PROVINCIE UTRECHT

RAPPORTAGE FUNCTIONARIS VOOR GEGEVENSBESCHERMING

DATUM	18-2-2022
VERSIE	1.0
DOCUMENT NUMMER	Documentnummer
RAPPORTAGEPERIODE	1 januari 2021 tot 1 januari 2022

INLEIDING

2021 was in Nederland een veelbewogen jaar op het gebied van privacy. Het jaar begint met een grootschalig datalek bij de GGD en eindigt met een fikse boete voor de Belastingdienst voor profileren (de Toeslagenaffaire). Daartussen zaten hacks van onderwijsinstellingen en de Media Markt (met flinke losgeldeisen), illegaal filmende auto's van de gemeente Rotterdam die de naleving van de corona-regels controleerden, BSN's van duizenden kinderen uit de gemeente Aalten die door een stagiair naar een verkeerd adres zijn gemaild en lege kaasschappen bij Albert Heijn door een hack bij de leverancier.

Ook binnen de provincie is er afgelopen jaar veel werk verzet op het gebied van privacy. Nu we het vijfde jaar in zijn gegaan van de werking van de Algemene Verordening Gegevensbescherming (AVG) is er een duidelijke doorontwikkeling te zien van implementeren van nieuwe regels naar inbedden en controleren. De basis staat, de belangrijkste stap die nu wordt genomen is om privacy te laten landen in het DNA van de medewerker.

Privacy is niet langer 'extra' werk, maar wordt geïncorporeerd in alle werkzaamheden. Dit vraagt voortdurende inzet van alle betrokkenen. Ook betekent dit dat privacy geen 'afvinklijst' moet zijn, maar opgenomen wordt in een plan-do-check-act cyclus. Het is niet voldoende om een verwerkersovereenkomst af te sluiten, maar de uitvoering van de voorwaarden die daarin gesteld worden, moeten met enige regelmaat nagegaan worden. Het is niet voldoende om met een DPIA privacyrisico's vast te stellen, deze risico's moeten ook op planmatige wijze gemitigeerd worden. Het is niet voldoende om eenmalig het register van verwerkingen te vullen, dit register moet bij iedere aanpassing van een proces gecontroleerd en zo nodig aangevuld worden.

In deze jaarrapportage wordt een overzicht gegeven van de belangrijkste privacy-ontwikkelingen binnen de provincie en worden aanbevelingen gegeven voor de doorontwikkeling. Veel van deze aanbevelingen richten zich niet alleen tot de privacy officers, maar juist ook tot teamleiders en medewerkers. Privacy is immers ieders verantwoordelijkheid. Laten we gezamenlijk het motto van het programma informatieveiligheid en privacy naleven:

'WIJ MAKEN DE PROVINCIE UTRECHT IEDERE DAG VEILIGER!'

STEFANIE KELTERMAN,
Functionaris voor Gegevensbescherming.

ORGANISATIEBREED

1. CIP SELF ASSESSMENT

De AVG stelt regels over privacy waaraan ook de provincie Utrecht moet voldoen. De AVG is een Europese verordening met weinig concrete resultaatverplichtingen. In de tekst van de verordening staan veel aanduidingen als ‘de verantwoordelijke treft voldoende technische en organisatorische maatregelen om gegevens te beschermen’. Het is dan aan de organisatie om te bepalen wat ‘voldoende’ is. Deze vage termen zijn nodig om de verordening ‘techniekonafhankelijk’ te maken; de ontwikkelingen in de techniek gaan sneller dan een verordening aangepast kan worden. Tegelijkertijd is het daarmee onmogelijk om de eenvoudige vraag ‘voldoet de provincie Utrecht aan de AVG?’ te beantwoorden. Daarvoor moet eerst bepaald worden wanneer de provincie voldoende waarborgen heeft getroffen.

a. Volwassenheidsniveaus CIP

Om die reden heeft het Centrum Informatiebeveiliging en Privacy (CIP) een systeem beschreven van verschillende volwassenheidsniveaus met de bijbehorende maatregelen. Dit systeem helpt organisaties te groeien naar het volwassenheidsniveau dat past bij de visie en de missie van de organisatie ten aanzien van de privacybescherming. Er worden 5 volwassenheidsniveaus onderscheiden, grofweg van geen of versnipperde aandacht voor privacy, tot perfecte organisatiebrede beheersing en benutting van de privacybescherming. Een niveau geeft daarbij de mate aan, waarin de 'organisatie van privacy' is gesystematiseerd en geïnternaliseerd in de organisatie.
Het CIP geeft aan dat op voorhand niveau 3 een redelijk volwassenheidsniveau is voor organisaties die persoonsgegevens verwerken. Het is doorgaans voldoende om de compliance-toets te doorstaan en het is ook een niveau dat voor grotere en kleinere organisaties alleszins haalbaar is.
De provincie Utrecht heeft zich tot doel gesteld te groeien naar volwassenheidsniveau 3. Binnen de provincie worden immers zeker persoonsgegevens verwerkt. Waarbij ook gevoelige of bijzondere persoonsgegevens zijn, zoals personeelsgegevens, camerabeelden en BIBOB-gegevens. De provincie kent echter niet een grootschalige verwerking van zeer gevoelige gegevens, zoals bijvoorbeeld de politie. Volwassenheidsniveau 3 is daarmee proportioneel.
Opgemerkt wordt dat het behalen van het gestelde volwassenheidsniveau niet betekent dat het daarna ‘klaar’ is. Om dit niveau te handhaven is continu aandacht en inzet nodig om ontwikkelingen bij te houden.

b. Uitvoering self assessment

Om het huidige volwassenheidsniveau van de organisatie te toetsen heeft het CIP een self assessment ter beschikking gesteld. Hiermee bepaalt een organisatie aan de hand van een vragenlijst het volwassenheidsniveau van de organisatie. Deze vragenlijst is ingedeeld in de hoofdonderwerpen:

