breed karakter hebben).

Na de 19 miljoen documenten uit categorie 3, analyseren we deze 20 miljoen documenten. Daarna werken we de aanpak voor deze categorie verder uit. In een volgende rapportage informeren we u hierover verder.

1.3.6 Overzicht in tabel

Het aantal en type documenten (categorie), de aanpak en de status van het dichten van het datalek zijn in onderstaand overzicht samengevat:

	Centraal deel iDMS		Persoonlijke werkmappen
Totaal iDMS	50,3 miljoen documenten		
Totaal aantal	30,3 miljoen documenten		20 miljoen documenten
Aantal en type documenten	11,3 miljoen 'archief- en oude documenten'	19 miljoen 'actuele documenten'	20 miljoen 'documenten in persoonlijke mappen'
Aanpak	Concern-breed, geautomatiseerd en later geavanceerde analyse	Concern-breed, geautomatiseerd na geavanceerde analyse door analysetool	Specifiek, geautomatiseerd na geavanceerde analyse door analysetool en mogelijk na overleg met eigenaar
Status	Afgerond. Centrale toegangsrechten ontnomen. Op een later moment analyse in batches van 4 miljoen documenten, begin 2025.	PoC met 2 miljoen documenten eind september gereed. Daarna analyse in batches van 4 miljoen documenten tot eind 2024. Op basis van analyse passen we toegang en rechten aan.	Specifieke aanpak voor deze categorie documenten ontwikkelen we in kwartaal 4 van 2024. Daarna analyse in batches van 4 miljoen documenten begin 2025. Op basis van analyse passen we toegang en rechten aan.

1.4 Informeren betrokkenen

De provincie onderschrijft het belang van het informeren van betrokkenen van het datalek. Dit stelt hen in staat stelt alert te zijn op de mogelijke gevolgen, en om er zich daar waar mogelijk tegen te beschermen. Het liefst zouden we álle betrokkenen individueel informeren. Dit is helaas niet haalbaar, vanwege de technische inrichting van iDMS en de omvang van 50,3 miljoen documenten. De huidige manier van loggen en de inrichting van de groepsaccounts maken het onmogelijk te achterhalen of de documenten onrechtmatig in te zien zijn/waren, of ingezien zijn.

Wat hebben we wél gedaan?

De stuurgroep keurde op advies van het kernteam de procedure voor het informeren van betrokkenen goed. Het advies is uitgebracht na afstemming met de FG en is besproken met de gedeputeerde.

Stap 1. Het datalek heeft zowel betrekking op persoonsgegevens van medewerkers, als op die van externe partijen. Op 11 april 2024 plaatsten we een bericht op ons intranet (intern) en op zuid-holland.nl (extern) om medewerkers en externe betrokkenen te informeren.

Stap 2: Vervolgens informeerden we op 11 juli 2024 alle interne en externe medewerkers nader met een e-mail en (opnieuw) een bericht op intranet.

Overige betrokkenen hebben we helaas niet in beeld. Daardoor kunnen we ze niet afzonderlijk informeren. Het best beschikbare alternatief was het collectief informeren via onze website.

De e-mail, intranetberichten, en het bericht op zuid-holland.nl vindt u in de bijlagen.

1.5 Nawoord

We hebben sinds de vorige rapportage flinke stappen gezet in het dichten van het datalek in iDMS. We verfijnden onze aanpak door documenten in het iDMS op te splitsen in specifieke categorieën. Daarnaast namen we een geavanceerde analysetool in gebruik, waarmee we elke 4 weken ongeveer 4 miljoen documenten kunnen scannen op privacy-gevoelige informatie. Op basis van deze analyses kunnen we gerichte maatregelen nemen om het datalek voor elke batch documenten aan te pakken.

Voordat we de tool in gebruik namen, doorliepen we eerst een DPIA-traject. Vanwege het belang van de kwestie was dit traject intensief en zorgde het voor een nauwe samenwerking van alle betrokken partijen. Dit verbeterde zowel de communicatie als het onderlinge begrip tussen het kernteam, de FG, de Eenheid Privacy, en het team Informatieveiligheid.

1.6 Bijlagen

Bijlage 1: Nieuwsbericht Intranet op 11 april 2024

Bijlage 2: Berichtgeving zuid-holland.nl op 11 april 2024

Bijlage 3: E-mail concerndirecteur aan medewerkers op 11 juli 2024

Bijlage 4: Nieuwsbericht Intranet op 11 juli 2024

2. Spoor 2: Het volwassenheidsniveau verhogen

2.1 Inleiding

Het naleven van wet- en regelgeving op het gebied van privacy betekent niet alleen het voldoen aan formele eisen, maar ook het invoeren van passende maatregelen binnen de organisatorische en technologische infrastructuur. Met de 'privacy-volwassenheids-benadering' kunnen we op een gestructureerde manier deze mate van volwassenheid op het gebied van privacy en gegevensbescherming beoordelen in onze organisatie.

2.2 Doelstellingen en uitgangspunten

We stelden onze doelstelling op dit onderdeel bij. Het oorspronkelijke doel was om voor het eind van 2025 het volwassenheidsniveau 3 te bereiken. Dit is bij nader inzien niet realistisch en haalbaar. Daarom verlegden we deze deadline naar 31-12-2026. De overwegingen die hierbij een rol speelden, zijn:

- Onze organisatie nam lange tijd privacy niet echt serieus en investeerde hier onvoldoende in. Het is daarom niet mogelijk om een voldoende niveau van bewustzijn op het vlak van privacy in 15 maanden te realiseren.
- Uit eerdere wervingstrajecten bleek dat het lastig is om op korte termijn voldoende ervaren privacy officers te werven om de geïdentificeerde werkzaamheden uit te voeren.
- We startten op 3 september met de personeelsuitbreiding van de Eenheid Privacy. Dit heeft een zekere doorlooptijd nodig (aanbestedingsproces in geval van externe inhuur en opzegtermijn bij werving van nieuwe medewerkers). Dit zorgt ervoor dat de restant doorlooptijd steeds knellender wordt.

We erkennen dat we te laat zijn gestart met de werkzaamheden die nodig zijn om volwassenheidsniveau 3 te behalen. De voortgang liep hiermee vertraging op. Oorzaken hiervoor zijn onder meer een gebrek aan ervaring met dit soort grote privacy-projecten, beperkte capaciteit en ook een beperkte focus op dit onderdeel (door prioriteit te geven aan het oplossen van het datalek). Hier leren we van en verbeteren we in de stappen die we nog te zetten hebben.

2.3 Stand van zaken

2.3.1 Vastgesteld privacy-beleid en governance

Het college van Gedeputeerde Staten stelde op 25 juni 2024 ons privacy-beleid vast. Sindsdien liggen de rollen en verantwoordelijkheden met betrekking tot gegevensbescherming expliciet in ons beleid vast. De governance blijft ongewijzigd en ziet er als volgt uit:

- Het college van Gedeputeerde Staten (GS) is bestuurlijk eindverantwoordelijk voor het naleven van de privacywet- en regelgeving en voor de kaders van het verantwoord omgaan met persoonsgegevens. Als verantwoordelijk gezag stellen GS het privacy-beleid vast. Over de uitvoering ervan leggen GS verantwoording af aan Provinciale Staten (PS).

- Het Directieteam (DT) bestaat uit de provinciesecretaris en de concerndirecteur. Het DT is ambtelijk eindverantwoordelijk voor de bedrijfsvoering van de provincie Zuid-Holland. Daarmee is zij dat ook voor de uitvoering van - en sturing op - de beleidskaders voor privacy. Op basis van het privacy-beleid wijst het DT taken,

verantwoordelijkheden en bevoegdheden toe. Het DT heeft op basis van zijn actieve informatieplicht de verantwoordelijkheid om GS te informeren wanneer er sprake is van kritieke risico's, of wanneer het privacy-beleid niet wordt nageleefd (non-compliancy).

- De dagelijkse verantwoordelijkheid voor het voldoen aan de uitgangspunten van de privacy-wet- en -regelgeving binnen de provincie, ligt bij de Ambtelijk Opdrachtgevers (AOG's) en de p-managers. De AOG's en p-managers zorgen ervoor dat men binnen de opgaven volgens het privacy-beleid werkt. De AOG geeft de Ambtelijk Opdrachtnemer (AON) aanwijzingen hoe deze de randvoorwaarden het beste kan invullen binnen diens opdracht. De AOG's en p-managers zijn binnen hun werkzaamheden verantwoordelijk om de juiste disciplines, op het juiste moment, te betrekken. Voor privacy is dat de Eenheid Privacy.

