PROVINCIE UTRECHT

RAPPORTAGE FUNCTIONARIS VOOR GEGEVENSBESCHERMING

DATUM	28-9-2021
VERSIE	1.0
DOCUMENT NUMMER	Documentnummer
RAPPORTAGEPERIODE	Juli 2020 tot juli 2021

INLEIDING

Hierbij bied ik de rapportage aan van de functionaris voor gegevensbescherming van de provincie Utrecht over de periode juli 2020 – juli 2021. Zowel binnen de provincie als daarbuiten is er in die periode veel gebeurd op het gebied van privacy. Binnen de organisatie brachten verschillende wisselingen van functionarissen voor gegevensbescherming en privacy officers mee dat tijd nodig was voor inwerken en samenwerking. Inmiddels is de samenstelling van het team stabiel en ligt de focus volledig op het overbrengen van kennis en ervaring en ondersteuning van de organisatie.

Maar ook in de maatschappij was er veel aandacht voor privacy. Twee jaar na het van kracht worden van de Algemene Verordening Gegevensbescherming (AVG) blijkt dat heel veel organisaties - bewust of onbewust - privacy-technisch nog niet op orde zijn. De gevolgen daarvan worden zichtbaar, ook voor organisaties die qua werkveld dicht bij de provincie Utrecht staan. De gemeente Enschede heeft bijvoorbeeld in maart 2021 een boete van €600.000 opgelegd gekregen van de Autoriteit Persoonsgegevens, voor het inzetten van wifi-tracking, zonder dat daar een geldige grondslag voor was. In diezelfde periode was de provincie Utrecht de mogelijkheden van wifi-tracking aan het verkennen om de drukte in natuurgebieden te monitoren en te sturen. De boete voor de gemeente Enschede maakte eens te meer duidelijk wat de risico's van dergelijke ontwikkelingen zijn en dat het bijzonder belangrijk is om tijdig een privacydeskundige te betrekken bij dit soort initiatieven.

Daarnaast bleek een belangrijke samenwerkingspartner van de provincie, BIJ12, door – kort gezegd – verouderde software, een groot beveiligingsrisico te lopen. Ook met data die onder verantwoordelijkheid van of namens de provincie Utrecht werden verwerkt. Deze data bevatten ook persoonsgegevens, waardoor door de functionarissen voor gegevensbescherming van alle provincies gezamenlijk is geadviseerd om een melding te doen bij de Autoriteit Persoonsgegevens. Uit onderzoek bleek dat deze beveiligingsrisico's al langere tijd bestonden, maar dat de provincies hadden vertrouwd op de expertise van de samenwerkingspartner en daardoor hun eigen controlerende taak hadden laten liggen.

Beide voorbeelden geven het belang aan van kennis en bewustzijn binnen de provincie. Een sterk functionerend privacyteam ondersteunt de organisatie, maar iedere medewerker, teamleider en manager zal zelf alert en kritisch moeten zijn en tijdig de benodigde ondersteuning moeten vragen.
Het komende jaar zal de uitdaging dan ook vooral daar liggen: is iedereen binnen de provincie zich bewust van zijn eigen verantwoordelijkheden op het gebied van het naleven van de privacywetgeving? En vraagt hij of zij tijdig ondersteuning daarin?

Ik nodig u daarom ook van harte uit om mee te denken over dit belangrijke onderwerp en te zorgen dat gegevens van onze medewerkers, burgers of andere betrokkenen veilig zijn bij de provincie. 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.

STAND VAN ZAKEN ALGEMEEN

1. DATALEKKEN

a. Proces

Het proces voor het melden van datalekken is duidelijk beschreven. Dit betreft zowel het proces voor de medewerker voor het melden van mogelijke datalekken, als het proces dat gevolgd wordt op het moment dat een melding binnenkomt bij de privacy officer. Deze processen zijn vastgesteld en gepubliceerd op intranet. Ook vindt op de juiste momenten afstemming plaats met de functionaris voor gegevensbescherming.

b. Meldingen

In de periode van 1 juli 2020 tot 1 juli 2021 zijn in het totaal 19 meldingen binnengekomen van mogelijke datalekken. 18 meldingen betroffen een proces binnen de provincie Utrecht, 1 melding betrof een proces bij een verwerkende partij (waarvoor de provincie Utrecht verantwoordelijk is). Van de 19 meldingen werd bij 2 meldingen geconcludeerd dat de inbreuk op de privacy zodanig was dat een melding gedaan moest worden bij de Autoriteit Persoonsgegevens. In 4 gevallen werden de betrokkenen geïnformeerd over het datalek.