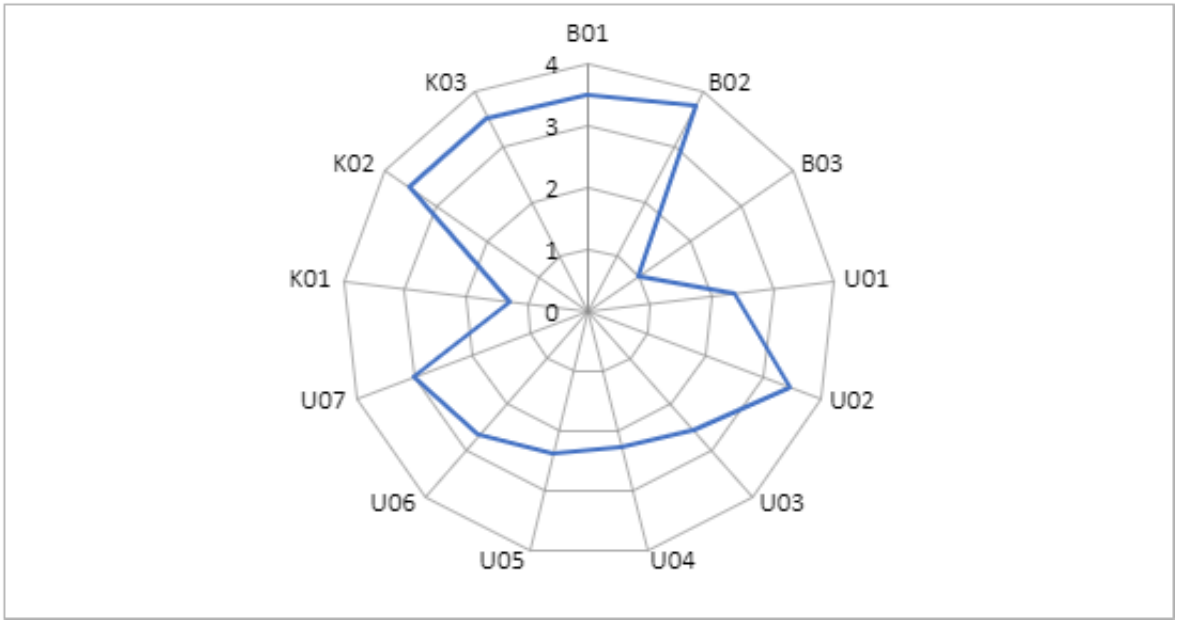
- Privacy Beleid: het beleidsdomein
- Privacy Uitvoering: het uitvoeringsdomein
- Privacy Control: het control- of beheerdomein

Naar aanleiding van de aanbevelingen uit de voorgaande FG-jaarrapportage heeft het programma IV&P besloten om dit self assessment te gebruiken om het volwassenheidsniveau van de provincie op het gebied van privacy doorlopend te meten. In 2021 hebben de privacy officers onder coördinatie van de FG tweemaal een self-assessment uitgevoerd op basis van de privacy baseline van het CIP. Nu dit CIP self assessment niet eerder door de provincie is uitgevoerd is er dit jaar voor gekozen om deze in te vullen met input van alleen de ‘privacydeskudigen’. Zo werd beter inzicht gekregen in de werking van het assessment. Voor komend jaar is het voornemen om hierbij ook teamleiders en andere stakeholders te betrekken.

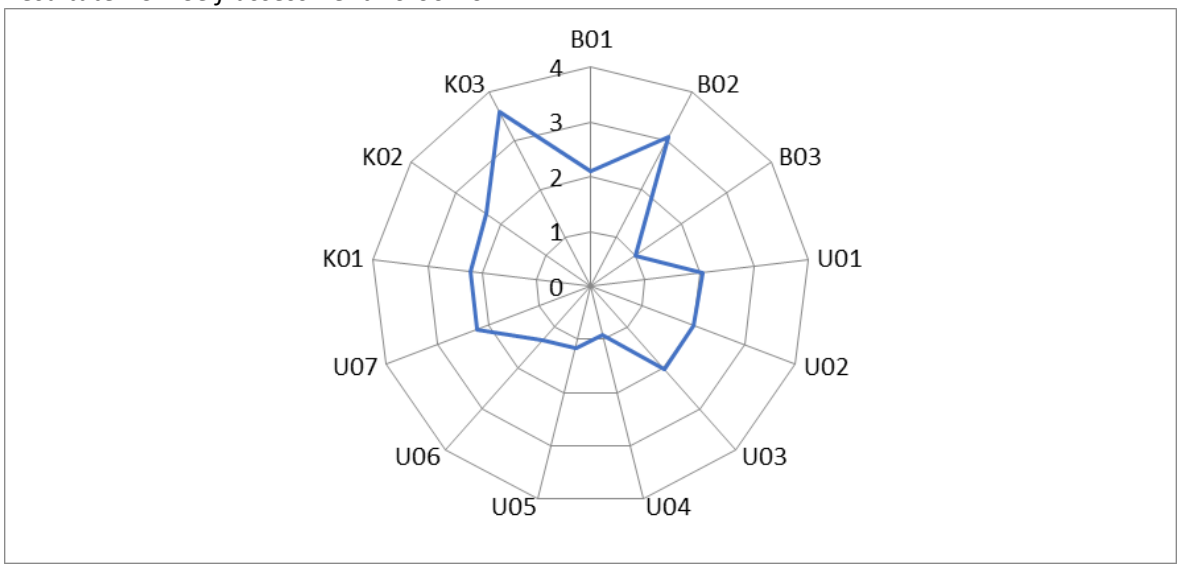
De self-assessments zijn uitgevoerd op 16 juni en 29 november. Hieronder worden de resultaten weergegeven van beide assessments. Bij de meeste onderwerpen is

een (flinke) groei te zien in het assessment van november. Dit wordt enerzijds veroorzaakt door gerichte werkzaamheden naar aanleiding van de resultaten van het eerste assessment. Anderzijds door een minder terughoudende wijze van invullen van het tweede assessment.

Resultaten CIP Self-assessment 29-11-2021



Resultaten CIP Self-assessment 16-06-2021



c. Resultaten CIP Self-assessment per domein

Privacy Beleid: het beleidsdomein	
B.01 Privacy Beleid geeft duidelijkheid en sturing De organisatie heeft beleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen.	
Score 29-11-2021	3.5
Score 16-06-2021	2.1
B.02 Organieke inbedding De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld.	
Score 29-11-2021	3.7
Score 16-06-2021	3.1
B.03 Risicomanagement, Privacy by Design en de GEB[1] De organisatie draagt zorg voor het beoordelen van de privacy risico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen.	
Score 29-11-2021	1.1
Score 16-06-2021	1.0

Privacy Uitvoering: het uitvoeringsdomein	
U.01 Doelbinding gegevensverwerking Doeleinden en rechtvaardigingsgronden van alle verzamelingen en verwerkingen van persoonsgegevens zijn tijdig, welbepaald en uitdrukkelijk omschreven.	
Score 29-11-2021	2.4
Score 16-06-2021	2.1
U.02 Register van verwerkingsactiviteiten Gegevens over de gegevensverwerkingen in een register vastgelegd, waarbij het register een actueel en samenhangend beeld geeft van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.	
Score 29-11-2021	3.5
Score 16-06-2021	2.0
U.03 Kwaliteitsmanagement Kwaliteitsmanagement is ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen.	
Score 29-11-2021	2.6
Score 16-06-2021	2.0
U.04 Beveiligen van verwerking van persoonsgegevens De organisatie treft technische en organisatorische maatregelen voor verwerking van persoonsgegevens op een passend beveiligingsniveau.	
Score 29-11-2021	2.3
Score 16-06-2021	0.9
U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens Bij elke verzameling van persoonsgegevens wordt tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar gesteld, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor de verwerking.	

