Jaarrapportage 2022 – Functionaris Gegevensbescherming

Rapportageperiode: 1 januari 2022 – 31 december 2022

Inhoud

Samenvatting en Aanbevelingen

De PU bevindt zich in een cruciale fase ten aanzien van de privacy functie binnen haar organisatie. De AVG is inmiddels bijna 5 jaar van kracht, en het programma IV&P staat op het punt van afronden. De opbouwfase is dus voorbij, en de staande organisatie moet privacy nu in al haar processen blijven waarborgen. Tegelijkertijd gaan de digitale ontwikkelingen onverminderd snel door en raken automatisering en data steeds meer vervlochten met alle aspecten van ons werk, zowel in de bedrijfsvoering als in de uitvoering van de kerntaken van de PU. Vragen als welke (persoons)gegevens wil en mag ik hebben (en hoe lang), wie bepaalt wat we er mee doen, hoe zorgen we voor de beschikbaarheid, integriteit en vertrouwelijkheid van al die data, en hoe waarborgen we dat we blijvend aan alle wetten en regels voldoen op dit terrein, zijn niet meer los van elkaar te beantwoorden. Het wordt dus steeds belangrijker om integraal regie te voeren op al deze aspecten, zowel in de strategie, de bedrijfsvoering als de controle hierop.

Er is inmiddels veel bereikt binnen de PU. Het bewustzijn (*awareness*) over zowel de vele mogelijkheden als de mogelijke gevaren van het werken met (persoons)gegevens is sterk toegenomen, en de belangrijkste 'infrastructuur' om de privacy functie te borgen (beleidskaders, adviesfunctie, rapportagemiddelen, risicoanalyses) is gereed of is gepland om gereed te maken. De privacy volwassenheid beweegt daarmee langzaam richting het door de organisatie gewenste niveau van 3. Hierbij past wel de belangrijke kanttekening dat de laatste stapjes om naar het niveau van 3 door te groeien weerbarstig te zijn. Het gaat dan met name over risicomanagement, informatieveiligheid en monitoring/toezicht, stuk voor stuk onderwerpen waarvoor de hele organisatie betrokken moet zijn om dit goed in te regelen. Ook hier is integrale regie en aansturing dus noodzakelijk om dit voor elkaar te krijgen.

Meer duiding over de interne en externe ontwikkelingen, de voortgang die is geboekt en de aandacht die nog nodig is, is verder uitgewerkt in de navolgende rapportage. De aanbevelingen die hierin zijn genoemd zijn hieronder in tabelvorm weergegeven en genummerd.

Nummer	Aanbeveling	§
FG-2023-1	Zorg dat teamleiders meer proactief bewerkstelligen (al dan niet via hun IV&P contactpersonen of stafbureaus) dat het verwerkingsregister up-to-date is	4.1
FG-2023-2	Breng de privacy officers onder op een relatief onafhankelijke en herkenbare plek die recht doet aan de 2e lijns rol (kaderstelling, advies, ondersteuning en monitoring).	5
FG-2023-3	Breng de privacy officers onder op een plek die recht doet aan een integrale aanpak van de i-functie.	5
FG-2023-4	Borg procesmatig dat Quickscans en/of DPIA's op tijd worden uitgevoerd.	6.1
FG-2023-5	Implementeer een PDCA-cyclus om zowel de herijking van Quickscans en DPIA's als de monitoring van de daarin voorgestelde maatregelen meer structureel vorm te geven.	6.2
FG-2023-6	Geef meer prioriteit aan het op orde brengen van de informatiebeveiliging van de PU, met bijzondere aandacht voor de governance van de I-assets en de rapportage aan en sturing door of namens het CMT.	7
FG-2023-7	Zorg dat ontbrekende verwerkersovereenkomsten zo spoedig mogelijk alsnog worden opgesteld.	9.1
FG-2023-8	Borg procesmatig dat verwerkersovereenkomsten tijdig worden afgesloten.	9.1
FG-2023-9	Organiseer een bepaalde vorm van monitoring van verwerkers(overeenkomsten).	9.1
FG-2023-10	Borg procesmatig dat bij het aangaan van samenwerkingsverbanden vooraf wordt gecheckt of en zo ja welke privacy bepalingen moeten worden opgenomen.	9.2