De binnengekomen meldingen zijn zeer divers. Van het achterlaten van een tas met laptop in de trein tot het per abuis op de website publiceren van adresgegevens van een burger. Wel ziet een groot deel van de meldingen op het verkeerd gebruik van e-mail. Het vermelden van een groep adressanten buiten de provincie in de cc in plaats van in de bcc is de meest voorkomende fout. Direct gevolgd door het verzenden van een e-mail aan de verkeerde persoon doordat Outlook het adres automatisch afmaakt. Afhankelijk van de inhoud van de e-mail en de waarschijnlijkheid dat adresgegevens al bekend waren bij de groep van geadresseerden is al dan niet sprake van een datalek.

c. Bewustwording

Het onderwerp datalekken wordt meegenomen in het reguliere opleidingstraject. Daarnaast is de eerste digitale nieuwsbrief IV&P geheel gewijd aan het onderwerp datalekken. Minder zichtbaar is of meldingen van datalekken worden ingezet voor het lerend vermogen van de organisatie. Op welke manier leert de organisatie van een datalek? Hiervoor is goede afstemming nodig met de teamleider van het team waarover de melding is gedaan.

AANBEVELINGEN:

- Organiseer op korte termijn een bewustwordingscampagne gericht op het juiste gebruik van e-mail;
- Richt het proces melden datalekken zo in dat de leidinggevende altijd terugkoppelt op welke wijze de organisatie heeft geleerd van het datalek;
- Bespreek gemelde datalekken (geanonimiseerd) met het organisatiebrede netwerk van privacy-contactpersonen.

2. REGISTER VAN VERWERKINGEN

In Q4 2020 en Q1-2 2021 is het verwerkingsregister geactualiseerd en is er een slag gemaakt om het register eenduidiger en toegankelijker te maken. Er is besloten tot interne openbaarmaking van het register. Extern wordt dit register niet gepubliceerd. Deze actualiseringsslag heeft geleid tot een professioneler en voor de organisatie toegankelijker register. Er zijn echter nog enkele aandachtspunten geconstateerd:

- Er ontbreekt op verschillende plekken eenduidigheid in het register. Bijvoorbeeld de manier waarop grondslagen of betrokkenen worden beschreven;
- De actualiseringsslag de in Q4 2020 is uitgevoerd is niet door elke privacy officer op dezelfde manier uitgevoerd. Voor die processen waarvoor slechts is uitgevraagd of deze nog juist zijn is het (bij instemming of ontbreken van een antwoord) maar de vraag of de ingevulde gegevens inderdaad correct en volledig zijn;

- Gelet op de Wet open overheid, die waarschijnlijk in 2022 in werking zal treden, is het de vraag of vastgehouden kan worden aan het besluit om het register uitsluitend intern te publiceren.

AANBEVELINGEN

- 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;
- Laat een terzake deskundig jurist kijken naar de verplichtingen die de WOO eventueel meebrengt voor het register.

3. HOOG RISICO VERWERKINGEN

In december 2020 is een uitvraag gedaan gericht aan de teamleiders om aan te geven welke processen binnen hun team een hoog risico inhouden op het gebied van IV&P. Uit de reacties die hierop zijn ontvangen is een lijst gemaakt van hoog risico processen. In samenwerking met het programma 'de Wasstraat' is vervolgens een aanvang gemaakt met het beschrijven van deze processen met als doel inzicht te krijgen in risico's op het gebied van IV&P en mogelijk mitigerende maatregelen door te voeren. Daartoe worden de volgende stappen doorlopen:

- De Wasstraat maakt een procesbeschrijving (IST-situatie) en een informatieanalyse;
- Door Informatieveiligheid wordt een Business Impact Assessment (BIA) opgesteld;
- Door Privacy wordt een advies gegeven over het gebruik van persoonsgegevens (als dat het geval is) en eventueel wordt een Data Protection Impact Assessment (DPIA) uitgevoerd;
- Door archivering wordt een advies gegeven over het bewaren/vernietigen van documenten;
- In samenwerking met de Wasstraat wordt door het verantwoordelijke team opnieuw gekeken naar het proces om eventuele aanbevelingen vanuit IV&P en Archivering te verwerken. Er wordt een nieuwe procesbeschrijving gemaakt (SOLL-situatie).