1 GEB (Gegevensbeschermingseffectbeoordeling) is de Nederlandse vertaling van DPIA (Data protection impact assessment).

Score 29-11-2021	2.4
Score 16-06-2021	1.2
U.06 Bewaren van persoonsgegevens Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.	
Score 29-11-2021	2.7
Score 16-06-2021	1.3
U.07 Doorgifte persoonsgegevens Bij doorgifte aan andere verwerkingsverantwoordelijken zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn er afdoende garanties. Bij de doorgifte naar buiten de EU worden aan strikte criteria gehanteerd.	
Score 29-11-2021	3.0
Score 16-06-2021	2.2

Privacy Control: het control- of beheerdomein	
C.01[2] Intern toezicht Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.	
Score 29-11-2021	1.4
Score 16-06-2021	2.2
C.02 Toegang tot gegevensbewerking voor betrokkenen De organisatie biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.	
Score 29-11-2021	3.5
Score 16-06-2021	2.3
C.03 Meldplicht Datalekken De organisatie meldt een datalek binnen de daaraan gestelde termijn aan de Autoriteit Persoonsgegevens, documenteert de inbreuk, en informeert de betrokkene, indien van toepassing.	
Score 29-11-2021	3.5
Score 16-06-2021	3.6

d. Beoordeling uitkomsten self assessment

Algemeen

Het gewenste volwassenheidsniveau 3 is nog niet over de hele linie bereikt, maar dat er een sterke positieve ontwikkeling plaatsvindt is duidelijk zichtbaar. De grootste uitdagingen liggen kort gezegd op de informatie-uitwisseling tussen de teams en de privacy officers, een risico gerichte benadering van privacy, vroegtijdige betrokkenheid van privacy bij nieuwe ontwikkelingen en op het gebied van informatiebeveiliging.

Binnen de teams vindt de daadwerkelijke verwerking van persoonsgegevens plaats. De meeste kennis over het AVG-proof verwerken van persoonsgegevens bevindt zich bij de privacy officers. In termen van de 3 Lines zijn dit de eerste lijn (de teamleiders als procesverantwoordelijken) en de tweede lijn (de privacy officers als adviserende en ondersteunende krachten). Gebleken is dat het inschakelen van de tweede lijn door de eerste lijn niet is vastgelegd in werkprocessen of dat medewerkers onvoldoende kennis hebben van deze processen. Hierdoor wordt het inschakelen van de privacy officers niet afgedwongen en geëvalueerd. Het inschakelen

2 Er zit een fout in het CIP-model voor dit domein. De letter "C" wordt gebruikt in de nummering van de onderdelen binnen dit domein. In de eerder opgenomen spin-diagrammen wordt echter de letter "K" gebruikt.

van de tweede lijn is afhankelijk van de kennis van de teamleider of collega's, de (toevallige) aanwezigheid van een privacy officer of een FG. Zie hiervoor ook verderop in deze rapportage waarin ik inga op de domeinspecifieke ontwikkelingen.

Daarbij ontbreekt binnen de eerste lijn vaak actieve kennis van organisatiebrede afspraken over het moment waarop de tweede lijn wordt betrokken. Dit verlaagt het volwassenheidsniveau op verschillende onderdelen van het self assessment en brengt risico's mee voor de uitvoering van de processen. Deze risico's bestaan uit de verwerking van persoonsgegevens in strijd met de AVG en de daarbij komende gevolgen van reputatieschade en boetes en risico's die een vertraging van de uitvoering van een voorgenomen proces meebrengen, doordat op een laat tijdstip alsnog een risicoanalyse uitgevoerd moet worden.

Privacy Beleid: het beleidsdomein

Binnen het beleidsdomein is de grootste uitdaging het (tijdig) uitvoeren van DPIA's en andere risicobeoordelingen en de uitvoering van de aanbevelingen die daaruit volgen. Zoals ook is aangegeven in de tussentijdse rapportage van september 2021 is in december 2020 een uitvraag gedaan naar hoog risico processen. Voor de uitvoering van de risicobeoordelingen is veelal de samenwerking gezocht met het programma 'de Wasstraat' en met het traject dat Informatieveiligheid is aangegaan met bureau Verdonck, Klooster & Associates om risicobeoordelingen op de informatieveiligheid uit te voeren. Beide samenwerkingen hebben echter in plaats van versnelling, gezorgd voor vertraging van het proces. Eind 2021 is daarom besloten om de uitvoering van de DPIA's niet meer te laten beïnvloeden door deze samenwerkingen. Door de privacy officers worden aan de hand van een stocklist DPIA's uitgevoerd, onder meer op volgorde van risico. Daarbij wordt voor al afgenomen DPIA's bepaald of er aanleiding is deze aan te passen of opnieuw uit te voeren.
Een tweede uitdaging is het tijdig betrokken worden voor een risicobeoordeling. Het is de verantwoordelijkheid van de procesverantwoordelijke om een DPIA uit te laten voeren onder begeleiding van een privacy officer, voorafgaand aan de start van een proces of project. Het komt echter regelmatig voor dat hier pas op het allerlaatste moment om wordt gevraagd of zelfs dat via vragen of via de media wordt ontdekt dat de provincie een proces of project met een zeker privacyrisico uitvoert. Dat dan alsnog onder hoge druk een DPIA uitgevoerd moet worden is voor alle betrokkenen onwenselijk.

Ten slotte ziet de organisatie de DPIA nog als 'het zetten van een vinkje'. Maar als de DPIA is afgerond begint vaak pas het echte werk. Er is met de DPIA immers slechts in kaart gebracht waar risico's zich bevinden en welke maatregelen deze risico's kunnen mitigeren. Het is dan vervolgens aan de procesverantwoordelijke om deze maatregelen tijdig uit te voeren. Dit vraagt vaak een plan van aanpak. Belangrijk is daarbij om organisatiebrede afspraken te maken over het toezicht op de naleving van de maatregelen. Dit is een onderwerp dat terugkomt in het FG-toezichtsplan.

Privacy Uitvoering: het uitvoeringsdomein

Voor de resultaten ten aanzien van het uitvoeringsdomein is een terugkerend item dat de juiste werkzaamheden (meestal) wel plaatsvinden, maar onvoldoende geborgd zijn. Wanneer enige vorm van risicoanalyse plaatsvindt wordt gekeken naar doel, grondslag, dataminimalisatie en overige onderwerpen die relevant zijn voor de uitvoering. Zoals eerder al opgemerkt, is het initiatief tot het doen van een DPIA (of andere risicoanalyse) of het afsluiten van een verwerkersovereenkomst te veel afhankelijk van eventuele kennis en inzet van de procesverantwoordelijke of zelfs van binnengekomen vragen of klachten.
Dit vraagt niet slechts een vastlegging van werkprocessen op papier, maar het doordringen van deze werkafspraken in de werkwijze van alle medewerkers.
Dit geldt ook voor het verwerkingsregister. De grootste uitdaging is om het register compleet

te krijgen Deze informatie moet vanuit de eerste lijn aan de privacy officers worden aangeleverd. Alleen de eerste lijn zelf weet immers welke processen en projecten er uitgevoerd worden. De privacy officers ondersteunen hierin door uitvragen te doen naar de volledigheid en actualiteit van de gegevens.