2.3.2 Programma Privacy

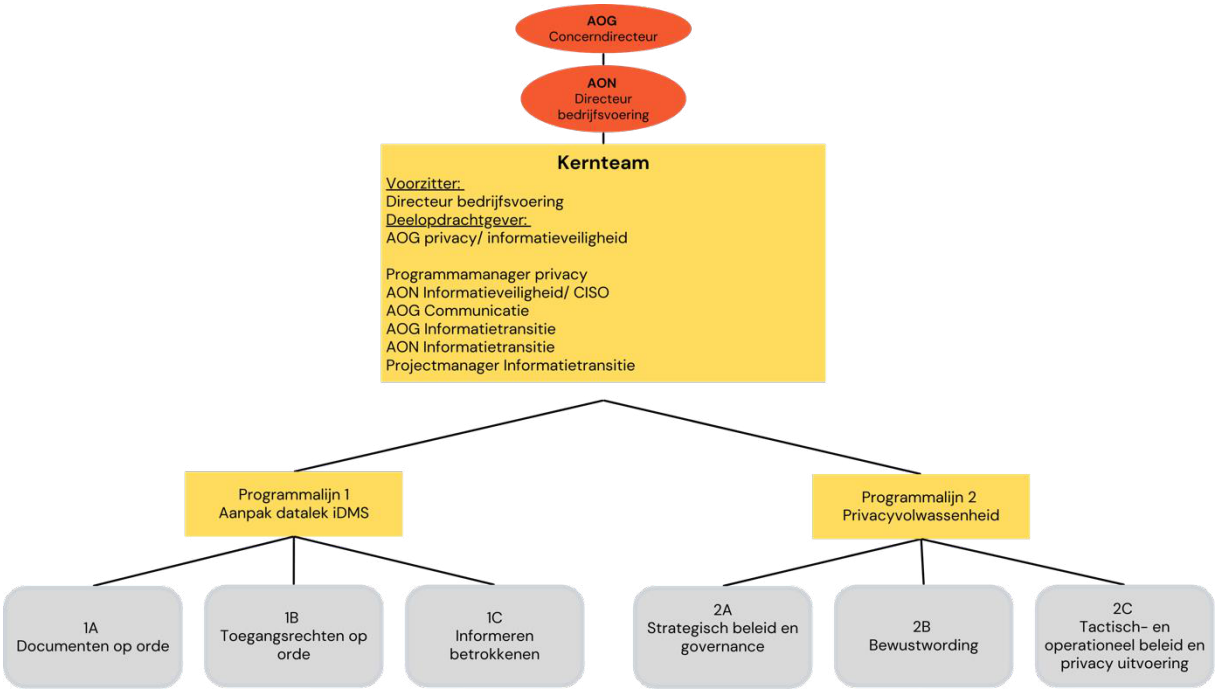
Voor het dichten van het datalek en de gewenste groei van de privacy-volwassenheid is communicatie en betrokkenheid van medewerkers en management noodzakelijk. De concerndirecteur is ambtelijk opdrachtgever van dit programma. Daarmee benadrukken we de urgentie van dit programma en borgen we een sterke aansturing en ondersteuning. Met deze keuze maken we ook in de organisatie duidelijk dat we de doelstellingen van dit programma tot hoogste prioriteit hebben gemaakt. De concerndirecteur is voorzitter van de stuurgroep die verder bestaat uit:

- Directeur bedrijfsvoering (ambtelijk opdrachtnemer)
- Ambtelijk opdrachtgever Privacy en Informatieveiligheid
- Programmamanager Privacy
- Ambtelijk opdrachtgever Communicatie
- Functionaris voor Gegevensbescherming

De stuurgroep bespreekt tweewekelijks de aanpak, resultaten en voortgang van het programma. Tijdens deze bijeenkomsten worden inhoudelijke of strategische keuzes toegelicht en afgestemd. Waar dat aan de orde is, neemt de stuurgroep besluiten. Er is ook periodiek afstemming met de verantwoordelijke Gedeputeerde. Wanneer keuzes verstrekkende gevolgen hebben, vindt hier overleg en besluitvorming plaats.

Naast de stuurgroep is er een kernteam dat de dagelijkse aansturing van het programma afstemt en aanstuurt. Het programma is onder regie van de Eenheid Privacy, maar inhoudelijke en implementatiekeuzes gaan langs het kernteam. Zo besluit zij over de aanpak, (deel)producten en beoogd resultaat (uiteraard binnen de kaders die zijn meegegeven vanuit de stuurgroep). Het kernteam zorgt voor draagvlak binnen PZH en maakt waar nodig keuzes in de gebruikelijke besluitvormingscyclus.

Het kernteam is volgens onderstaand schema vormgegeven:



De Functionaris voor Gegevensbescherming (FG) heeft tweewekelijks overleg met de concerndirecteur en 6-wekelijks met de portefeuillehouder. De portefeuillehouder is lid van het college van Gedeputeerde Staten (provinciebestuur) en heeft een wekelijks overleg met zijn teamstaf. Daar staat het onderwerp privacy regelmatig op de agenda. De concerndirecteur sluit ook regelmatig bij deze overleggen aan.

Gedeputeerde Staten en Provinciale Staten worden in overeenstemming met de rapportagecadans op de hoogte gehouden van de voortgang.

2.3.3 Wat hebben we de afgelopen periode gedaan?

In de vorige rapportage stelden we onze doelstellingen voor 2024 vast. Inmiddels concludeerden we dat enkele van deze doelstellingen te ambitieus waren. Ze blijven van kracht, maar we hebben meer tijd nodig om ze waar te maken. Hieronder vindt u een overzicht van de doelen die we reeds hebben bereikt. De doelen waaraan we momenteel werken of die we de komende 3 maanden oppakken, bespreken we in paragraaf 2.3.4.

- **Beleid vastgesteld**
  Het college van Gedeputeerde Staten (GS) stelde het privacy-beleid van de provincie Zuid-Holland vast op 25 juni 2024.

  De verantwoordelijkheid voor de naleving van het centrale privacy-beleid is verankerd binnen de opdrachten en geldt voor alle functionarissen die werkzaam zijn bij/voor de provincie. De Eenheid Privacy zorgt ervoor dat de uitvoering van dit beleid consistent is in alle opdrachten. De FG houdt toezicht op de naleving. De Eenheid Privacy speelt een sleutelrol in het monitoren en rapporteren van de uitvoering van het beleid en heeft daarmee een signalerende en adviserende functie. Het privacy-beleid vindt u in de bijlagen.

- **De Eenheid Privacy kreeg een stevige verankering in de organisatie**
  We werkten aan de inbedding van de Eenheid Privacy binnen onze nieuwe organisatiestructuur: OGO (Opgavegericht Organiseren). Sinds 1 september jongstleden is het opdrachtenregister klaar. In het opdrachtregister is al het werk van de provincie opgenomen en beschreven in opdrachten. De opdracht 'Gegevensbescherming' krijgt daarin ook een plek. Dit zorgt ervoor dat verantwoordelijkheden en rapportagelijnen vastliggen. Met een gekaderde opdracht in de OGO-structuur is er vanaf komend jaar ook structureel budget voor het beschermen van persoonsgegevens.

- **Inrichting programma privacy**

  Voor het dichten van het datalek en het verhogen van het volwassenheidsniveau van de organisatie zijn aanvullende middelen nodig, zowel materieel budget als arbeidscapaciteit. Om onze inspanningen te versterken en te versnellen, startten we met het werven van extra capaciteit van onder meer Privacy Officers. We voegen hen toe aan onze Eenheid Privacy.

- **Bewustwordingsacties**
  De Eenheid Privacy startte met een brede campagne die zich richt op alle medewerkers, van nieuwe collega's tot leidinggevenden. Dit met als doel de bewustwording rondom privacy en gegevensbescherming binnen de organisatie te vergroten. Deze campagne omvat verschillende initiatieven en communicatiekanalen waarmee we het belang van de AVG - en de juiste omgang met persoonsgegevens - onder de aandacht brengen:
    - Op ons intranet, het Binnenplein, bestaat een speciale groep 'Privacy-AVG' waar de Eenheid Privacy regelmatig publicaties plaatst;
    - Tijdens het onboarding-programma voor nieuwe medewerkers besteden we aandacht aan privacy en gegevensbescherming;
    - De Eenheid Privacy organiseert regelmatig voorlichtingssessies voor diverse teams binnen de organisatie. Daarnaast is ze sinds juni met haar trainingen onderdeel van de PZH-akademie (een aanbod van interne opleidingen).
    - Alle leidinggevenden krijgen een verplichte AVG-training;
    - Er is een Q&A-sectie over datalekken beschikbaar op ons intranet;
    - Op 12 november organiseren we een 'Privacy Show' met een externe spreker.