In Q1 2021 is er veel overleg geweest met de Wasstraat over de juiste aanpak van het bovenstaande. Dit heeft geleid tot vertraging in het oppakken van de hoog risico processen. Inmiddels heeft de Wasstraat een start gemaakt, maar er zijn nog geen processen overgedragen voor advies aan IV&P en Archivering. Dit leidt tot het risico dat op korte termijn een zeer groot aantal processen wordt aangeboden, waardoor de betrokken medewerkers onvoldoende tijd hebben om deze processen allemaal tijdig te verwerken. Het is belangrijk om hiervoor aandacht te houden en afspraken te maken over een soepelere doorgang van processen.

AANBEVELINGEN

- Houd een strakke planning aan voor de verwerkingen van hoog risico processen binnen de Wasstraat;
- 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.

4. SAMENWERKINGSVERBANDEN

Door de privacy officers is in samenwerking met team Inkoop geïnventariseerd welke samenwerkingsverbanden er bestaan binnen de provincie. Van al deze samenwerkingen is bepaald of sprake is van een uitwisseling van persoonsgegevens (waardoor de AVG van toepassing zou zijn) en of de afspraken over de uitwisseling van deze gegevens voldoende geborgd is, bijvoorbeeld in de vorm van een verwerkersovereenkomst. Met deze inventarisatie is meer duidelijkheid gekomen over potentiële risico's (in veel gevallen verlaten persoonsgegevens immers de organisatie).

AANBEVELINGEN

Maak een duidelijke planning– afhankelijk van de risico's – voor de acties die voortvloeien uit deze inventarisatie.

5. PRIVACYBELEID

Op 18 februari 2021 hebben Gedeputeerde Staten het privacybeleid voor de provincie Utrecht vastgesteld. Het privacy beleid 2021 – 2025 geeft aan welke uitgangspunten de provincie Utrecht hanteert en hoe zij invulling geeft aan alle verplichtingen die op haar rusten ingevolge de AVG. De vaststelling van het privacybeleid staat niet op zichzelf, maar is onderdeel van de gehele implementatie van de AVG. Onderdeel van deze implementatie is onder meer het opstellen van diverse modelovereenkomsten, een procedure datalekken en het verhogen van de bewustwording onder de medewerkers. Met de vaststelling van het privacybeleid zijn de basismaatregelen getroffen, waarna de nadruk zal moeten komen te liggen op het treffen van maatregelen om risico's te mitigeren en blijvende aandacht te vragen voor bewustwording door de hele organisatie heen.

Op 14 april 2021 hebben Provinciale Staten besloten voor de eigen werkzaamheden aan te sluiten bij de uitgangspunten van het privacybeleid 2021 - 2025, zoals dat door GS is vastgesteld. PS stelt daarmee geen eigen privacybeleid op, maar heeft wel aantoonbaar uitgangspunten vastgesteld voor de uitvoering van de eigen werkzaamheden in lijn met de AVG.

Opgemerkt wordt dat de provincie – naast het vastgestelde privacybeleid – beschikt over een Statuut Gegevensbescherming (provinciale verordening). In dat Statuut zijn bepalingen opgenomen over de positionering en taken van de FG en de privacy officers en over de verantwoordelijkheden van teamleiders en opgavemanagers. De werking van dit Statuut wordt in de tweede helft van 2021 geëvalueerd, waarin ook de verhouding van het Statuut tot het Privacybeleid wordt meegenomen.

6. DPIA'S

Een data protection impact assessment (DPIA) is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Het is verplicht een DPIA uit te voeren bij processen (gegevensverwerkingen) waarin een hoog risico is voor de bescherming van de privacy van betrokkenen. Door de PO's is aan de hand van het verwerkingsregister een overzicht gemaakt van uit te voeren DPIA's op bestaande processen. Deze lijst wordt doorlopend aangevuld met DPIA's voor nieuwe processen, bijvoorbeeld voor pilots met camera's of slimme technieken om data te genereren. Op dit moment bevat de 'stocklist DPIA's' 36 DPIA's. Dit betreft geheel nieuwe DPIA's en herbeoordelingen van bestaande DPIA's. Een deel van deze DPIA's komt uit het proces van de Wasstraat, zoals beschreven onder 3.