Voorwoord

Met de voortgaande digitalisering van vrijwel ieder aspect van ons leven, is ook het belang van en de aandacht voor het onderwerp privacy nog steeds groeiende. Vrijwel dagelijks lezen we berichten over bedrijven of instellingen die onzorgvuldig zijn omgegaan met persoonsgegevens en/of die slachtoffer zijn geworden van cybercriminaliteit. De bekendheid met de in 2018 in werking getreden Algemene Verordening Gegevensbescherming (AVG) is navenant groeiende, omdat vrijwel iedereen er inmiddels wel eens mee te maken heeft gehad. Zakelijk omdat steeds vaker en systematischer voorwaarden worden gesteld aan het gebruik van persoonsgegevens, bijvoorbeeld bij het bijhouden van adressenbestanden, het opslaan en gebruiken van (bijzondere) personeelsgegevens, het maken van videobeelden of het monitoren van mensen. Maar ook privé, bijvoorbeeld bij slimme camera's bij de voordeur, het maken van videobeelden met een drone of het plaatsen van klassenfoto's op Internet.

De ontwikkelingen in de techniek gaan daarbij onverminderd snel door. De Big Tech bedrijven hebben steeds meer data en technieken tot hun beschikking om onze keuzes te beïnvloeden in een richting die aansluit bij hun eigen verdienmodellen en er bestaat toenemende zorg over hun invloed op onze levens en maatschappij. Er zijn steeds meer camera's en deze worden ook steeds scherper en slimmer. Dat er ergens een grens is aan wat burgers nog acceptabel vinden in de aantasting van hun privacy, blijkt bijvoorbeeld uit de commotie die ontstond rondom het plaatsen van camera's op de Universiteit Leiden. Een zeer actueel onderwerp is de vooruitgang op het gebied van kunstmatige intelligentie (AI). In 2017 kwam al het verrassende nieuws dat het computerprogramma AlphaGo slechts 24 uur nodig had om via een zelflerend algoritme sterker te worden dan de wereldkampioen schaken. Inmiddels is AI niet meer beperkt tot vooral wiskundige toepassingen, maar kunnen scholieren bijvoorbeeld met het programma ChatGPT binnen een handomdraai werkstukken generen die nauwelijks meer van echt zijn te onderscheiden.

Beleidsmakers en toezichthouders spelen uiteraard in op de hierboven geschetste ontwikkelingen. De komende jaren zal een grote hoeveelheid nieuwe wet- en regelgeving van kracht worden op de aan elkaar gerelateerde gebieden van digitale dienstverlening, privacy en informatiebeveiliging. De Autoriteit Persoonsgegevens (AP) is ook nadrukkelijk in beeld met betrekking tot de bescherming van privacy en persoonsgegevens in Nederland. Met enige regelmaat geeft de AP kritische adviezen bij wetgevingsvoorstellen, zoals bijvoorbeeld ten aanzien van het plan van aanpak witwassen. Daarnaast werd in 2022 bekend dat de AP in 2023 de toezichthouder zal worden voor het toezicht op algoritmes. Daarnaast is ook in 2022 weer gebruikt gemaakt van het boete-instrument als ultiem middel. De gemeente Rotterdam kreeg een boete van 50.000 euro omdat ze in Coronatijd camera-auto's liet rondrijden zonder daarvoor eerst een risicoanalyse te hebben uitgevoerd. DPG Media kreeg een boete van 525.000 euro omdat mensen die hun persoonsgegevens wilden inzien ten onrechte werd gevraagd om hun identiteitsbewijs te uploaden ter identificatie. Meest in het oog springend echter was de boete van 3,7 miljoen euro die werd opgelegd aan de Belastingdienst, vanwege illegale verwerking van persoonsgegevens in de Fraude Signalering Voorziening. Dat was een zwarte lijst waarop de Belastingdienst signalen van fraude bijhield. Met vaak grote gevolgen voor mensen die ten onrechte op die lijst stonden.