- **Nieuwe DPIA-systematiek**
  We ontwierpen een nieuw DPIA-proces. Deze bestaat uit een pre-DPIA-model en een DPIA-model. Ook voegden we een ethisch kader aan de (pre-)DPIA-systematiek toe. De modellen en tooling pasten we hierop aan.

- **Nieuw proces rechten betrokkenen**
  In het kader van het correct beleggen van verantwoordelijkheden binnen de organisatie, richtten we het proces rond verzoeken op grond van de AVG opnieuw in. Het proces is op meerdere niveaus gestroomlijnd en efficiënter ingericht. Hierbij was specifieke aandacht voor de coördinatie van het verzoek en een betere monitoring van de voortgang. Dit proces dient nog te worden vastgesteld.

2.3.4 Wat gaan we de komende 3 maanden doen?

Hoewel we flinke vooruitgang boekten, erkennen we dat er nog ruimte is voor verbetering. We blijven ons inzetten om onze doelen te bereiken. De afgelopen periode zetten we veel van onze capaciteit (naast het reguliere werk) in voor het dichten van het datalek in iDMS (lijn 1). Dit had invloed op de snelheid waarmee we de andere onderdelen van ons programma konden uitvoeren. Wij hebben de volgende werkzaamheden gepland voor het vierde kwartaal:

- **Besluitvorming**
  We leggen in processen vast dat bij elke nieuwe projectinitiatie, systeemimplementatie, of wijziging in bedrijfsprocessen, een pre-DPIA (of waar nodig een DPIA) wordt uitgevoerd. Voor alle besluitvormingsdocumenten wordt een standaard checklist een vast onderdeel. We ontwikkelen daarnaast richtlijnen die aangeven wanneer en hoe de Eenheid Privacy en/of de FG betrokken moet(en) worden in het besluitvormingsproces. Daarmee borgen we dat alle belangrijke beslissingen – die invloed hebben op gegevensbescherming – worden beoordeeld, en van een advies worden voorzien. Deze adviezen worden onderdeel van de besluitvorming. Bij het documenteren van de genomen besluiten moet worden opgenomen of en hoe de adviezen worden opgevolgd.

  Bij het afwijken van de gegeven adviezen speelt een afwijkingsbesluit een belangrijke rol. Meer informatie daarover staat in ‘De omgang met FG-adviezen' in hoofdstuk 2.4.

- **E-learning**
  Er komt een e-learning-module die voor alle medewerkers verplicht is. De Eenheid Privacy en het team Informatieveiligheid sluiten zich aan bij het bredere Learning Management System (LMS) van de organisatie. De verwachting is dat het LMS in kwartaal 4 van 2024 operationeel is. Het marktonderzoek naar mogelijke aanbieders loopt, en we streven naar de invoering van een eigen e-learning in kwartaal 1 van 2025.

- **FAQ website**
  We ontwikkelen een veel-gestelde-vragen-sectie (FAQ) voor onze website. Deze FAQ zal gericht zijn op het beantwoorden van veelvoorkomende vragen van betrokkenen: bijvoorbeeld over hoe hun persoonsgegevens worden verwerkt, welke rechten zij hebben, en hoe zij deze rechten kunnen uitoefenen.

- **Opdrachtkaders**
  Binnen de provincie Zuid-Holland (PZH) werken we opgavegericht. Elke opgave wordt opgedeeld in specifieke opdrachten. We richten onze uitvoeringskaders in op het niveau van de opdrachten. Zo kunnen we de gegevensbescherming effectief beheersen en de verantwoordelijkheden volgens het privacy-beleid op het juiste niveau beleggen.

  Elke opdracht wordt gestart met een opdrachtformulier. Daarin worden privacy en gegevensbescherming expliciet opgenomen. De Eenheid Privacy ging in kwartaal 3 ook aan de slag met een leidraad voor ambtelijk opdrachtgevers, waarin zij kaders stelt. Op deze manier waarborgen we 'privacy by design' en krijgen we beter inzicht in de gegevensverwerkingen die binnen elke opdracht plaatsvinden. We verwachten de afronding hiervan in kwartaal 4 van 2024.

- **Datalekken melden**

De Eenheid Privacy en het team Informatieveiligheid werken in kwartaal 4 toe naar 1 meldloket voor zowel beveiligingsincidenten als datalekken. Daarbij komen de meldingen bij beide partijen binnen. Samen maken zij vervolgens de afweging of het om een beveiligingsincident en/of een datalek gaat.

- **Geheimhouding en integriteit**
  PZH werkt al met geheimhoudings- en integriteitsverklaringen. Daarnaast besteden wij aandacht aan onderwerpen als screening, gebruik van social media en gedragscodes. Toch is het onze doelstelling om deze uitvoeringskaders verder te versterken, uit te breiden en/of volledig te maken. Dit doen we in lijn met AVG-compliancy. In kwartaal 4 van 2024 onderzoekt de Eenheid Privacy – in samenwerking met Personeel & Organisatie – hoe we privacy en gegevensbescherming tot een integraal onderdeel van deze kaders kunnen maken.

- **Informatieveiligheid**
  Om de samenwerking tussen de Eenheid Privacy en het team Informatieveiligheid te stimuleren en te borgen, zetten we in op regelmatige afstemming en integratie van de werkzaamheden. We gaan tweewekelijkse overlegmomenten organiseren waarin beide teams gezamenlijk de voortgang bespreken, uitdagingen identificeren, en gezamenlijke doelstellingen vaststellen. Daarnaast ontwikkelen we een gezamenlijke ‘roadmap’. Hierin komen de prioriteiten en acties van beide teams. Om de samenwerking verder te versterken, delen we onderling kennis en ‘best practices’. Dit doen we met gezamenlijke workshops en trainingen, waardoor medewerkers van beide teams elkaars expertise beter leren kennen en benutten.

- **Wegwerken achterstand DPIA’s**
  Uit het register blijkt dat circa 60 verwerkingen ‘waarschijnlijk een hoog risico inhouden voor de betrokkene’. Dit is een criterium waarbij de AVG eist dat een DPIA voor een verwerking wordt uitgevoerd. Om de achterstand in DPIA’s weg te werken, pakken we meerdere DPIA’s binnen soortgelijke opdrachten tegelijk aan. Daarnaast breiden we de capaciteit uit. Deze opzet zorgt voor een beheersbare werklast en draagt bij aan een gestructureerde en efficiënte werkwijze.

- **Verwerkingenregister**
  We brachten de verwerkingen van persoonsgegevens in kaart en registreerden ze in Privacy Nexus. Het gaat om circa 240 verwerkingen. De FG accordeerde iets meer dan de helft van deze verwerkingen, die nu dus volledig zijn. Verder geldt voor een aantal verwerkingen dat er enige twijfel is over de volledigheid en juistheid van de registraties. Daarnaast zijn we ons ervan bewust dat we nog niet alle verwerkingen in beeld hebben.

  Het compleet maken van het verwerkingsregister is een doorlopend proces, waar we uiteraard al jaren aan werken. Ook in de komende maanden gaan we met de gevraagde extra capaciteit hiermee verder. Dit combineren we zo veel mogelijk met het uitvoeren van pre-DPIA’s en de hiervoor beschreven DPIA-aanpak. Daarmee zorgen we ervoor dat het register op termijn correct gevuld is met de voorgeschreven rubrieken. En dat het een actueel en samenhangend beeld biedt van de gegevensverwerkingen binnen de organisatie.

  Om dit te realiseren, betrekken we de ambtelijk opdrachtgevers van de verschillende opdrachten actief bij het proces. Hun input is essentieel om een volledig inzicht te krijgen in de gegevensverwerkingen.

2.4 FG-adviezen

2.4.1 De omgang met FG-adviezen

De provincie Zuid-Holland erkent de cruciale rol van de Functionaris voor Gegevensbescherming in het geven van weloverwogen adviezen. In de afgelopen jaren heeft de FG ons voorzien van stevige en deskundige aanbevelingen.