In het afgelopen jaar zijn slechts enkele DPIA's uitgevoerd. Dit brengt als risico's mee dat onvoldoende inzicht is in mogelijke privacy risico's binnen processen en wanneer zich binnen een hoog risico proces een incident voordoet, zoals een datalek, niet aangetoond kan worden aan de toezichthouder dat voldaan is aan de verplichting uit de AVG om risico's in kaart te brengen en te mitigeren. Er zal dus komende tijd vol ingezet moeten worden op het uitvoeren van DPIA's. Aandachtspunt daarbij is dat de inzet van de Wasstraat voor de procesbeschrijving die nodig is voor het uitvoeren van de DPIA's, dit jaar niet het gewenste resultaat heeft gehad. In plaats van een versnelling heeft dit geleid tot vertraging, doordat de output van de Wasstraat uitbleef. De meerwaarde van inzet van de Wasstraat zal dus heroverwogen moeten worden.

Door het in kaart brengen van de verplichte DPIA's én doordat het privacyteam uitgebreid is met deskundige privacy officers ligt het in lijn der verwachting dat er komend jaar een flinke inhaalslag plaatsvindt op deze DPIA's.

Een belangrijk aandachtspunt is gelegen in de opvolging van de aanbevelingen die voortkomen uit de DPIA. Deze aanbevelingen zijn gericht aan de procesverantwoordelijke

(doorgaans de teamleider) van het proces waarop de DPIA ziet. Er bestaat op dit moment echter geen vastgesteld proces met bijbehorende verantwoordelijkheden op de controle op de naleving van deze aanbevelingen. Aanbevolen wordt om in een plan do check act-cyclus deze controle vorm te geven.

AANBEVELINGEN

- 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 risico proces' 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.
- 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;
- Betrek de privacycontactpersonen 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.

7. BEWUSTWORDING

Een privacybewuste organisatie maakt een privacyvolwassen organisatie. Alleen als iedereen die werkzaam is voor de provincie kennis heeft van zijn of haar taken en verantwoordelijkheden op het gebied van privacy én voldoende basiskennis van het onderwerp heeft, passend bij de uitvoering van zijn taken, kan de organisatie het gewenste volwassenheidsniveau behalen. Dit is nu nog niet het geval.

Vanuit het programma IV&P zijn het afgelopen jaar verschillende activiteiten ontplooid om de organisatie mee te nemen. Voorbeelden hiervan zijn:

- Webinars en inspiratiesessies over IV&P-gerelateerde onderwerpen;
- Een tweemaandelijkse digitale nieuwsbrief met telkens een relevant thema (zoals datalekken en het herkennen van phishing);
- Sessies aan de managementtafel met toelichting en praktijkvoorbeelden;
- Informatiesessies voor verschillende teams;
- Uitbreiding van de informatie op intranet;

Ook is een opleidingsplan opgesteld waarin per doelgroep (medewerkers, teamleiders, etc.) is opgenomen op welke wijze zij worden gefaciliteerd om de benodigde basiskennis op te doen. De uitvoering van dit plan laat echter op zich wachten. Inmiddels is een projectleider aangesteld die uitvoering gaat geven aa n het opleidingsplan. Daadwerkelijke opleiding vanuit het plan heeft echter nog niet plaatsgehad.

De uitwerking van de inzet op bewustwording wordt steeds duidelijker zichtbaar in de organisatie. Vooral doordat medewerkers de privacy officers weten te vinden met vragen. Ook worden de privacy officers steeds vaker tijdig verzocht om aan te sluiten bij een nieuw project of programma. Zo zijn er privacy officers vast onderdeel van ontwikkelingen als Hybride werken, Data gedreven werken/digitale transformatie, Digitaal slagvaardige medewerker, Integriteit en de Omgevingswet.

AANBEVELINGEN

Geef prioriteit aan het daadwerkelijk geven van trainingen boven het benoemen en uitwerken van 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.

8. PROGRAMMA IV&P

Het programma IV&P is met name in Q1-2 van 2021 uitgebreid met extra capaciteit. Zowel op het gebied van informatieveiligheid als van privacy is de bezetting uitgebreid. Dit heeft ertoe geleid dat na een inwerkperiode meer

werk is opgepakt, waaronder ook ‘achterstallig onderhoud’ zoals het bijwerken van het register van verwerkingen. Deze uitbreiding is zeker positief, maar vraagt ook goede afstemming binnen het programma.

Binnen het programma is veel gesproken over de verdeling van het werk tussen ‘programmadoelen’ en ‘ad hoc werk’. Wat hier bedoeld wordt is dat over het algemeen veel tijd gaat naar vragen uit de organisatie, waardoor minder tijd overblijft voor langere termijn doelen. Door het programma is toegezegd dat eind 2021 een bepaald volwassenheidsniveau wordt behaald (voor privacy volwassenheidsniveau 3 van het normenkader van het Centrum Informatiebeveiliging en Privacybescherming, CIP).