Een concreet risico vormt het beperkte inzicht in risico's op het gebied van informatieveiligheid. Informatieveiligheid vormt een zelfstandig onderdeel binnen de provincie, maar heeft veel invloed op het volwassenheidsniveau op het gebied van privacy. De AVG stelt immers de voorwaarde dat – onder meer – voldoende technische maatregelen worden getroffen om persoonsgegevens te beschermen. In de samenwerking met informatieveiligheid is meermaals gebleken dat het inzicht in beveiligingsrisico's onvoldoende is. Zo is er nog altijd geen sluitend advies gekomen over de vraag of SharePoint – de samenwerkingstool die de provincie gebruikt voor het overgrote deel van haar processen – voldoende veilig is om hiervoor te gebruiken. Het hierna beschreven datalek met SharePoint wijst dan ook in tegengestelde richting.

Privacy Control: het control- of beheerdomein

Ten aanzien van control C.01: de score van 29-11 (1.4) is veel lager dan de score van 16-6 (2.2). We hebben niet kunnen achterhalen door welk onderdeel deze achteruitgang met name wordt veroorzaakt. Een verklaring kan zijn dat het onderdeel op 16-6 te positief is beoordeeld. De beoordeling van 29-11 lijkt realistisch te zijn.

Binnen het control domein is met name het intern toezicht een aandachtspunt. Het intern toezicht heeft tot doel vast te stellen of de gegevensverwerkingen rechtmatig zijn en of daarvoor de juiste maatregelen zijn getroffen, zodat voldaan wordt aan de privacy-eisen.

Toezicht is mogelijk doordat vanuit de uitvoering wordt gerapporteerd over hoe aan de wettelijke vereisten wordt voldaan en welke technische en organisatorische maatregelen daarvoor zijn genomen. Bevindingen vormen de input voor het compliance proces, zodat de verwerking van de persoonsgegevens kan worden bijgestuurd, al dan niet door het bijstellen of uitbreiden van het beleid. Bevindingen kunnen het gevolg zijn van veranderde wet- en regelgeving, nieuwe inzichten, ambities of ervaringen.

Uit gesprekken met medewerkers en teamleiders is gebleken dat binnen de provincie Utrecht (nog) onvoldoende sprake is van een cultuur gericht op meten, evalueren en (continue) verbeteren. Daarbij heeft de focus binnen het privacyteam het afgelopen jaar vooral gelegen op het opstellen en initiëren van beleids- en werkdocumenten en niet zozeer op het monitoren, evalueren en verbeteren. Dit geldt ook voor verwerkersovereenkomsten en DPIA's: de focus lag op het opstellen en minder op de controle op de naleving en de evaluatie ervan.

Dit alles leidt tot een (te) laag volwassenheidsniveau. Komend jaar zal de stap gezet moeten worden van de opzet en bestaan van privacy naar de werking: een cyclisch en zelflerend proces. Deze omslag vraagt inzet vanuit alle lagen binnen de organisatie. Er zal immers informatie uit de teams moeten komen, toezicht vanuit management en weer verbeteringen vanuit de teams. Het management zal hierop cyclisch moeten sturen.

2. DATALEKKEN, KLACHTEN EN UITOEFENING VAN RECHTEN VAN BETROKKENEN

a. Datalekken

In 2021 zijn 24 incidenten gemeld bij de privacy officers als mogelijk datalek. 9 van deze incidenten zijn gemeld bij de betrokkene(n) omdat er een risico was voor de privacy van betrokkenen én het niet onevenredig belastend was om betrokkenen te bereiken en te informeren.
4 meldingen hebben geleid tot een melding datalek bij de Autoriteit Persoonsgegevens.

Deze meldingen zijn alle gedaan binnen de gestelde termijn van 72 uur na ontdekking. De Autoriteit Persoonsgegevens heeft geen contact opgenomen voor nadere informatie en ook is er geen nader onderzoek gedaan.
De gemelde datalekken zijn terug te voeren op de volgende gedragingen:

- Verkeerd gebruik van e-mail (cc in plaats van bcc of verkeerde geadresseerde);
- Abusievelijke publicatie van persoonsgegevens op internet
- Verwisseling van naar rechtbank verstuurd papieren dossier
- Mogelijke toegang tot geheim overleg via Teams
- Gestolen/vermiste laptop of telefoon
- Hack van (mogelijke) samenwerkingspartner
- Documenten geplaatst in SharePoint waartoe iedere medewerker toegang had
- Kwetsbaarheid in Java-software

CERT

In 2021 is een Computer Emergency Response Team (CERT) opgericht. Het CERT is een crisisteam dat bijeengeroepen wordt wanneer sprake is van een digitaal impactvolle situatie. In Q4 2021 is het CERT 2 maal bijeengeroepen. Hieronder een nadere beschrijving van die situaties.

Datalek SharePoint
Door een ICT-specialist van de provincie is begin november 2021 ontdekt dat in de digitale samenwerkomgeving (Teams/SharePoint) gevoelige documenten via de algemene zoekfunctie gevonden en gelezen konden worden door alle medewerkers van de provincie. Het ging onder meer om medewerkersgegevens en gevoelige college-informatie.

De inschatting was dat dit een omvangrijk datalek betrof. Daarom is het CERT bijeengeroepen. Vervolgens zijn de volgende acties gestart:

- De leesrechten van de groep ‘alle medewerkers PU’ zijn van alle open Sharepointsites gehaald, waardoor de gevoelige informatie uitsluitend nog leesbaar was voor de leden van de SharePoint site;
- De Autoriteit Persoonsgegevens is geïnformeerd over een mogelijk datalek;
- Er is onderzoek gedaan naar onbevoegde raadpleging van documenten die ten onrechte openbaar stonden.

Hoe heeft deze situatie kunnen ontstaan?
Uit onderzoek is gebleken dat de documenten openbaar hebben gestaan doordat medewerkers die documenten ten onrechte op een open Digitale Samenwerkomgeving (Teams) site hebben geplaatst. Bij de aanvraag van een Teams site wordt met de eigenaar besproken of deze site open of gesloten moet zijn. Wanneer de site open is kunnen alle leden van de site documenten plaatsen en bewerken, maar alle overige medewerkers van de provincie kunnen documenten ook lezen (niet bewerken). Er is echter gebleken dat medewerkers niet altijd weten of een site open of gesloten is. Daarom zijn er vertrouwelijke documenten op open sites geplaatst.

Er is door de privacy officers steekproefsgewijs onderzoek gedaan naar geraadpleegde documenten. Daarin is niet aantoonbaar gebleken dat er documenten ingezien zijn door ‘onbevoegden’, maar dit kan ook niet uitgesloten worden.
De medewerkers zijn hierover geïnformeerd. Zij zijn gevraagd alert te blijven en zij zijn gewezen op de gedragscode, waarin is opgenomen dat een medewerker die vertrouwelijke informatie onder ogen komt, deze geheim houdt.

Daarnaast is versneld gewerkt aan de uitrol van zogenaamde ‘vertrouwelijkheidslabels’. Hierdoor wordt op iedere Teams site zichtbaar hoe open of gesloten die site is.