Wij probeerden altijd de wet- en regelgeving zorgvuldig in acht te nemen en deze zo goed mogelijk te integreren in onze andere verplichtingen, belangen en bedrijfsvoering. Toch erkennen wij dat de documentatie rondom deze afwegingen ontbreekt. Daarom besloten wij om nog in 2024 een formele procedure in te voeren. Hiermee borgen we de juiste documentatie voor de opvolging van adviezen van de FG. De directie voorziet het jaarrapport van de FG van een oplegger. Hierin wordt per ontvangen advies uiteengezet welke overwegingen er zijn gemaakt met betrekking tot de opvolging van dit advies. Deze procedure zal ook van toepassing worden op reguliere (niet periodieke) FG-adviezen.

In geval van afwijking van een advies van de FG zijn de ambtelijke opdrachtgevers en -nemers verplicht tot het formuleren van een afwijkingsbesluit, waarmee ze de directie adviseren. Hierin staat waarom het advies van de FG niet is opgevolgd. Het hoogste managementniveau moet dit afwijkingsbesluit goedkeuren. Zo waarborgen we dat de beslissing zorgvuldig is overwogen en dat er voldoende begrip is voor de mogelijke gevolgen. Alle afwijkingsbesluiten documenteren we op een nader te bepalen locatie, waarbij we passende beveiligingsmaatregelen treffen. Met deze formele procedure willen we de transparantie en verantwoording met betrekking tot de naleving van FG-adviezen versterken.

We bevestigen als provincie onze inzet voor een strikte naleving van de privacywetgeving, en de samenwerking met de Eenheid Privacy, die als intern organisatieonderdeel de organisatie adviseert. Door deze adviserende rol en de nauwe samenwerking met de Functionaris Gegevensbescherming (FG) werken we gezamenlijk aan een effectievere en efficiëntere aanpak van privacyvraagstukken binnen onze organisatie.

2.4.2 De werkdruk van de FG in het licht van de achterstanden

Inmiddels voegden wij per 1 augustus een volledige FTE toe in de rol van FG. Dit betekent in ons geval een verdubbeling qua bezetting. Wij verwachten dat dit voldoende is voor de toegenomen werkdruk.

We namen de FG op 5 en 12 september mee in de voorliggende rapportage. Wij zijn daarom van mening dat de FG voldoende tijd heeft gehad om deze te beoordelen en van commentaar te voorzien.

2.5 Nawoord

Hoewel we vooruitgang boekten, erkennen we dat de snelheid waarmee we de privacy-volwassenheid van onze organisatie verhogen, beter kan.

Om onze inspanningen te versterken en verder te versnellen, werven we de komende tijd actief extra capaciteit. Dit zorgt dat we meer snelheid kunnen maken met de resterende werkzaamheden om het volwassenheidsniveau te verhogen. Daarnaast draagt het ook bij aan

het waarborgen van de continuïteit van ons reguliere werk. We blijven ons inzetten voor het verbeteren van onze processen en het verhogen van onze privacy-volwassenheid.

2.6 Bijlagen

Bijlage 5. Privacy-beleid

Bijlage 6. Programmaplan

3. Reflectie op vragen AP

In antwoord op uw brief voorzien wij in deze rapportage elk aandachtspunt van een reactie.

Betrokkenheid van diverse aansturingslagen bij de provincie

- *Daarbij geeft u specifiek aan dat u zich zorgen maakt over de geringe betrokkenheid van het politieke bestuur bij zowel het oplossen van het datalek als het verhogen van het privacy-volwassenheidsniveau. De AP verzoekt de provincie hierover - en over hoe de verantwoordelijkheden precies belegd zijn - meer duidelijkheid te geven in de eerstvolgende rapportage.*

Onze reactie:

De concerndirecteur is ambtelijk opdrachtgever van dit programma. Daarmee benadrukken we de urgentie van dit programma en borgen we een sterke aansturing en ondersteuning. Met deze keuze maken we ook in de organisatie duidelijk dat we de doelstellingen van dit programma tot hoogste prioriteit hebben gemaakt. De concerndirecteur is voorzitter van de stuurgroep die verder bestaat uit:

- Directeur bedrijfsvoering (ambtelijk opdrachtnemer)
- Ambtelijk opdrachtgever Privacy en Informatieveiligheid
- Programmamanager Privacy
- Ambtelijk opdrachtgever Communicatie
- Functionaris voor Gegevensbescherming

De stuurgroep bespreekt tweewekelijks de aanpak, resultaten en voortgang van het programma. Tijdens deze bijeenkomsten worden inhoudelijke of strategische keuzes toegelicht en afgestemd. Waar dat aan de orde is, neemt de stuurgroep besluiten. Er is ook periodiek afstemming met de verantwoordelijke Gedeputeerde. Wanneer keuzes verstrekkende gevolgen hebben, vindt hier overleg en besluitvorming plaats.

De Functionaris voor Gegevensbescherming (FG) heeft tweewekelijks overleg met de concerndirecteur en 6-wekelijks met de portefeuillehouder. De portefeuillehouder is lid van het college van Gedeputeerde Staten (provinciebestuur) en heeft een wekelijks overleg met zijn teamstaf. Daar staat het onderwerp privacy regelmatig op de agenda. De concerndirecteur sluit ook regelmatig bij deze overleggen aan.

Gedeputeerde Staten en Provinciale Staten worden in overeenstemming met de rapportagecadans op de hoogte gehouden van de voortgang.

- *U geeft specifiek aan dat u zorgen heeft over de betrokkenheid van de diverse managementlagen binnen de provincie. De AP verzoekt de provincie hierover - en over hoe de verantwoordelijkheden precies belegd zijn - meer duidelijkheid te geven in de eerstvolgende rapportage.*

Onze reactie:

Naast de hierboven genoemde stuurgroep is er een kernteam. Dit team stuurt wekelijks op de uitvoering van de besluiten en bereidt besluiten voor. Het kernteam bestaat uit:

- Directeur Bedrijfsvoering
- Ambtelijk opdrachtgever Privacy en Informatieveiligheid
- Programmamanager 'Zorgvuldig omgaan met persoonsgegevens'
- Projectmanager Datalek
- CISO
- Ambtelijk opdrachtgever Informatietransitie
- Programmamanager Informatietransitie
- Communicatieadviseur

Het kernteam heeft een afvaardiging van de diverse direct betrokken managementlagen binnen de organisatie. Hiermee creëren we eenheid van beleid en richting. Het kernteam geeft gezamenlijk richting aan de uitvoering van het project en neemt de operationele beslissingen. De stuurgroep neemt wezenlijke besluiten, onder leiding van de concerndirecteur.

Naast de aansturing van het project vindt er, indien noodzakelijk, afstemming plaats met de diverse AOG's en p-managers binnen de domeinen die te maken hebben met (de gevolgen van) dit project. Wij informeren hen wanneer activiteiten impact hebben op hun werkzaamheden.

Snelheid

De AP maakt uit de rapportage op dat de provincie nog werkt aan het inventariseren van de benodigde verbeteringen om op privacy-volwassenheidsniveau 3 (CIP-model) te komen. De AP had gehoopt dat een dergelijke inventarisatie al afgerond was en dus onderdeel had uitgemaakt van de eerste rapportage. De AP roept de provincie Zuid-Holland op vaart te maken met de inventarisatie van de benodigde verbeteringen om op privacy-volwassenheidsniveau 3 (CIP-model) te komen.

Onze reactie:

Deze inventarisatie vond inmiddels plaats en dit resulteerde in een lijst van verbeteringen en concrete acties. Deze moeten we doorvoeren om op niveau 3 te komen. Deze opbrengst leidde tot belangrijke input voor het programmaplan. Het programmaplan vindt u als bijlage bij deze rapportage.

Het valt de AP ook op dat niet veel vaart lijkt te worden gemaakt met het vaststellen van een privacy-beleid voor de provincie Zuid-Holland. De AP doet een oproep om het concept privacy-beleid formeel vast te stellen, en de AP te informeren over hoe de verantwoordelijkheden precies zijn belegd.

Onze reactie:

Het privacy-beleid voor de provincie Zuid-Holland is formeel vastgesteld op 25 juni 2024. In de bijlage treft u dit beleid aan.

Het college van Gedeputeerde Staten (GS) is bestuurlijk eindverantwoordelijk voor het naleven van de privacy-wet-en regelgeving en voor de kaders van het verantwoord omgaan met persoonsgegevens. Als verantwoordelijk gezag stellen GS het privacy-beleid vast. Over de uitvoering ervan leggen GS verantwoording af aan Provinciale Staten (PS).