Inmiddels zijn binnen het programma afspraken gemaakt over de verdeling van de verschillende werkzaamheden. Wel wil ik er in dit verband nog nadrukkelijk op wijze dat het slagen van het programma IV&P – en daarmee het succesvol voldoen aan het beloofde volwassenheidsniveau – afhankelijk is van de vraag hoezeer medewerkers, leidinggevenden en management zich ondersteund en geholpen voelen door het programma. Voor een voldoende inzicht in IV&P-risico’s is het van groot belang dat procesverantwoordelijken het programma betrekken bij hun processen, pilots en projecten. Een te starre houding tegenover ‘ad hoc-vragen’ uit de organisatie leidt ertoe dat deze ondersteuning niet ervaren wordt en dat het programma niet gevoed wordt met informatie. Daarmee zou het programma zijn eigen doel voorbij streven.

Wat betreft de ambitie – zoals uitgesproken in het jaarplan – om eind 2021 voor de belangrijkste onderdelen te voldoen aan volwassenheidsniveau 3 van het CIP, lijkt het programma op de goede weg te zijn. Om het volwassenheidsniveau aan het einde van het jaar inzichtelijk te maken is afgesproken om dan een self-assessment van het CIP uit te voeren onder coördinatie van de FG. Uit een ‘oefensessie’ met dit self-assessment in de zomer van 2021 bleek dat de gaps tot niveau 3 vooral lagen in reeds bekende actiepunten waarop de benodigde uitvoering al ingepland is. Aan het einde van 2021 moet blijken of deze acties hebben geleid tot een aantoonbaar volwassenheidsniveau 3. Hierover zal eind 2021, begin 2022 verslag worden uitgebracht.

AANBEVELINGEN

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.

9. GOVERNANCE

Het onderwerp privacy is de verantwoordelijkheid van de hele organisatie. Iedereen heeft daar zijn of haar eigen aandeel in. Taken en rollen zijn vastgelegd in het privacybeleid en het statuut gegevensbescherming. De kennis en het bewustzijn van deze verantwoordelijkheden zijn echter zeer wisselend binnen de organisatie. De onderwerpen informatieveiligheid en privacy wordt door een deel van de organisatie nog gezien als ‘lastig, geen onderdeel van de reguliere werkzaamheden en als verantwoordelijkheid van het programma IV&P’. Dit komt terug in uitwisselingen van persoonsgegevens en organisatiebrede dataprojecten waarbij het programma pas laat wordt betrokken.

Vanuit het programma IV&P zal duidelijk gecommuniceerd moeten worden wat de vastgelegde taken en verantwoordelijkheden zijn op dit gebied. Daarnaast ligt er een taak voor het management om de procesverantwoordelijken hierop te wijzen. Alleen wanneer ‘top down’ wordt gestuurd op deze taken en verantwoordelijkheden, zullen deze organisatiebreed worden gedragen.

AANBEVELINGEN

- Neem t.a.v. de onderwerpen informatieveiligheid en privacy concrete resultaatafspraken op in de

managementcontracten[1] 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.

10. OPSLAG VAN INFORMATIE

Vervanging Documentum
Documentum voorzag in een dynamisch deel (Document Management Systeem (DMS)) voor samenwerken en een (semi) statisch deel voor het archiveren van informatie. Documentum wordt vervangen voor een nieuwe samenwerkomgeving (Sharepoint Online en MS Teams) en een nieuw Archiefsysteem, waarvoor de aanbestedingsprocedure loopt. In Documentum staan dossiers waarin persoonsgegevens zijn opgenomen. Vervanging van dit systeem brengt dus risico's mee voor de bescherming van die gegevens. Het gaat dan om:
- Gearchiveerde dossiers in Documentum die overgezet worden in een nog aan te schaffen systeem. Worden hierin de juiste bewaartermijnen geborgd? Vindt tijdens de overdracht geen verlies van gegevens plaats? Worden de juiste metadata overgezet, zodat documenten terugvindbaar zijn?
- Lopende dossiers in Documentum die overgezet worden in Sharepoint en Teams. Naast de aandachtpunten genoemd onder de vorige bullet geldt hier ook het aandachtspunt voor of toegang tot documenten juist is ingeregeld (kunnen er niet meer mensen bij dan nodig?) .

AANBEVELINGEN
- Stem tijdig af met de privacyofficers over deze aandachtspunten en voordat er keuzes worden gemaakt over overdracht van dossiers;
- Besteed ook aandacht aan het tijdig en veilig vernietigen van informate waarvan de bewaartermijn is verstreken.