Kwetsbaarheid Javascript LOG4J
Half december 2021 werd wereldwijd gecommuniceerd over een kritieke kwetsbaarheid in Apache Log4j. Apache Log4j is een softwareproduct dat wordt gebruikt voor het vastleggen van meldingen in software. Het wordt onder andere gebruikt

voor het vastleggen van inlogpogingen maar de software zit daarnaast in vele honderden, zo niet duizenden softwareproducten en applicaties. Het gevolg hiervan was dat er wereldwijd werd gescand naar kwetsbare systemen.

Om de kwetsbaarheid af te dichten werden vanuit JAVA updates uitgegeven. Enkele van die opvolgende updates bleken echter ook kwetsbaarheden te bevatten. Daarom heeft het enige tijd geduurd voordat vastgesteld kon worden dat de software geen kwetsbaarheden meer bevatte.
De provincie heeft dit incident serieus opgepakt. Het CERT is bijeengeroepen en ook is interprovinciaal nauw samengewerkt. Omdat bij aanvang niet duidelijk was of er ook bij de provincie misbruik was gemaakt van deze kwetsbaarheid is een melding bij de Autoriteit Persoonsgegevens gedaan.

De grootste uitdaging lag in de controle van de leveranciers waarmee de provincie samenwerkt. Door hen moest bevestigd worden dat zij de laatste update hadden doorgevoerd. Er bleek echter binnen de provincie geen sluitend overzicht te bestaan van applicaties die door de provincie in gebruik zijn en evenmin over wie verantwoordelijk is voor het beheer van dat overzicht. Hierdoor is serieuze vertraging ontstaan in de aanpak van het incident.
Begin 2022 is het CERT afgeschaald en zijn lopende zaken overgedragen aan een werkgroep.

b. Klachten

Betrokkenen kunnen, als zij van mening zijn dat de verwerking van hen betreffende persoonsgegevens inbreuk maakt op de AVG, een klacht indienen bij de FG, alvorens hierover de Autoriteit Persoonsgegevens te benaderen. De FG ziet toe op de afhandeling van de klacht van de betrokkenen.
In 2021 zijn geen klachten ingediend als hiervoor bedoeld.

c. Rechten van betrokkenen

In 2021 zijn 3 verzoeken binnengekomen om inzage in de eigen persoonsgegevens. Volgens de AVG heeft iedereen het recht om een organisatie te vragen welke persoonsgegevens van de verzoeker worden verwerkt. De provincie heeft – in tegenstelling tot bijvoorbeeld gemeenten – weinig rechtstreeks contact met burgers. Hierdoor is het aantal inzageverzoeken de afgelopen jaren zeer laag geweest (sinds 2018 zijn slechts 3 verzoeken binnengekomen). Deze inzageverzoeken waren echter afkomstig van eigen medewerkers en zagen op het verstrekken van hun persoonsgegevens aan derde partijen voor het naar het huisadres toesturen van presentjes.

Deze verzoeken zijn – na onderzoek binnen de organisatie – beide tijdig afgedaan. Daarbij is binnen de organisatie aandacht gevraagd voor het gebruik van persoonsgegevens voor dit doeleinde.

3. IV&P CONTACTPERSONEN

Informatieveiligheid en Privacy zijn onderwerpen die de hele organisatie aangaan. Alleen als iedere medewerker scherp is op het naleven van privacyregels, zorgvuldig omgaat met informatie en tijdig de hulp inroept van een deskundige kunnen we als organisatie veilig ons werk doen.

Het programma Informatieveiligheid en Privacy ondersteunt daarin, maar kan vanzelfsprekend niet overal in de organisatie aanwezig zijn. Daarom is in 2021 gebouwd aan een netwerk van contactpersonen IV&P. Zij zijn extra ogen en oren om knelpunten te melden en extra monden om tips en aanwijzingen binnen de organisatie te verspreiden.

Vanuit het programma IV&P worden de contactpersonen IV&P iedere maand uitgenodigd voor een informatieve sessie van max. 1 uur. Tijdens deze sessie worden de contactpersonen meegenomen in relevante ontwikkelingen op het gebied van informatieveiligheid en privacy. Daarnaast kunnen de contactpersonen met elkaar delen welke vragen en uitdagingen er binnen de teams zijn en krijgen zij tips en aanbevelingen mee om te delen binnen de teams.

De sessie met de contactpersonen zijn interessant, omdat daar zaken naar voren komen die via de reguliere weg vaak nog niet bij de juiste personen van IV&P terecht zijn gekomen. Aandachtspunten zijn de aanwezigheid van de contactpersonen en de terugkoppeling die zij in hun team geven. De (digitale) opkomst van de contactpersonen is wisselend. Daarbij zijn enkele vaste deelnemers, maar ook enkele contactpersonen die bijna iedere sessie verstek laten gaan en ook geen vervanger regelen. Dit zorgt voor een kennisachterstand voor het hele team.

Zoals ook hierna zal blijken uit de domeinspecifieke informatie, geven lang niet alle contactpersonen terugkoppeling van hetgeen besproken wordt in de sessies. Dit doet afbreuk aan het doel dat het kennisniveau van de hele organisatie verhoogd zou worden door de contactpersonen.

4. EVALUATIE STATUUT GEGEVENSBESCHERMING

Op 2 juli 2019 is door Gedeputeerde Staten besloten tot vaststelling van een Statuut Gegevensbescherming (hierna: Statuut) voor de provincie Utrecht. In het Statuut worden de taken, verantwoordelijkheden en bevoegdheden van de functionaris gegevensbescherming (FG) zoals vastgelegd in artikel 13b van het Organisatiebesluit provincie Utrecht 2004, nader uitgewerkt. Daarnaast wordt ingegaan op de functionele relatie met andere functionarissen die een rol spelen bij de bescherming van persoonsgegevens. Tijdens deze vergadering heeft GS ook besloten tot evaluatie van het statuut in 2021.

Deze opdracht is extern uitgezet. In december 2021 heeft VKA een evaluatie van het Statuut uitgevoerd op basis van de volgende onderzoeksvragen:

- In hoeverre geeft het Statuut voldoende richting aan de verdeling van taken, verantwoordelijkheden en bevoegdheden m.b.t. de naleving van de AVG?
- In hoeverre geeft het Statuut voldoende invulling aan de wettelijke vereisten vanuit de AVG voor de rol van de functionaris gegevensbescherming?
- In het Statuut zijn drie Lines of Defense geformuleerd. Is dit een werkend systeem?
- Is de aansluiting van de bepalingen in het Statuut op de bepalingen in het privacybeleid optimaal?
- Is er sprake van onnodige overlap of strijdigheden tussen de hiervoor genoemde documenten?

De resultaten van deze evaluatie worden in Q1 van 2022 opgeleverd. De diverse gremia zullen hier separaat over worden geïnformeerd.

STAND VAN ZAKEN DOMEINEN

Het verwerken van persoonsgegevens in lijn met de AVG is een verantwoordelijkheid van de gehele organisatie. De ondersteuning door de privacy officers is uitsluitend effectief wanneer men binnen de teams de eigen verantwoordelijkheden kent en uitvoert. Om een beeld te krijgen van de kennis en de uitvoering binnen de teams is daarom voorafgaand aan het opstellen van deze jaarrapportage een korte vragenlijst uitgezet naar iedere teamleider en opgavemanager. In deze vragenlijst werden vragen gesteld over de wijze waarop privacy een plek heeft in de werkprocessen.