Het Directieteam (DT) bestaat uit de provinciesecretaris en de concerndirecteur. Het DT is ambtelijk eindverantwoordelijk voor de bedrijfsvoering van de provincie Zuid-Holland. Daarmee is zij dat ook voor de uitvoering van - en sturing op - de beleidskaders voor privacy. Op basis van het privacy-beleid wijst het DT taken, verantwoordelijkheden en bevoegdheden toe. Het DT heeft op basis van zijn actieve informatieplicht de verantwoordelijkheid om GS te informeren wanneer er sprake is van kritieke risico's, of wanneer het privacy-beleid niet wordt nageleefd (non-compliancy).

De dagelijkse verantwoordelijkheid voor het voldoen aan de uitgangspunten van de privacy-wet- en -regelgeving binnen de provincie, ligt bij de Ambtelijk Opdrachtgevers (AOG's) en de p-managers. De AOG's en p-managers zorgen ervoor dat men binnen de opgaven volgens het privacy-beleid werkt. De AOG geeft de Ambtelijk Opdrachtnemer (AON) aanwijzingen hoe deze de randvoorwaarden het beste kan invullen binnen diens opdracht. De AOG's en p-managers zijn binnen hun werkzaamheden verantwoordelijk om de juiste disciplines, op het juiste moment, te betrekken. Voor privacy is dat de Eenheid Privacy.

Concretisering

Het is de AP opgevallen dat, hoewel de rapportage veelomvattend is, niet alle punten die benoemd worden ook echt concreet zijn uitgewerkt. Onder het kopje 'uitvoeringsdomein', worden wel veel zaken benoemd, maar niet duidelijk wordt hoe, wanneer en door wie aan deze punten gewerkt gaat worden, laat staan welke acties precies nodig zijn.

Onze reactie:

Deze inventarisatie vond inmiddels plaats en dit resulteerde in een lijst van verbeteringen en concrete acties. Deze moeten we doorvoeren om op niveau 3 te komen. Deze opbrengst leidde tot belangrijke input voor het programmaplan. Het programmaplan vindt u als bijlage bij deze rapportage.

Datzelfde geldt bijvoorbeeld ook heel concreet voor het punt van het toevoegen van een ethische afweging in de nieuwe (pre-)DPIA-systematiek die de provincie klaarblijkelijk voorstaat.

Onze reactie:

Als onderdeel van de vorige DPIA-systematiek en modellen probeerden we een eerste stap te zetten richting het vormen van een ethisch kader - en een daarbij passende, meetbare systematiek -, gericht op het verhogen van bewustzijn rond ethische problemen bij verwerkingen. Voor deze eerste stap gebruikten we destijds de Ethische Data Assistent (DEDA) van de Data School van de Universiteit Utrecht. Samen met een begeleidend hoofdstuk over ethiek namen we de opsteller van de pre-DPIA mee in eventuele ethische afwegingen. Deze kunnen gemaakt worden bij het in kaart brengen van de risico's van een verwerking.

In de nieuwe systematiek zetten we hierin een grote stap. De vraagstelling en thematiek van de Ethische Data Assistent en het Impact Assessment Mensenrechten en Algoritmes (IAMA) is geïnventariseerd en geëvalueerd. Op basis van beide instrumenten voegden we een 'Ethiek Assessment' toe aan de nieuwe pre-DPIA- en DPIA-modellen.

Het gebrek aan concreetheid laat zich ook zien bij het op orde krijgen van het verwerkingenregister. Dit lijkt moeizaam te verlopen, maar wat de redenen hiervoor zijn, is niet duidelijk.

Onze reactie:

We brachten de verwerkingen van persoonsgegevens in kaart en registreerden ze in Privacy Nexus. Het gaat om circa 240 verwerkingen. De FG accordeerde iets minder dan de helft van deze verwerkingen, die nu dus volledig zijn. Verder geldt voor een aantal verwerkingen dat er enige twijfel is over de volledigheid en juistheid van de registraties. Daarnaast zijn we ons ervan bewust dat we nog niet alle verwerkingen in beeld hebben.

Het vullen van het verwerkingenregister was de afgelopen jaren voornamelijk bij de Eenheid Privacy belegd. Dat had als oorzaak dat de verantwoordelijkheid van de eerste lijn nog onvoldoende was ingericht. Met het privacy-beleid ligt de verantwoordelijkheid voor de naleving van de AVG in de eerste lijn (three-lines-of-defence) van de provincieorganisatie. Dat houdt in dat de eerste lijn – de ambtelijk opdrachtgever – formeel verantwoordelijk is voor een juiste registratie van de verwerkingen in het verwerkingenregister. De Eenheid Privacy neemt deze verplichting niet over. Wel ondersteunt en faciliteert zij met kennis en expertise.

We combineren het compleet maken van het verwerkingsregister zoveel mogelijk met de in de vorige paragraaf beschreven DPIA-aanpak. Daarmee zorgen we ervoor dat het register op termijn correct gevuld is met de voorgeschreven rubrieken. En dat het een actueel en samenhangend beeld biedt van de gegevensverwerkingen binnen de organisatie.

Omgang FG

Het is dan ook goed om in de rapportage te lezen dat er nu een formele procedure wordt ingericht voor het reageren op de adviezen van de FG. Ook hier geldt echter dat veel nog onduidelijk is over hoe deze procedure precies vorm zal krijgen. Hier is dan ook nadere verduidelijking gewenst.

Onze reactie:

Dit jaar (dus over het FG-jaarverslag over 2023) besloten we een formele procedure in te voeren. Daarmee borgen we de juiste documentatie voor de opvolging van adviezen van de FG. De directie voorziet het jaarrapport van de FG van een oplegger. Hierin wordt per ontvangen advies uiteengezet welke overwegingen er zijn gemaakt met betrekking tot de opvolging van dit advies. Deze procedure zal ook van toepassing worden op reguliere (niet periodieke) FG-adviezen.

In geval van afwijking van een advies van de FG zijn de ambtelijke opdrachtgevers en -nemers verplicht tot het formuleren van een afwijkingsbesluit, waarmee zij de directie adviseren. Hierin staat waarom het advies van de FG niet is opgevolgd. Alle afwijkingsbesluiten documenteren we op een nader te bepalen locatie, waarbij we passende beveiligingsmaatregelen treffen.

In de rapportage wordt vermeld dat er een dertigtal achterstallige DPIA's is. Dat is een behoorlijk aantal voor een organisatie om nog in te halen, maar zeker ook voor een FG om allemaal te beoordelen. Uit de rapportage wordt niet duidelijk of de FG hier naast zijn doorlopende werkzaamheden voldoende tijd en middelen voor heeft.

Onze reactie:

Inmiddels voegden wij per 1 augustus een volledige FTE toe in de rol van FG. Dit betekent in ons geval een verdubbeling qua bezetting. Wij verwachten dat dit voldoende is voor de toegenomen werkdruk.

Tot slot wijst de AP erop dat de FG nu slechts kort voordat de rapportage aan de AP werd opgestuurd pas de gelegenheid kreeg om de rapportage te beoordelen. Dit is dan ook van invloed geweest op de (on)volledigheid van zijn reactie. De AP verzoekt de provincie Zuid-Holland de FG bij de eerstvolgende rapportage eerder om zijn reactie te vragen.

Onze reactie:

We namen de FG op 5 en 12 september mee in de voorliggende rapportage. Wij zijn daarom van mening dat de FG voldoende tijd heeft gehad om deze te beoordelen en van commentaar te voorzien. Het gaat ons in aansluiting op het voorgaande niet alleen om de beoordeling van de rapportage maar om het geheel aan documenten ter beoordeling aan de FG. Wij waarderen zijn inbreng ten zeerste en zijn ons ervan bewust dat wij soms te weinig gebruikmaken van zijn expertise en ervaring. Alhoewel wij in het afgelopen kwartaal dit wel enigszins verbeterden, zetten wij deze ontwikkeling, waarin de FG nauwer betrokken wordt, door.

Datalek

Nog steeds is de volledige omvang van het lek niet in beeld. En evenmin is dus te zeggen dat alle betrokkenen in beeld zijn.

Onze reactie:

Dit klopt. Na afronding van de PoC (eind september 2024) zijn wij in staat om een uitspraak te doen over de omvang van het lek op basis van een eerste selectie van 2 miljoen documenten. De volledige omvang is daarmee niet bepaald maar deze analyse geeft een eerste indicatie van de omvang. Pas nadat de restant 19 miljoen documenten zijn geanalyseerd (met behulp van een analysetool) kunnen we de omvang van dit datalek beter duiden.