Einde project Sharepoint en Teams
Het gebruik van Sharepoint en Teams als samenwerkingomgeving voor de medewerkers is opgezet in projectvorm, waarin veel kennis bijeen is gebracht. Deze kennis zit vaak bij ingehuurde externen. De eindfase van het implementatietraject lijkt aanstaande te zijn, al is een exacte datum nog niet genoemd. Na de beëindiging van dit project zal het beheer van Sharepoint en Teams over moeten gaan naar de bestaande organisatie. Het is echter niet zeker of de organisatie beschikt over voldoende kennis om deze omgevingen voldoende beveiligd hun werk te laten doen.

AANBEVELINGEN
- Draag zorg voor een warme overdracht van het project naar de organisatie en bepaal goed op welk moment de specialistische kennis van de ingehuurde externen voldoende overgedragen is aan de organisatie.

[1] Denk hierbij bijvoorbeeld aan afspraken over het in kaart brengen van hoog risico processen, het afsluiten van verwerkersovereenkomsten en het uitvoeren van DPIA's.

STAND VAN ZAKEN DOMEINEN

Door verschillende wisselingen van de FG-functie in 2020 en het thuiswerken i.v.m. Coronamaatregelen kan ik nog geen sluitend beeld geven over de naleving van de AVG binnen de domeinen. Duidelijk zichtbaar is dat een deel van de teams al goed hun weg kunnen vinden naar de privacy officers en de FG wanneer dat nodig is en dat andere teams hier veel actiever op gewezen moeten worden.

DOMEINPLANNEN 2021

In alle domeinplannen is een (kort) stukje opgenomen over informatieveiligheid en privacy. Hiermee is in ieder geval bewerkstelligd dat het onderwerp op de agenda staat. Onderstaande teksten zijn 1-op-1 overgenomen uit de diverse domeinplannen.

1. Domeinplan BDV
Informatieveiligheid en privacy
Uit diverse onderzoeken is gebleken dat de Informatieveiligheid en privacy binnen de provincie nog op onvoldoende niveau is. In 2025 wil de provincie Utrecht informatieveiligheid en privacy aantoonbaar op orde hebben conform de Algemene Verordening Gegevensverwerking en Baseline Informatiebeveiliging Overheid.
Er is een programma IV&P opgezet binnen de PU en heeft tot doel informatieveiligheid en privacy structureel te verbeteren en in te bedden in de provinciale organisatie om vervolgens aantoonbaar op orde te zijn en te blijven. De provincie Utrecht heeft een functionaris gegevensbescherming aangesteld die in samenwerking met de organisatie een top 25 opstelt met meest gevoelige processen en bij deze processen wordt vervolgens getoetst of ze IV&P-proof zijn.
Informatieveiligheid en privacy worden in toenemende belangrijk voor de teams binnen het domein. In gesprekken aan de keukentafel met stakeholders komen er soms zeer gevoelige zaken ter sprake. Daarnaast kunnen er ook zeer gevoelige zaken zitten in grondonderhandelingen. Het is zaak daar alert op te blijven.
Het verwerkingsregister is door het programma IV&P eind 2020 geactualiseerd. Vanaf 2021 zorgt de domeinmanager ervoor dat de verwerkingen die voor ons domein zijn opgenomen in het verwerkingsregister juist en actueel zijn. Hiervoor zal een werkproces worden opgesteld wat ondersteund zal worden vanuit team GEB.

Acties IV&P voor domein Bedrijfsvoering: 1.

1. Binnen het domein zal met ondersteuning van het programma IV&P dit jaar alle werkprocessen bekeken worden waar de processen aangepast moeten worden.
2. Processen aanpassen en IV&P proof maken
3. Medewerkers bewust maken van de privacy regels door dit jaar een training te volgen
4. Werkproces uitwisselen gegevens opstellen.

2. Domeinplan BDO
Informatieveiligheid en privacy (IV&P)
Er is een programma IV&P opgezet om de informatieveiligheid en privacy structureel te verbeteren. Er is een functionaris gegevensbescherming aangesteld die een top 25 opstelt met de meest gevoelige processen. Voor BD1 is de bestuurlijke besluitvorming als kritisch proces aangemeld voor de wasstraat om te toetsen of deze IV&P-proof is. Ook zijn samen met Bedrijfsvoering de processen met betrekking tot de declaraties van bestuurders beschreven en aangemeld voor de wasstraat.
De teamleider BD1 neemt deel aan de klankbordgroep IV&P.
Voor heel BDO zullen wij de werkprocessen met ondersteuning van IV&P prioriteren om te bezien waar aanpassing op nodig is.
Het verwerkingsregister is door het programma IV&P eind 2020 geactualiseerd. Vanaf 2021 zorgt de

domeinmanager ervoor dat de verwerkingen actueel blijven.