Over bovenstaande ontwikkelingen zou een nog veel langer verhaal geschreven kunnen worden, maar dat zou in het kader van een inleiding bij de jaarrapportage van de FG te ver voeren. De korte versie volstaat denk ik om te kunnen concluderen dat het onderwerp privacy – als onvermijdelijke pendant van de digitale samenleving – ons allen aan gaat en ook aan belang toeneemt. Iedere organisatie heeft zich tot dit onderwerp te verhouden, zowel inzake relatief operationele onderwerpen als adressenbestanden en smoelenboeken als inzake meer filosofische onderwerpen als het gebruik van data en persoonsgegevens voor de (grootschalige) monitoring (en mogelijk beïnvloeding) van mensen en hun omgeving. Bij die laatste onderwerpen gaat het dan mogelijk ook niet alleen meer om de vraag 'wat mag ik allemaal' conform de geldende wet- en regelgeving, maar ook om de vragen als 'wat wil ik eigenlijk' en 'waarom'. De mate waarin een organisatie zich met die privacy vragen bezig moet houden is overigens geen statisch

gegeven. Het hangt steeds samen met de ambities die de organisatie heeft in de digitale wereld (en dus met de hoeveelheid data en persoonsgegevens die de organisatie verwerkt), de omvang van de risico's die de betrokken (wier persoonsgegevens het betreft) lopen, en de middelen die de organisatie redelijkerwijs kan inzetten om die risico's te mitigeren. De AVG, als belangrijkste kader waaraan dit getoetst moet worden, houdt ook nadrukkelijk rekening met deze drie aspecten.

Ik ben op 3 oktober 2022 gestart in mijn rol als Functionaris Gegevensbescherming (FG) van de provincie Utrecht (PU); daarvoor was ik werkzaam als privacy officer (PO) bij de PU. Conform artikel 7 lid 6 van het Statuut Gegevensbescherming zoals vastgesteld door Gedeputeerde Staten op 2 juli 2019, 'brengt de FG jaarlijks verslag uit aan de algemeen directeur en Gedeputeerde Staten over de stand van zaken met betrekking tot de naleving van de AVG door de provinciale organisatie'.

In deze jaarrapportage geef ik als FG een overzicht van de belangrijkste ontwikkelingen op het gebied van privacy binnen de PU in het jaar 2022. Op onderdelen doe ik daarbij ook aanbevelingen om de naleving van privacy regels te verbeteren. Het is daarbij van belang te op te merken dat 'de naleving van privacy regels' geen 'afvinklijst' is die bij tijd en wijle door een privacy team wordt afgewerkt. Privacy aspecten komen continu voor bij vrijwel alle processen en alle medewerkers van de organisatie. Denk aan het versturen van uitnodigingen, het aanmaken van een nieuwe Teams-site, het aanschaffen van een nieuwe applicatie of het opzetten van een website, het starten van een nieuw (datagedreven) onderzoek, etc. En doordat alle medewerkers via hun *devices* verbonden zijn met de diverse interne en externe netwerken, zijn we per definitie allemaal een schakel in de omgang met data en persoonsgegevens door de PU, waarbij we dus ook allemaal een verantwoordelijkheid dragen om hier zorgvuldig mee om te gaan en er voldoende kennis over te hebben. Privacy hoort dus, net als bijvoorbeeld vertrouwelijkheid en integriteit, in het DNA van iedere medewerker te zitten. Dat het management en bestuur hierin een extra verantwoordelijkheid hebben, doordat zij eigenaar zijn van de processen en tevens een voorbeeldfunctie hebben naar de rest van de organisatie ('*tone at the top*') spreekt voor zich maar kan toch niet voldoende benadrukt worden. Laten we gezamenlijk het motto van het programma informatieveiligheid en privacy naleven: *'Wij maken de provincie Utrecht iedere dag veiliger'.*