De bereidheid om de vragenlijst in te vullen was groot, vooral onder de teamleiders. Van de opgavemanagers heeft ongeveer de helft de vragenlijst ingevuld. Van hen kwamen veel vragen over hun verantwoordelijkheden ten aanzien van de AVG en de vraag of zij überhaupt persoonsgegevens verwerken. Hier ligt duidelijk een informatievraag voor het management in samenwerking met de privacy officers.

1. RESULTATEN

a. Verwerkingsregister

Alle processen waarin persoonsgegevens worden verwerkt, moeten worden opgenomen in het Verwerkingsregister van de provincie. Dit register is sinds begin november 2021 online in te zien. De teamleider is verantwoordelijk voor de juistheid en compleetheid van de verwerkingen in het register die zijn team uitvoert. Met ingang van Q2 2022 zullen de privacy officers enkele keren per jaar vragen aan de teamleiders om het register te controleren en aanvullingen en wijzigingen door te geven. Vooruitlopend hierop is de teamleiders gevraagd of zij hun verwerkingen al hebben bekeken in het register.

Vraag: Heb je dit jaar de verwerkingen van jouw team in het Verwerkingsregister gecontroleerd?

Ondanks dat de link naar het register in de vraag stond, geeft ongeveer de helft van de respondenten aan nog niet in het register gekeken te hebben. Dit is een (te) groot aantal. Een teamleider is verantwoordelijk voor de juistheid en de volledigheid van de gegevens in het register. Wanneer het register niet up-to-date is brengt dit risico's mee voor de organisatie. Niet alleen heeft de organisatie dan zelf geen goed inzicht in de processen (en eventuele omissies), maar ook bestaat het risico dat de Autoriteit Persoonsgegevens inzage vraagt in het register en concludeert dat dit niet actueel is. Dit is een boetewaardige overtreding van de AVG.

Hierbij kunnen wel twee kanttekeningen worden geplaatst. Ten eerste stond het register ten tijde van de uitvraag slechts 3 maanden online, waardoor een deel van de teamleiders er wellicht nog niet aan toegekomen was om hiernaar te kijken. Ten tweede is er begin 2021 door de privacy officers een volledige controleslag uitgevoerd over het verwerkingsregister, waarbij iedere teamleider gevraagd is om naar zijn/haar eigen processen te kijken. Dit waren echter toegestuurde Excelbestanden. Het is mogelijk dat teamleiders dit niet meenemen in hun antwoord op deze vraag. Eenzelfde uitvraag over een jaar zal meer duidelijkheid geven over de bereidheid van de eerste lijn om eigen processen in te zien.

b. Risicoanalyses

Om privacyrisico's in kaart te brengen is het belangrijk dat er risicoanalyses worden uitgevoerd in de vorm van een BIA (Business impact analyse), eventueel gevolgd door een DPIA (data protection impact assessment). Dit jaar zijn ook (voorbereidingen van) risicoanalyses uitgevoerd door de Wasstraat

en Bureau VKA. Aan de teamleiders is de vraag gesteld of er in 2021 binnen het team risicoanalyses privacy of informatieveiligheid zijn uitgevoerd en zo ja, voor welke processen.

Vraag: Zijn er dit jaar binnen jouw team risico-analyses privacy of informatieveiligheid uitgevoerd?

Zoals ook al bleek uit de eigen waarneming geeft een groot deel van de teams aan dat er geen risicoanalyse is uitgevoerd, maar dat dit wel nodig is. Dit benadrukt de noodzaak om vaart te zetten achter de uitvoering van risicoanalyses. Ook is belangrijk om na te gaan of de vrij omvangrijke groep die aangeeft dat een risicoanalyse niet nodig is, voldoende op de hoogte is van de regels en afspraken over de noodzaak van het uitvoeren van een risicoanalyse.

Uit controle van de opgegeven, uitgevoerde risicoanalyses door de privacy officers bleek dat bijna alle teamleiders goed op de hoogte zijn van wat als 'risicoanalyse' wordt gezien.

c. Privacy by design

Binnen de provincie werken we volgens het beginsel 'privacy by design'. Dit betekent dat al bij de opstart van een proces, project of samenwerking gekeken wordt naar de bescherming van de privacy van betrokkenen. Op die manier richten we onze processen privacyvriendelijk in en hoeven de privacy officers en de FG niet als 'noodrem' te fungeren.
Om inzicht te krijgen in hoeverre dit principe is geborgd binnen de teams is de vraag gesteld op welke manier is geborgd dat advies wordt gevraagd aan een privacy officer bij de start van een project, proces of samenwerking waarbij persoonsgegevens zijn betrokken.

De antwoorden op deze (open) vraag waren divers, maar hadden voor een groot deel dezelfde strekking: in beginsel is er zeker de intentie om privacy te betrekken bij nieuwe processen en projecten, maar het ontbreekt aan bekendheid met een gedocumenteerd en gecontroleerd proces. Weliswaar zijn afspraken beschreven op intranet en vastgelegd in een DPIA-procesbeschrijving, maar de bekendheid hiermee is zeer beperkt, evenals de naleving.
In bredere zin is de i-governance onvoldoende ingeregeld over de breedte van de organisatie. Weliswaar worden verantwoordelijkheden hieromtrent bij de teamleiders neergelegd, maar de naleving hiervan wordt onvoldoende afgedwongen.

'Bij mijn weten is daar geen standaard procedure/borging voor'

'Waar nodig wordt dit per project aangevraagd'

'Via goed opdrachtgeverschap'

Het risico dat dit meebrengt is dat het inschakelen van een privacy officer te veel afhangt van de kennis van een of enkele personen. Een goed ingewerkte teamleider zal zijn medewerkers hierop wijzen, maar deze werkwijze vervalt zodra de teamleider (of andere geïnformeerde medewerker) wordt vervangen. Dat hier nog geen sprake is van een sluitend proces is het afgelopen jaar verschillende keren ervaren, wanneer via vragen van binnen of buiten de organisatie processen naar voren kwamen die in het geheel niet bekend waren bij de privacy officers.

d. Verwerkers- en dataleveringsovereenkomsten

Wanneer de provincie persoonsgegevens wil uitwisselen met een partij buiten onze eigen organisatie, moeten hierover goede afspraken worden gemaakt. Deze worden opgenomen in een verwerkersovereenkomst of een dataleveringsovereenkomst. De privacy officers kunnen ondersteunen bij het

opstellen van deze overeenkomsten, maar de teamleiders zijn er verantwoordelijk voor dat de overeenkomst tijdig wordt afgesloten.

Daarom is de vraag gesteld hoe binnen het team is geborgd dat bij uitwisseling van persoonsgegevens een verwerkersovereenkomst of dataleveringsovereenkomst wordt afgesloten.