Het klopt dat nog niet alle betrokkenen in beeld zijn. Wij gaven eerder in onze brief van 25 juli 2024 aan dat we het liefst alle betrokkenen voor wie het datalek een hoog risico inhoudt, individueel zouden willen informeren. Dit is helaas op dit moment niet haalbaar, vanwege de technische inrichting van iDMS en de omvang van 50,3 miljoen documenten. De huidige manier van loggen en de inrichting van de groepsaccounts maken het onmogelijk te achterhalen of de documenten onrechtmatig in te zien zijn/waren, of ingezien zijn.

We investeren op het moment veel in het verkrijgen van inzicht in de documenten in IDMS. Met behulp van slimme software gaan we zo spoedig mogelijk de documenten in iDMS scannen en analyseren. De tooling controleert alle documenten inhoudelijk op aanwezigheid van persoonsgegevens. Dat helpt ons bij het dichten van het datalek. De invoering van dergelijke tooling vraagt om zorgvuldigheid. Het scannen van de grote hoeveelheid documenten vergt veel tijd. We zijn eind augustus begonnen met deze scans.

Een bijkomend voordeel van deze scans zou kunnen zijn dat we betrokkenen beter kunnen identificeren.

Ook wil de AP enkele onjuistheden rondom het datalek benoemen. Op de website van de provincie Zuid-Holland is gecommuniceerd dat er een datalek is geweest. Feitelijk vindt het datalek nog steeds plaats (het datalek ligt niet slechts in het verleden). Dit is dus niet goed gecommuniceerd richting betrokkenen.

Onze reactie:

We herstelden deze onjuistheid in nadere berichtgeving op de website.

Reactie FG

Inleiding

De FG spreekt zijn waardering uit voor de inspanningen van allen die meewerken aan het programma Privacy. De FG meent dat eenieder binnen de programmaorganisatie onder aanvoering van de concerndirecteur inmiddels doordrongen is van de noodzaak om het datalek zo snel mogelijk te beëindigen als ook het privacy-volwassenheidsniveau binnen de gehele organisatie te verhogen. Het kost echter nog grote inspanningen en neemt een geruim tijdsverloop in beslag voordat dit besef ook in de haarvaten van de gehele organisatie zit. De FG begrijpt om die redenen ook dat de provincie de streefdatum om volwassenheidsniveau drie te behalen heeft verlaat naar 31 december 2026. Een jaar eerder is gewoonweg niet realistisch.

De plannen zoals genoemd in deze rapportage zien er op hoofdlijnen positief uit. Echter zijn veel onderdelen nog onvoldoende uitgewerkt om een scherp oordeel te kunnen geven. Ten aanzien van het oplossen van de problemen rondom het datalek in IDMS zijn in het afgelopen kwartaal de eerste stappen gezet. Het verhogen van het privacy volwassenheidsniveau gaat helaas tot op heden minder voortvarend. Zeker daarop wordt het voor PZH tijd om te gaan leveren.
Daarover heeft de FG echter gerede twijfels, gelet op de prestaties in het afgelopen jaar. De rapportage heeft nogal wat positieve aannames waarbij wordt uitgegaan van voldoende (arbeids-)capaciteit. Daartegenover stelt de provincie in deze rapportage dat het uitdagend is om tijdig voldoende en bekwaam personeel te werven.

De FG is blij te constateren dat zijn feedback op eerdere conceptversies van deze rapportage een positief effect heeft gehad.

Programmalijn 1: dichten van het datalek

Omvang persoonlijke werkomgeving

De FG begrijpt dat de risico-gebaseerde aanpak van de provincie erin resulteert dat de 20 miljoen items in de persoonlijke werkomgeving van medewerkers in een later stadium worden opgepakt. De FG is geschrokken van de enorme omvang van de opgeslagen documentatie in deze omgeving en meent dat dit, weliswaar wat later, serieus de aandacht verdient. Het kan niet anders dan dat medewerkers toegang hebben tot documentatie waar zij uit hoofde van hun huidige functie geen toegang meer toe behoren te hebben. Dit maakt daarmee onverkort onderdeel uit van dit datalek en moet zo snel mogelijk worden opgelost.

De organisatie meldt dat voor 11,3 miljoen items de concernbrede rechten zijn ingetrokken. Er wordt daarmee de indruk gewekt dat daarmee de betreffende documenten niet meer toegankelijk zijn voor alle medewerkers. Dat is in principe waar, maar daarbij dient te worden opgemerkt dat, door (onterechte) “stapeling van rechten” nog veel documenten onterecht toegankelijk zijn.

De FG heeft ook zorgen over de aantoonbaarheid van de effectiviteit van de getroffen maatregelen. Zijns inziens zou het wenselijk zijn als de organisatie gaat werken met processen-verbaal van uitgevoerde acties, zeker waar het gaat over het ontnemen danwel toekennen van rechten, maar ook bij het gebruik van de analysetool.

Nieuwe organisatiestructuur

Een ander probleem is, zo voorziet de FG, dat de structuur van het iDMS niet correspondeert met de gewijzigde organisatiestructuur van de provincie. Dit maakt dat de FG nog niet is overtuigd dat, zoals de provincie schrijft, het project IAM kan garanderen dat de toewijzing van autorisaties aan medewerkers geautomatiseerd en juist verloopt en daarmee een structurele oplossing biedt ter voorkoming van het schenden van de AVG.

Informeren van betrokkenen

De FG meent dat de provincie stelling dient te nemen jegens de AP over het informeren van betrokkenen. Gelet op de wijze van loggen en het gebruik van groepsaccounts is het onmogelijk te achterhalen welke persoonsgegevens onrechtmatig zijn ingezien. Waarom gebruik van de analysetool dit anders zou maken is de FG niet duidelijk. Als er niet gelogd is, kan een tool die logging ook niet analyseren. De FG meent dat de provincie dit ook zo aan de AP moet rapporteren en de doelstelling in paragraaf 1.2 daarop dient te worden aangepast.
Daarnaast lijkt de laatste vraag AP niet consistent beantwoord in lijn met rapportage.

Onduidelijkheden

Ook op een aantal andere punten roept de rapportage vragen op bij de FG.

De PoC is op moment van schrijven van deze rapportage nog niet uitgevoerd danwel afgerond. De FG heeft daar ook nog geen enkel inzicht in gekregen en evenmin in de resultaten die de PoC heeft opgeleverd af ten dele heeft opgeleverd. In aansluiting daarop leeft bij de FG de zorg of de vermelde planning realistisch is gelet op de resultaten van de PoC.

Programmalijn 2: verhogen volwassenheid van de organisatie

Het valt de FG op dat de provincie pas heel recent besloten heeft om extra privacy officers te gaan werven. Waar de conclusie op is gebaseerd dat er geen geschikte mensen op de arbeidsmarkt beschikbaar zijn, is de FG onduidelijk. De FG merkt op dat het tempo waarin het HRM-proces wordt uitgevoerd te traag is, zeker met het oog op de kwetsbare positie van de eenheid Privacy.

De provincie sprak in de vorige rapportage de verwachting uit dat er in Q2 2024 een Learning Management System beschikbaar zou zijn. Indien dat niet het geval zou zijn, zou de eenheid Privacy inzetten op een eigen e-learning in 2024. Thans is dit laatste verschoven naar Q1 2025. De FG maakt zich zorgen over deze vertraging.

De FG maakt zich daarnaast zorgen over het tempo waarmee DPIA’s worden opgepakt en het verwerkingsregister wordt gevuld. De FG voorziet dat het een uitdaging wordt om binnen de gestelde einddatum de achterstand te hebben ingehaald.

De FG is content dat er een proces wordt ingericht over de omgang met zijn adviezen. Wel meent de FG dat bij afwijking van zijn advies de beslissingsbevoegdheid niet op het niveau van ambtelijk opdrachtnemer behoort te liggen. De FG meent dat dit besluit door de concerndirecteur genomen behoort te worden.

In het programmaplan is het informeren van betrokkenen onderdeel van programmalijn 1. Op pagina 20 leest de FG dat het inzicht verkrijgen in onrechtmatig gebruik van documenten buiten scope is. Daarmee geeft de provincie te kennen ook vooralsnog geen poging te doen om betrokkenen te identificeren. Het programmaplan is daarmee in tegenspraak met het vermelde hieromtrent in de AP-rapportage.

Tot slot wenst de FG nog op te merken dat een stevige aansturing door de concerndirecteur onmisbaar is voor het slagen van het programma.