Utrecht, 28 april 2023

EUGENE REBERS
Functionaris Gegevensbescherming

1. Privacy Volwassenheid

De AVG is een Europese verordening met relatief weinig concrete resultaatverplichtingen en veel open normen. Hiermee wordt bewerkstelligd dat de verwerkersverantwoordelijke de maatregelen kan afstemmen op '[…] de aard, omvang, context, doeleinden en risico's van de verwerkingen', en daarbij ook rekening mag houden met 'de stand van de techniek en de uitvoeringskosten'. Het gaat dus vooral om het treffen van adequate maatregelen die 'passend' zijn voor de organisatie. Vanwege het ontbreken van een concrete 'afvinklijst' is het niet goed mogelijk om een absolute uitspraak te doen over de vraag of een instelling aan de AVG voldoet.

Als alternatief heeft het Centrum Informatiebeveiliging en Privacy (CIP) een systeem beschreven van verschillende volwassenheidsniveaus met de bijbehorende maatregelen. 'Privacy volwassenheid' geeft aan hoe volwassen de organisatie is in de borging van privacy. Er worden vijf volwassenheidsniveaus onderscheiden, grofweg van geen of versnipperde aandacht voor privacy (niveau 1), tot perfecte organisatie brede beheersing en benutting van de privacybescherming (niveau 5).

Het CIP heeft tevens een Self Assessment ontwikkeld waarmee organisaties aan de hand van een uitgebreide vragenlijst zelf het volwassenheidsniveau van de organisatie kunnen bepalen. Deze vragenlijst is ingedeeld in de hoofdonderwerpen:

- Privacy Beleid
- Privacy Uitvoering
- Privacy Control

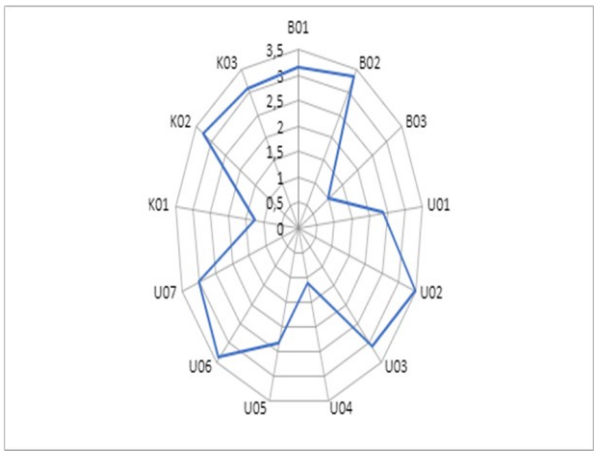
Naast het vaststellen van de volwassenheid geeft de Self Assessment ook inzicht in de maatregelen die nog genomen moeten worden om – indien gewenst – te groeien in volwassenheid.

De provincie Utrecht heeft zich tot doel gesteld te groeien naar volwassenheidsniveau 3, een niveau dat ook volgens het CIP een redelijk volwassenheidsniveau is voor de meeste 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. Binnen de provincie worden persoonsgegevens verwerkt (waaronder ook gevoelige of bijzondere persoonsgegevens, zoals personeelsgegevens, camerabeelden en BIBOB-gegevens), maar de provincie kent geen grootschalige verwerking van zeer gevoelige gegevens, zoals bijvoorbeeld de politie. Volwassenheidsniveau 3 is daarmee proportioneel.

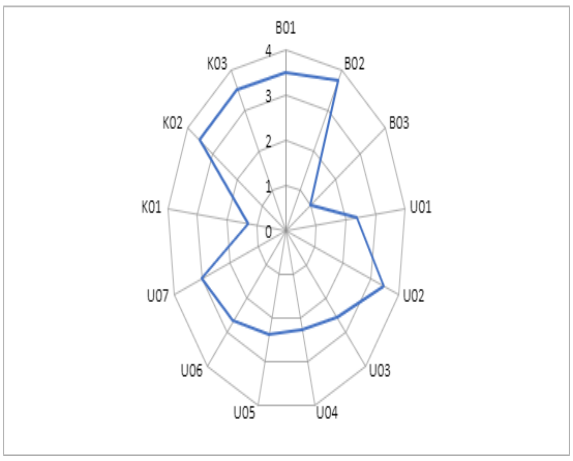
Van belang is om op te merken dat het behalen van het gestelde volwassenheidsniveau niet betekent dat het daarna 'klaar' is. Om dit niveau te handhaven is continu aandacht en inzet nodig voor effectieve uitvoering en monitoring van vastgesteld beleid, en voor aanpassing van dit beleid aan interne en externe ontwikkelingen.