De antwoorden hierop zijn vergelijkbaar met de antwoorden op de vraag over privacy by design. Er is bewustzijn over de verplichting om verwerkers- of dataleveringsovereenkomsten af te sluiten, maar een geborgd en gecontroleerd proces ontbreekt. Ook wordt team Inkoop genoemd als borging voor het afsluiten van verwerkers- en dataleveringsovereenkomsten. Uit de informatie van team Inkoop blijkt echter dat zij slechts inkoopprocessen begeleiden wanneer sprake is van overschrijding van de Europese aanbestedingsgrens. Daarbij geven zij aan wel te wijzen op de verplichting van het afsluiten van een verwerkersovereenkomst, maar niet verantwoordelijk te zijn voor de nakoming daarvan.

'Het bewustzijn is wel gegroeid, collega's vragen soms zelf 'of er niet iets moet'. Maar dat is geen 100% dekking'

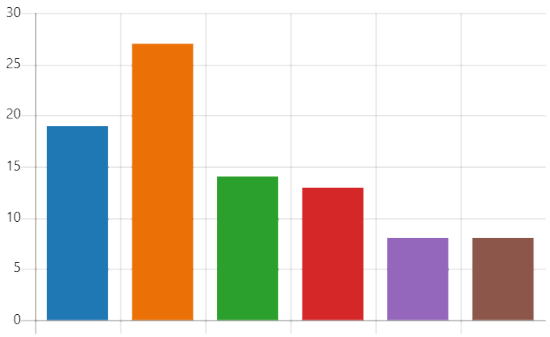
'Kennis erover delen, daarnaast weet ik er genoeg van om dit soort processen te herkennen'

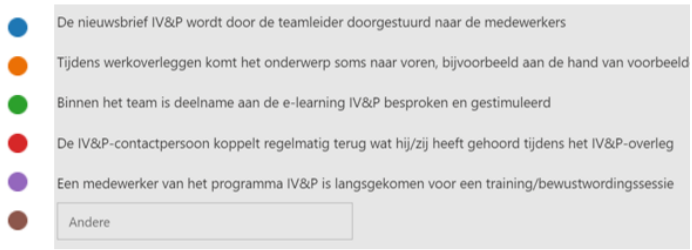
'Inkoop neemt dit op in overeenkomsten en communiceert dit met leveranciers'

Wanneer voor een uitwisseling van gegevens ten onrechte geen verwerkers- of dataleveringsovereenkomst wordt afgesloten, ontstaat een onwenselijke situatie. De provincie blijft immers verantwoordelijk voor de verwerking van de persoonsgegevens, ook als dat gebeurt door een derde partij. Mocht er nu bij die derde partij een datalek ontstaan of anderszins niet zorgvuldig worden omgegaan met de persoonsgegevens, dan wordt de provincie hierop aangesproken. Zowel door de toezichthouder (met risico op een boete) als door de media (met risico van reputatieschade). Afspraken over het veilig verwerken van persoonsgegevens en controle daarop verkleinen die risico's aanzienlijk.

e. Bewustwording

Vanuit het programma IV&P worden veel bewustwordingsactiviteiten aangeboden. Hiermee wordt de teamleider ondersteund in zijn rol. De teamleider heeft een eigen verantwoordelijkheid om het onderwerp privacy onder de aandacht van zijn/haar medewerkers te brengen. Aan de teamleider is de vraag voorgelegd op welke manier er binnen het team aandacht is besteed aan bewustwording op het onderwerp privacy.





Het is goed om te zien dat 27 van de respondenten aangeeft het onderwerp privacy te bespreken in het werkoverleg. Wanneer privacy een regulier terugkerend onderwerp is binnen het team, volgen andere onderdelen zoals het betrekken van een privacy officer of het afsluiten van een verwerkersovereenkomst, vanzelf.

Het stimuleren van deelname aan de e-learning IV&P wordt relatief weinig gedaan. Dit is zorgwekkend, ook gelet op het feit dat het CMT ervoor gekozen heeft deelname hieraan niet verplicht te stellen. Deze combinatie zou ertoe kunnen leiden dat het deelnamepercentage aan de e-learning laag blijft. Dit zal komende tijd blijken uit de deelnamecijfers.

Ook de beperkte terugkoppeling van de IV&P-contactpersonen is een punt van aandacht. Het netwerk van IV&P-contactpersonen is in het leven geroepen om op een laagdrempelige manier een groot deel van de organisatie te bereiken. Wanneer IV&P-contactpersonen de opgedane kennis echter niet delen met hun eigen team, wordt dat doel niet bereikt. Dit beeld wordt versterkt door een aanvullende vraag van een van de teamleiders. Hij vroeg om terugkoppeling van hetgeen tijdens de contactsessies is gedeeld met de contactpersonen IV&P en was zich er blijkbaar niet van bewust dat dit nu juist de taak is van de IV&P-contactpersoon.

CONCLUSIES & AANBEVELINGEN

Mijn eerste volledige kalenderjaar als FG van de provincie Utrecht is achter de rug. En ondanks dat ik de meeste collega's nog nooit in levenden lijve heb gezien, heb ik wel het idee dat ik de organisatie op privacygebied goed heb leren kennen. Wat ik zie is dat er binnen de organisatie steeds meer bewustwording is van de noodzaak om zorgvuldig om te gaan met privacy. Datalekken en andere incidenten die in de media worden beschreven dragen hieraan bij. Tegelijkertijd is de kennis van hoe die privacy moet worden beschermd vaak niet toereikend. Onbekend maakt onbemind, dus bestaat het risico dat de stap naar de privacy officers niet wordt gemaakt. En dat brengt risico's mee.

Risico's die zich uiten in vragen of zelfs klachten van medewerkers en burgers. Want waarom staat er een camera van de provincie gericht op de weg waarlangs ik iedere dag naar mijn werk rijd? Of waarom wordt mijn privéadres gedeeld met commerciële instellingen? Leerzame trajecten voor alle betrokkenen. Maar beter om deze te voorkomen door tijdig advies te vragen van een deskundige.

In de voorbereiding op deze rapportage is aan de teamleiders en opgavemanagers gevraagd om input. Dit om te voorkomen dat er een te eenzijdig beeld zou worden geschetst. Dit gaf interessante antwoorden en reacties. Zoals hiervoor beschreven kwamen de opmerkingen van de teamleiders vaak overeen met hetgeen we al vanuit het programma hadden geconstateerd. Het is goed om een vermoeden zo onderbouwd te zien.

In Q3 2021 heb ik een tussentijdse rapportage opgeleverd. De afspraak om tussentijds te rapporteren is gemaakt om een meer doorlopend beeld te geven van de privacyontwikkeling. In die tussentijdse rapportage is ook een heel aantal aanbevelingen gegeven. Nu er niet heel veel tijd is verstreken tussen het opleveren van de tussentijdse rapportage en deze jaarrapportage is het logisch dat niet alle aanbevelingen al zijn uitgevoerd. Ik heb daarom hierna een overzicht opgenomen van de aanbevelingen uit de tussentijdse rapportage, de voorgenomen opvolging uit de managementreactie en de stand van zaken naar mijn inzicht.

Om de organisatie niet te overvoeren met aanbevelingen en de al gegeven aanbevelingen nog altijd relevant zijn, laat ik het bij die aanbevelingen.