3. Domeinplan LLO

Informatieveiligheid en Privacy (IV&P)

Uit diverse onderzoeken is gebleken dat de Informatieveiligheid en privacy binnen de provincie nog op onvoldoende niveau is. In 2025 wil de provincie Utrecht informatieveiligheid en privacy aantoonbaar op orde hebben conform de Algemene Verordening Gegevensverwerking en Baseline Informatiebeveiliging Overheid.
Er is een programma IV&P opgezet binnen de PU en heeft tot doel informatieveiligheid en privacy structureel te verbeteren en in te bedden in de provinciale organisatie om vervolgens aantoonbaar op orde te zijn en te blijven. De provincie Utrecht heeft een functionaris gegevensbescherming aangesteld die in samenwerking met de organisatie een top 25 opstelt met meest gevoelige processen en bij deze processen wordt vervolgens getoetst of ze IV&P-proof zijn.

Informatieveiligheid en privacy worden in toenemende belangrijk voor de teams binnen ons domein. In gesprekken aan de keukentafel met stakeholders komen er soms zeer gevoelige zaken ter sprake. Daarnaast kunnen er ook zeer gevoelige zaken zitten in grondonderhandelingen. Het is zaak daar alert op te blijven.
Het verwerkingsregister is door het programma IV&P eind 2020 geactualiseerd. Vanaf 2021 zorgt de concernmanager ervoor dat de verwerkingen die voor ons domein zijn opgenomen in het verwerkingsregister juist en actueel zijn. Hiervoor zal een werkproces worden opgesteld wat ondersteund zal worden vanuit team GEB. Aandachtspunt voor de langere termijn is de informatieveiligheid bij het (samen)werken met het digitale stelsel van de Omgevingswet vanaf 2022.

Acties IV&P:

1. Binnen het domein zal met ondersteuning van het programma IV&P dit jaar alle werkprocessen bekeken worden waar de processen aangepast moeten worden.
2. Processen aanpassen en IV&P proof maken
3. Medewerkers bewust maken van de privacy regels door dit jaar een training te volgen
4. Werkproces uitwisselen gegevens opstellen verwerkingsregister
5. Alle medewerkers werken met MFA.

4. Domeinplan SLO

Informatieveiligheid en Privacy

De aandacht voor dit onderwerp is sterk vergroot. De verantwoordelijkheid dat dit goed wordt uitgevoerd ligt bij de domeinmanager. Vanuit I&A is een aanpak uitgerold met opleidingsonderdelen. SLO is gevraagd een aantal mensen aan te wijzen die een soort eerstelijns advisering zouden kunnen zijn. Dit zou per team iemand moeten zijn. Tegelijkertijd beseffen we dat enige affiniteit met dit onderwerp en competentie op datagebied belangrijk is om de juiste personen naar voren te schuiven. Niet in elk team zijn hier voorbeelden van. We zien daarom 2021 als een overgangsjaar waarin we mede door het UPP een beeld kunnen krijgen wie we hier het best voor naar voren kunnen schuiven. Hierbij is niet persé de insteek om dit ook per team te regelen. Maar ca drie aanspreekpunten lijkt ons voldoende.

5. Domeinplan Mobiliteit

Informatievoorziening

Om goed te kunnen sturen op beleid en inhoud is een adequate organisatie en betrouwbare informatievoorziening van groot belang. Adequate en betrouwbare informatievoorziening houdt in dat informatie beschikbaar is, beheerd wordt, beveiligd is en voldoet aan de AVG.
Om dit te realiseren wordt de focus in 2021 gelegd op:

- Managementinformatie verder ontwikkelen en digitaliseren. Dit gaan we doen door een Dashboard Mobiliteit te ontwikkelen.
- Het in kaart brengen van de informatiestromen binnen het domein Mobiliteit met de opdracht "inzicht in informatie"
- Informatiebehoefte van de bestuurlijke, primaire (mobiliteit) en ondersteunende processen inzichtelijk maken en omzetten in een informatieplan
- Samen met I&A de informatievoorziening vorm geven zowel voor het domein als voor de provincie door invulling te geven aan de BIM-rol en betrokkenheid bij het regie-team.