Het programma IV&P heeft besloten om het hierboven beschreven CIP 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 dit voor de eerste keer gedaan, en ook in 2022 is dat weer gedaan. In Figuur 1 zijn de resultaten van beide jaren grafisch weergegeven.

De gemiddelde score qua volwassenheidsniveau over alle onderdelen is licht gezakt van 2,7 in 2021 naar 2,6 in 2022. Een 5-punts-schaal is echter niet tot achter de komma heel nauwkeurig, dus het is veilig om te concluderen dat het volwassenheidsniveau gelijk is gebleven en ook dit jaar nog net onder de gewenste waarde van 3 zit. Er kan ook in positieve zin op gewezen worden dat het aantal onderdelen dat onder de 3 scoort licht is gedaald, van 7 naar 5 onderdelen.



2022



2021

Score	*15-12-2022*	*29-11-2021*
Gemiddelde score	**2.6**	**2.7**
Onderdelen met score > 3.0	8	6
Onderdelen met score 2.0 - 2.9	2	5
Onderdelen met score 1.0 - 1.9	3	2
Onderdelen met score < 1.0	0	0

Figuur 1: Vergelijking CIP Self Assessment scores 2022 en 2021

De meerwaarde van dit assessment zit niet zo zeer in de exacte hoogte van de cijfers, maar in het bestuderen van de redenen waarom bepaalde onderdelen laag scoren, omdat dit inzicht geeft waar de komende periode de belangrijkste verbeteringen moeten worden doorgevoerd. Voor de drie onderdelen die in 2022 lager scoorden dan niveau 2 levert dit het volgende beeld op (een uitgebreidere analyse voor alle onderdelen is te vinden in de bijlage):

- ***Geen gestructureerd risicomanagement.*** Het uitvoeren van (updates van) risicoanalyses (waaronder Quickscans en DPIA's) wordt niet procesmatig afgedwongen en hangt daarmee te veel af van de individuele affiniteit van de proceseigenaren met dit onderwerp. Er is ook geen proces om te monitoren of voorgestelde maatregelen ter mitigering van de risico's worden geïmplementeerd en nageleefd.
- ***Informatiebeveiliging niet op het gewenste niveau***. De PU voldoet niet aan de voor iedere overheidsorganisatie geldende norm van de BIO (Baseline Informatiebeveiliging Overheid), en er is ook geen helder actieplan met wat gedaan moet worden en wie daarvoor per onderdeel verantwoordelijk is. Daarnaast bestaat er een grote achterstand met betrekking tot specifiek uit te voeren beveiligingsrisicoanalyses.
- ***Geen gestructureerd intern toezicht.*** De PU is vooral nog bezig met opzetten/implementeren van beleid, kaders en richtlijnen voor privacy, waardoor er nog weinig aandacht is geweest voor monitoren en houden van toezicht. Richtlijnen en werkwijze voor het houden van toezicht conform het *Three Lines of Defence* model zijn nog onvoldoende uitgewerkt. Het is onvoldoende duidelijk wat er gecontroleerd dient te worden, op welke wijze en aan wie gerapporteerd dient te worden.