16 september 2024

Niels Bons en Harmen Hoevers
Functionaris voor Gegevensbescherming PZH

Bijlagen

Bijlage 1: Nieuwsbericht Intranet op 11 april 2024

Bijlage 2: Berichtgeving zuid-holland.nl op 11 april 2024

Bijlage 3: E-mail concerndirecteur aan medewerkers op 11 juli 2024

Bijlage 4: Nieuwsbericht Intranet op 11 juli 2024

Bijlage 5. Privacy-beleid

Bijlage 6. Programmaplan

Bijlage 1: Nieuwsbericht Intranet op 11 april 2024

Provincie onder geïntensiveerd toezicht Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) stelt de provincie Zuid-Holland onder geïntensiveerd toezicht. Dat betekent dat de provincie concrete afspraken gaat maken met de AP over hoe ze zorgvuldiger omgaat met persoonsgegevens en daarover geregeld moet rapporteren. De AP heeft zorgen over de beveiliging van persoonsgegevens binnen de provincie. De provincie moet zo snel mogelijk actie ondernemen op signalen die zijn afgegeven over de veiligheid van informatie. Die signalen hebben betrekking op systemen die we gebruiken om informatie te verwerken en de manier waarop we de informatie opslaan. De zorgen richten zich vooral op het privacy-volwassenheidsniveau binnen de provincie, het nalaten om aanbevelingen van de Functionaris voor Gegevensbescherming op te volgen en de afhandeling van een recentelijk gemeld datalek. Daaruit blijkt dat de provincie niet voldoet aan een aantal vereisten uit de Algemene Verordening Gegevensbescherming (AVG).

Aanleiding: datalek

Concrete aanleiding vormt onder meer de melding van een datalek op 8 september 2023. Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is, waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

Wat is er gebeurd?

Het datalek waar vorig jaar melding van is gemaakt, betreft IDMS. Onze teams Privacy en Informatieveiligheid kwamen in IDMS persoonsgegevens tegen in mappen die voor iedereen die in IDMS kan kijken toegankelijk waren. Het betreft in dit geval een datalek omdat de mappen met daarin persoonsgegevens (mogelijk) zichtbaar zijn (geweest) voor mensen die die gegevens niet hadden mogen zien, omdat ze deze niet nodig hebben voor de uitvoering van hun werk. Nader onderzoek heeft uitgewezen dat nog meer persoonsgegevens toegankelijk zijn geweest voor medewerkers die voor de uitoefening van hun functie geen toergang nodig hadden tot deze gegevens.

De betrokken persoonsgegevens zijn per definitie alleen toegankelijk voor collega's. Het is daarom niet aannemelijk dat andere personen dan collega's de persoonsgegevens hebben ingezien. We hebben hier ook geen signalen over ontvangen.

Wat zijn de waarschijnlijke gevolgen voor medewerkers?

Alhoewel IDMS een intern systeem is en alleen collega's toegang hebben tot IDMS is er dus mogelijk wel toegang geweest door collega's tot documenten die niet noodzakelijk waren voor de uitvoering van de werkzaamheden. Wij verwachten dat dit datalek weinig tot geen gevolgen heeft voor collega's. Iedereen is gehouden een eed of belofte af te leggen of een geheimhoudingsverklaring te ondertekenen en integer om te gaan met de beschikbare informatie binnen de provincie. We hebben geen signalen ontvangen waaruit iets anders blijkt.

Welke maatregelen heeft de provincie genomen of gaat de provincie nemen?

Direct na melding van het datalek is er actie ondernomen, waaronder het identificeren en isoleren van documenten, het afsluiten van bepaalde mappen en het opnieuw instellen van bepaalde autorisaties. De AP heeft aangegeven dat de provincie op grond van de AVG de

betrokkenen bij dit datalek dient te informeren. Dit houdt in dat er een communicatietraject wordt voorbereid, waarin zowel medewerkers als externe betrokkenen geïnformeerd worden. Om maatregelen op langere termijn te identificeren en de veiligheid van de systemen te kunnen waarborgen is binnen het domein Bedrijfsvoering een opdracht gestart: ‘Bescherming persoonsgegevens provincie Zuid-Holland: Privacyvolwassenheid 3 en datalek IDMS’. Binnen deze opdracht zijn diverse teams betrokken, ieder met hun eigen expertise.

Jouw hulp is keihard nodig!

Het toezicht van de AP betekent dat we de komende tijd extra gaan inzetten op privacy. Daar is jouw hulp keihard bij nodig. We kunnen miljoenen investeren in de aanschaf van moderne systemen en betere techniek, maar uiteindelijk blijft privacy ook mensenwerk.

- Wees je bewust welke informatie privacygevoelig is en sla die informatie alleen op wanneer dat nodig is. Verwijder de informatie wanneer dat kan en zorg ervoor dat alleen mensen die die informatie gebruiken voor hun werk de informatie kunnen inzien.
- Ga hoe dan ook niet doelbewust in IDMS zoeken naar mogelijke persoonsgegevens van collega's, jezelf of wie dan ook als je die niet nodig hebt voor je werk! Dit is NIET toegestaan. Je creëert daarmee mogelijk een nieuw datalek en een integriteitskwestie.
- Controleer je eigen mailbox, je Teams-omgevingen, mappen in IDMS die je beheert en andere plekken waar je data opslaat. Verplaats of verwijder documenten met persoonsgegevens die daar niet thuishoren of niet (meer) relevant zijn.

Vragen?

Heb je vragen over dit datalek, dan kun je deze stellen aan onze Functionaris voor Gegevensbescherming, Niels Bons, via fg@pzh.nl. Bekijk ook de groep Privacy-AVG op Binnenplein eens voor handige tips en informatie. Volg voor meer informatie over hoe je zorgvuldig kunt omgaan met persoonsgegevens, data en informatie de groep ZO doen we dat! op Binnenplein.

Bijlage 2: Berichtgeving zuid-holland.nl op 11 april 2024

Provincie onder geïntensiveerd toezicht Autoriteit Persoonsgegevens

Gepubliceerd op 11 april 2024

De Autoriteit Persoonsgegevens (AP) stelt de provincie Zuid-Holland onder toezicht. Dat betekent dat de provincie concrete afspraken gaat maken met de AP over hoe de provincie zorgvuldiger om gaat met persoonsgegevens en daarover geregeld moet rapporteren.

De AP heeft zorgen over de bescherming van persoonsgegevens binnen de provincie en wil dat de provincie sneller actie gaat ondernemen op signalen die eerder zijn afgegeven over de vertrouwelijkheid van persoonsgegevens die we binnen de provincie verwerken en opslaan.

Aanleiding: datalek

Concrete aanleiding vormt onder meer de melding van een datalek op 8 september 2023. Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is, waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

Wat is er gebeurd?

Het datalek waar vorig jaar melding van is gemaakt betrof persoonsgegevens in een intern systeem dat de provincie gebruikt voor archivering, opslag van en intern samenwerken aan documenten. Onze teams Privacy en Informatieveiligheid kwamen in het systeem persoonsgegevens tegen die voor te veel medewerkers van de provincie toegankelijk waren. Nader onderzoek heeft uitgewezen dat nog meer persoonsgegevens toegankelijk zijn geweest voor medewerkers die voor de uitoefening van hun functie geen toegang nodig hadden tot deze gegevens.

De betrokken persoonsgegevens zijn per definitie alleen toegankelijk voor medewerkers van de provincie. Het is daarom niet aannemelijk dat andere personen dan (oud-)medewerkers de persoonsgegevens hebben ingezien.

Wat zijn de waarschijnlijke gevolgen van dit datalek voor betrokkenen?

Wij verwachten dat dit datalek weinig tot geen gevolgen heeft voor burgers en bedrijven van de Provincie Zuid-Holland. Het datalek heeft plaatsgevonden in een intern systeem. We hebben geen signalen ontvangen dat andere personen dan eigen medewerkers documenten hebben kunnen inzien. Onze medewerkers hebben als ambtenaar allen een eed of belofte afgelegd of een geheimhoudingsverklaring getekend voor het uitvoeren van werkzaamheden voor de provincie en zijn bekend met het onderwerp integriteit en het omgaan met (privacy)gevoelige informatie.

Welke maatregelen heeft de provincie genomen of gaat de provincie nemen?

Direct na melding van het datalek is er actie ondernomen, waaronder het identificeren en isoleren van documenten, het afsluiten van bepaalde mappen en het opnieuw instellen van bepaalde autorisaties. Om maatregelen op langere termijn te identificeren en de veiligheid van de systemen te kunnen waarborgen is binnen het domein Bedrijfsvoering een opdracht

gestart: ‘Bescherming persoonsgegevens provincie Zuid-Holland: Privacyvolwassenheid 3 en datalek IDMS’. Binnen deze opdracht zijn diverse teams betrokken, ieder met hun eigen expertise.