6. Eenheidsplan CCO

Met ingang van de programmabegroting 2021 zijn er voor het programma overhead ook doelen geformuleerd voor concerncontrol. Deze luiden:
De beheersing van de organisatie door en management en het bestuur is optimaal.

- Uitvoeren van concerncontrol waaronder onder andere adviseur van de Financiële Auditcommissie.
- Versterken van Verbijzonderde Interne Controle (VIC)
- Bijdragen aan bestuurlijke doelen zoals informatieveiligheid en privacy.

REACTIE EN VERVOLG

Deze teksten uit de domeinplannen zorgen weliswaar voor enige aandacht voor de onderwerpen privacy en informatieveiligheid, maar zijn bijna zonder uitzondering van een zodanig abstractie dat er geen concrete acties uit voortkomen. Om het gewenste privacyvolwassenheidsniveau te bereiken moet hier verandering in komen.

In Q4 2021 worden daarom gesprekken ingepland met de domeinmanagers om met hen te bespreken hoe zij het onderwerp privacy opnemen in hun plannen voor 2022 en hoe zij zich zullen inzetten om de doelen in deze plannen te bereiken. Hierin zal ook aandacht zijn voor de diverse verantwoordelijkheden voor privacy binnen de organisatie. Zo ligt de verantwoordelijkheid voor het benoemen van hoog risico processen niet bij de functionaris voor gegevensbescherming – welke indruk in een aantal domeinplannen wel wordt gewekt -, maar bij de proceseigenaren zelf.

Door hierin ondersteuning te bieden kunnen plannen concreter gemaakt worden en kunnen domeinen is samenwerking met het programma IV&P ervoor zorgen dat de organisatie als geheel een stap maakt in volwassenheid.

CONCLUSIES

Als functionaris voor gegevensbescherming zie ik met name binnen het programma IV&P een duidelijke positieve ontwikkeling. Er is veel kennis en kunde aanwezig, adviezen worden tijdig en duidelijk onderbouwd gegeven en risico's worden proactief benoemd door de privacy officers. Ook is de samenwerking met de organisatie goed. Daarbij moet de kanttekening worden geplaatst dat het dan gaat om collega's die de samenwerking met privacy hebben gezocht of zijn aangegaan.

Hier tegenover staat een (kleiner) deel van de organisatie dat voor de privacy officers moeilijk te bereiken is, waar weinig tot geen navolging wordt gegeven aan aanbevelingen en waarvandaan geen ondersteuning wordt gevraagd. Daar bevinden zich de grootste privacyrisico's voor de organisatie, omdat hier sprake is van onbekende risico's.
De reden dat de samenwerking moeizaam verloopt is wisselend. Medewerkers zijn zich niet bewust van het feit dat er een privacycomponent in een vraagstuk zit, denken hiervoor zelf voldoende kennis in huis te hebben of geven niet tijdig prioriteit aan dit onderwerp.

De oplossing voor deze situatie zal van verschillende kanten moeten komen. Vanuit het programma IV&P is het belangrijk dat organisatiebreed wordt ingezet op het vergroten van de kennis. Een bewuste medewerker zal sneller inzien dat sprake is van een privacyvraagtsuk en zal daardoor sneller deskundige hulp inschakelen.

Daarnaast zal vanuit het (centrale) management een duidelijkere boodschap afgegeven moeten worden dat het niet acceptabel is om bij de verwerking van persoonsgegevens niet of te laat een privacy officer in te schakelen. De risico's die gepaard gaan met risicovolle verwerkingen van persoonsgegevens zijn inmiddels reëel en omvangrijk. Niet alleen worden met enige regelmaat boetes van enkele tonnen opgelegd, maar ook de negatieve media-aandacht die vaak gepaard gaat met privacyovertredingen doet de geloofwaardigheid van de organisatie geen goed.

Op onderdelen is de betrokkenheid van het (centrale) management steeds beter te zien, zoals bij de instelling van het computer emergency response team (CERT) dat optreedt wanneer sprake is van grote digitale incidenten, zoals een hack. Hierover is het management niet alleen geïnformeerd, maar zij heeft ook bepalende keuzes moeten maken en de bijbehorende risico's geaccepteerd.

Deze proactieve, betrokken houding is nodig door de hele organisatie heen. Alleen dan wordt het gewenste privacyvolwassenheidsniveau gehaald.

SEPTEMBER 2021
Stefanie Kelterman,
Functionaris voor gegevensbescherming