Daarbij herhaal ik de boodschap die ik meermaals heb gegeven in deze rapportage, dat privacyvolwassenheid alleen kan groeien wanneer dit onderwerp door de hele organisatie heen wordt omarmd. Wanneer iedere medewerker de juiste verantwoordelijkheid voelt voor dit onderwerp, bereiken wij de gewenste volwassenheid. Ik doe daarbij een concrete oproep aan het management om te sturen op deze verantwoordelijkheid, daarbij ondersteund door de deskundigen op dit gebied.

FEBRUARI 2021
Stefanie Kelterman,
Functionaris voor gegevensbescherming

Aanbevelingen rapportage september 2021	Opvolging volgens managementreactie	Conclusie FG
Datalekken		
Organiseer op korte termijn een bewustwordingscampagne gericht op het juiste gebruik van e-mail.	Extra aandacht voor juist gebruik van de e-mail zal in de communicatiekalender worden opgenomen.	Onderwerp is opgenomen op communicatiekalender zonder prioriteit.
Richt het proces melden datalekken zo in dat de leidinggevende altijd terugkoppelt op welke wijze de organisatie heeft geleerd van het datalek.	Bij de volgende evaluatie van het datalekproces (eind 2021) zal dit onderwerp worden meegenomen, daarnaast zou het goed zijn als datalekken worden vertaald naar organisatiebrede activiteiten voor bewustwording.	Nog geen zichtbare actie
Bespreek gemelde datalekken (geanonimiseerd) met het organisatiebrede netwerk van privacy-contactpersonen.	Dit wordt op de lijst met te bespreken onderwerpen met de contactpersonen gezet.	Grote datalekken (SharePoint en Log4J) zijn besproken met contactpersonen.
Register van verwerkingen		
Verken de mogelijkheden voor een tool om het register van verwerkingen in bij te houden. Zo'n tool zorgt voor eenduidigheid in het vullen (door vaste velden), is toegankelijker voor teamleiders en medewerkers en maakt het eenvoudiger om managementinformatie te genereren en zo het hogere management beter te betrekken.	Het gebruik van een tool voor het beheer van het register is zeker een ontwikkeling waarnaar wordt gekeken. Op dit moment is het gebruik van het register nog in een leer- en ontwikkelingsfase. De organisatie lijkt het verstandig om pas over te gaan naar een tool op het moment dat de werkprocessen ten aanzien van het register volledig duidelijk zijn en dus ook duidelijk is welke functionele eisen er aan een tool moeten worden gesteld.	Verkend wordt om KCD hiervoor in te zetten.
Laat een ter zake deskundig jurist kijken naar de verplichtingen die de WOO eventueel meebrengt voor het register.	Het programmateam neemt deze aanbeveling over.	Nog geen zichtbare actie
Hoog risicoverwerkingen		
Houd een strakke planning aan voor de verwerkingen van	Binnen het IV&P team is er in de planning rekening	DPIA's worden opgepakt buiten de Wasstraat om

hoog risicoprocessen binnen de Wasstraat.	gehouden met het uitvoeren van DPIA's.	
Houd binnen het programma capaciteit vrij om in de tweede helft van 2021 DPIA's uit te voeren op de processen die de Wasstraat oplevert.		Prioriteit van de privacy officers ligt meer bij DPIA's
Samenwerkingsverbanden		
Maak een duidelijke planning– afhankelijk van de risico's – voor de acties die voortvloeien uit deze inventarisatie.	Het programmateam neemt deze aanbeveling over.	Er is een opzet gemaakt voor een memo om vervolgacties in te plannen n.a.v. inventarisatie samenwerkingsverbanden.
DPIA's		
Het uitvoeren van DPIA's zorgt voor inzicht in de risico's die de provincie loopt op het gebied van privacy. Geef het komend jaar daarom prioriteit aan het uitvoeren van DPIA's op die processen die als 'hoog risicoproces' gedefinieerd zijn. De Wasstraat kan hierin ondersteunend zijn, maar wanneer geen sprake is van een versnelling verdient het aanbeveling om de uitvoering van de DPIA's zelf op te pakken. Binnen het team.	Dit wordt meegenomen in het jaarplan IV&P 2022	DPIA's worden opgepakt buiten de Wasstraat om Prioriteit van de privacy officers ligt meer bij DPIA's
Maak duidelijke en gedragen afspraken over het opvolgen van de aanbevelingen die uit de DPIA volgen én over de wijze van acceptatie van eventuele risico's;	Dit wordt in de evaluatie van het proces uitvoeren DPIA's meegenomen.	Nog geen zichtbare actie
Betrek de privacy contactpersonen bij de uitvoering van de DPIA's en de resultaten. Zij kunnen ondersteunen in de uitvoering van de aanbevelingen en dit zorgt voor meer bewustwording binnen het team.	Dit wordt op de lijst met te bespreken onderwerpen voor de contactpersonen gezet.	Nog geen zichtbare actie
Bewustwording		
Geef prioriteit aan het daadwerkelijk geven van trainingen boven het benoemen en uitwerken van	Planning van het programma IV&P is om de eerste organisatiebrede opleidingsmodule in	Eerst deel van de e-learning (basisopleiding medewerkers) is uitgerold en van start gegaan

doelgroepen en behoeften. Het verdient voorkeur om een grote groep op korte termijn een basisopleiding te geven. Deze basisopleiding kan dan uitgebreid worden met toegespitste modules. Zolang immers binnen het programma/project opleiding nagedacht wordt over doelgroepen en inhoud, blijft de bewustwording binnen de organisatie (te) laag.	oktober/november uit te rollen.	
Programma IV&P		
De extra capaciteit op privacy is vooralsnog tijdelijk (voor een jaar). Gelet op de werkvoorraad en het ambitieniveau van de provincie lijkt deze extra capaciteit ook na dat jaar nodig te blijven. Ga na in hoeverre hier ruimte en mogelijkheden voor zijn.		Gekeken wordt naar continuering van capaciteit tot einde kalenderjaar.
Governance		
Neem t.a.v. de onderwerpen informatieveiligheid en privacy concrete resultaatafspraken op in de managementcontracten en laat dit als verplicht onderdeel opnemen in de domeinplannen; Laat deze onderwerpen bij ieder gesprek over de voortgang van de domeinen en teams terugkomen, zodat de verantwoordelijken hierover verantwoording kunnen afleggen.		Geen zichtbare actie
Opslag van informatie		
Stem tijdig af met de privacy officers over deze aandachtspunten en voordat er keuzes worden gemaakt over overdracht van dossiers;		Geen zichtbare actie
Besteed ook aandacht aan het tijdig en veilig vernietigen van informatie waarvan de bewaartermijn is verstreken.		Geen zichtbare actie
Draag zorg voor een warme overdracht van het project		De kwartiermaker CIO-office is aangetrokken en van start

naar de organisatie en bepaal goed op welk moment de specialistische kennis van de ingehuurde externen voldoende overgedragen is aan de organisatie.		gegaan en vanuit het programma IV&P is een memo geschreven over de wensen vanuit het programma met betrekking tot de overgang van programma naar organisatie.