Investeren in systemen en mensen

De provincie herkent zich in de brief van de AP dat het omgaan met informatie die de provincie is toevertrouwd essentieel is. Al vóór deze melding heeft de provincie €23 miljoen uitgetrokken voor de groei en transitie van de provinciale informatiehuishouding. Bovendien investeren we onder andere met een langlopende campagne en trainingen in het data-vaardiger maken van collega’s want zorgvuldig omgaan met data is ook mensenwerk. We zien het verscherpte toezicht van de Autoriteit Persoonsgegevens als een kans om deze transitie samen te versnellen.

Vragen?

Voor vragen of meer informatie over dit datalek kan contact worden opgenomen met de Functionaris voor Gegevensbescherming, Niels Bons, via fg@pzh.nl.

Meer informatie over hoe de provincie omgaat met persoonsgegevens is te vinden in de privacyverklaring op onze website.

Bijlage 3: E-mail concerndirecteur aan medewerkers op 11 juli 2024

Beste collega,

Ik mail jullie over een belangrijk onderwerp: het datalek in IDMS. Op 11 april hebben jullie al op Binnenplein kunnen lezen over dat datalek. In het kort komt het erop neer dat in iDMS documenten staan met persoonsgegevens die voor (oud-) collega's toegankelijk zijn (geweest) die die gegevens voor hun werk helemaal niet nodig hebben of hadden. Er is melding van het datalek gemaakt bij de Autoriteit Persoonsgegevens. Die heeft ons vervolgens onder verscherpt toezicht gesteld. Dat betekent dat we eens per kwartaal verantwoording moeten afleggen aan de Autoriteit Persoonsgegevens. Enerzijds over het dichten van het datalek, maar anderzijds ook over hoe we als organisatie beter om leren gaan met privacy en persoonsgegevens.

Op onze website hebben we vandaag een nieuwe update geplaatst om mensen die betrokken kunnen zijn bij het datalek te informeren. Ook jij kan betrokkene zijn want in IDMS kunnen ook persoonsgegevens van jou staan die een (oud-)collega in heeft kunnen zien. Ik wil je dan ook vragen om het bericht te lezen. Er zijn nu geen aanwijzingen voor misbruik van persoonsgegevens uit IDMS maar ik vind het belangrijk je desondanks mee te geven welke maatregelen je zelf kunt nemen om misbruik van persoonsgegevens tegen te gaan.

Ondertussen werkt een team hard aan het dichten van het datalek. Daarover krijg je binnenkort meer informatie. Zoals in het eerdere bericht gezegd: ga niet zelf op zoek naar persoonsgegevens in IDMS als je die niet nodig hebt voor je werk. Ik reken er op dat jullie dat ook nu niet doen.

Met vriendelijke groet,

Jan van Ginkel

Link naar het bericht: https://www.zuid-holland.nl/actueel/nieuws/juli-2024/update-datalek-intern-systeem-provincie-zuid/

Bijlage 4: Nieuwsbericht zuid-holland.nl op 11 juli 2024

Update datalek in intern systeem Provincie Zuid-Holland

Gepubliceerd op 11 juli 2024

De Autoriteit Persoonsgegevens (AP) heeft de provincie onder geïntensiveerd toezicht gesteld. Dat betekent dat de provincie concrete afspraken moet maken met de AP over hoe ze zorgvuldiger om wil gaan met persoonsgegevens en daarover geregeld moet rapporteren. Je hebt hier eerder over kunnen lezen op 11 april.

Wat is er ook alweer aan de hand?

Concrete aanleiding vormt vooral een datalek in een intern systeem dat we hebben gemeld op 8 september 2023. Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of de bedoeling is. Het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens zijn voorbeelden van datalekken. De provincie gebruikt voor de archivering en opslag van documenten en het intern samenwerken aan documenten een document management systeem. Het systeem bevat allerlei gegevens, van memo's en besluiten tot uiteenlopende (persoonlijke) gegevens van burgers, zakelijke contacten en (externe) medewerkers.

Onze teams Privacy en Informatieveiligheid kwamen in dat systeem (bijzondere) persoonsgegevens tegen die toegankelijk waren voor vrijwel alle medewerkers van de provincie. Categorieën van persoonsgegevens die zijn aangetroffen zijn onder meer NAW-gegevens, contactgegevens, geboortedata, kopieën van identiteitsdocumenten, BSN-nummers en gegevens over opleiding- en werkervaring. Veel medewerkers hadden geen toegang tot deze gegevens nodig om hun functie uit te oefenen. Dat betekent dat er sprake is van een datalek.

Wie hebben ongeoorloofd persoonlijke gegevens in kunnen zien?

Alleen mensen met toegang tot het document management systeem van de provincie hebben potentieel persoonlijke gegevens kunnen inzien die ze niet nodig hebben voor het uitoefenen van hun werk. Omdat het systeem al jaren oud is, betekent dit ook dat gegevens in het verleden toegankelijk zijn geweest voor medewerkers die nu niet meer voor de provincie werken.

Welke maatregelen heeft de provincie al genomen of gaan we nog nemen?

Direct na melding van het datalek is er actie ondernomen, waaronder het identificeren en isoleren van documenten en het afsluiten van bepaalde mappen. Daarmee is het datalek helaas nog niet opgelost. Om maatregelen op langere termijn te identificeren en de veiligheid van de systemen en bescherming van persoonsgegevens te kunnen waarborgen, is de provincie gestart met de opdracht: 'Bescherming persoonsgegevens provincie Zuid-Holland: Privacyvolwassenheid 3 en datalek IDMS'. Binnen deze opdracht zijn diverse teams betrokken, ieder met hun eigen expertise.

Investeren in systemen en mensen

De provincie herkent zich in de brief van de AP dat zorgvuldig met informatie omgaan die aan de provincie is toevertrouwd essentieel is. Al vóór deze melding heeft de provincie €23 miljoen uitgetrokken voor de groei en transitie van de provinciale informatiehuishouding. Dit

is een omvangrijk programma waarin de manier waarop we naar data en informatie kijken en hoe we ermee omgaan, centraal staat. Bovendien investeren we onder andere met een langlopende campagne en trainingen in het data-vaardiger maken van collega's want zorgvuldig omgaan met data is mensenwerk. We zien het verscherpte toezicht van de Autoriteit Persoonsgegevens als een kans om deze transitie te versnellen.

Wat zijn de waarschijnlijke gevolgen van dit datalek voor betrokkenen?

Het is niet aannemelijk dat andere personen dan (voormalig) medewerkers van de provincie de persoonsgegevens hebben ingezien. We hebben geen signalen ontvangen dat documenten extern toegankelijk zijn (geweest). Onze medewerkers hebben een eed of belofte afgelegd of een integriteitsverklaring getekend voor het uitvoeren van werkzaamheden voor de provincie en zijn dus bekend met het onderwerp integriteit en hoe met (privacy)gevoelige informatie om te gaan.

Hoewel wij niet verwachten dat dit datalek grote gevolgen heeft voor betrokkenen, kunnen we eventuele nadelige gevolgen niet uitsluiten. Als gevolg van dit datalek bestaat er een risico op identiteitsfraude, oplichting, financiële fraude of reputatieschade, afhankelijk van de aard van de gegevens. Vanwege het grote aantal documenten in het systeem is het vooralsnog niet mogelijk om individuele personen te berichten en doen wij deze kennisgeving in zijn algemeenheid.

Welke maatregelen kun je zelf nemen?

Maatregelen die je kunt nemen om mogelijke nadelige gevolgen van een datalek te beperken zijn alert blijven op mogelijke phishing mails en verdachte telefoontjes of verdachte Whatsapp berichten of signalen van identiteitsfraude. Overige maatregelen zoals het regelmatig wijzigen van wachtwoorden, het gebruik van sterke wachtwoorden en het instellen van tweefactor authenticatie zijn altijd goede voorzorgsmaatregelen in de digitale wereld. Wil je meer weten over mogelijke maatregelen na een datalek? Kijk dan op de webpagina voor betrokkene van een datalek(opent in nieuw venster) van de Autoriteit Persoonsgegevens.

Vragen?

Voor vragen of meer informatie over dit datalek kun je contact opnemen met onze Functionaris voor Gegevensbescherming, Niels Bons, via fg@pzh.nl.

Meer informatie over hoe de provincie omgaat met persoonsgegevens is te vinden in de privacyverklaring op onze website.

Bijlage 5. Privacy-beleid

Dit document is als losse bijlage (pdf) toegevoegd.

Bijlage 6. Programmaplan

Dit document is als losse bijlage (pdf) toegevoegd.