2. Beleid

2.1. Privacybeleid en informatiebeveiligingsbeleid

Op het gebied van privacybeleid is goede voortgang geboekt in 2022. Bestaand beleid (en indien aanwezig bijbehorende werkinstructies) wordt voor alle medewerkers goed toegankelijk ontsloten via Intranet,

en verder toegelicht in de periodieke sessies met de IV&P contactpersonen. Er wordt gewerkt met een doorlopende jaarkalender om dit bestaande beleid periodiek te actualiseren en waar nodig aan te vullen met nieuw beleid en/of werkinstructies. In 2022 is nieuw beleid ontwikkeld ten aanzien van zowel de bewaartermijn van persoonsgegevens als de wettelijke grondslag voor de verwerking van persoonsgegevens. Actualisatie van het beleid heeft plaats gevonden inzake de onderwerpen 'rechten van betrokkenen' en het uitvoeren van DPIA's. Ook is de procedure datalekken uitgebreid, waarbij nu onder andere meer aandacht is voor de processtap 'leren van het datalek' inclusief de vastlegging daarvan. Tot slot zijn ook de externe privacy statements van de provincie Utrecht geactualiseerd.

Op het gebied van informatiebeveiliging is het beeld wat minder compleet. Weliswaar is er een algemeen geldend informatiebeveiligingsbeleid, maar op diverse deelonderwerpen is nader beleid vereist dat nog niet aanwezig of verouderd is. In 2022 is wel gewerkt aan bijvoorbeeld ICT-middelenbeleid, logisch toegangsbeleid en back-up en restorebeleid, maar dit beleid is nog niet vastgesteld en omvat ook slechts een gedeelte van wat nog ontwikkeld moet worden. Hier is een relatie te trekken met het nog niet voldoen aan de BIO (zie paragraaf 7), omdat dit nadere beleid ook conform de BIO een vereiste is. Het is van belang om meer centraal inzicht te krijgen in wat nog benodigd is op het gebied van informatiebeveiligingsbeleid, en dat er vervolgens ook meer gestuurd gaat worden op het wegwerken van de achterstand.

2.2. Nieuwe wet- en regelgeving

Zoals in de inleiding al aangegeven, zal de komende jaren een grote hoeveelheid nieuwe wet- en regelgeving van kracht worden op de aan elkaar gerelateerde gebieden van digitale dienstverlening, privacy en informatiebeveiliging. Onder de paraplu van de in 2020 gepubliceerde datastrategie en cybersecuritystrategie heeft de Europese Unie een grote hoeveelheid aan nieuwe regelgeving in voorbereiding. De Europese Commissie wil hiermee bereiken dat de digitale markt competitief is en heldere spelregels heeft (Verordening digitale markten, Verordening digitale diensten), dat het datagedreven werken wordt bevorderd (Open data richtlijn, Data governance verordening, Data verordening), en dat de informatieveiligheid toeneemt (Richtlijn netwerk- en informatiebeveiliging, Cyberbeveiligingsverordening, Verordening horizontale cyberbeveiligingsvereisten). Daarnaast bereidt de Europese Unie een Verordening inzake kunstmatige intelligentie voor, waarmee afgebakend wordt wanneer kunstmatige intelligentie mag worden ingezet en welke transparantie daarover moet worden betracht. Ook in Nederland zijn er diverse wetten die onlangs van kracht zijn geworden of dat binnenkort zullen worden, welke de komende jaren stapsgewijs steeds meer eisen zullen stellen aan het informatiebeheer en de actieve openbaarmaking van documenten bij overheidsinstellingen. De belangrijkste hiervan zijn de Wet Open Overheid, de Omgevingswet en de Wet Digitale Overheid. Daarnaast is eind 2022 in Nederland het Algoritmeregister van start gegaan, wat nu nog op basis van vrijwilligheid wordt gevuld, maar wat naar verwachting binnen 1 à 2 jaar een verplichting zal worden.

De hierboven beschreven achterstand in bestaand beleid, in combinatie met de grote hoeveelheid nieuw te implementeren beleid, maakt dat een stevige inspanning nodig is om het gehele 'i-beleidskader' van de PU op orde te krijgen. Wat meespeelt bij het ontstaan van de achterstand is het feit dat de verantwoordelijkheid voor het maken van de benodigde beleidsdocumenten over meerdere afdelingen verdeeld is (zoals met name IEA, maar ook bijvoorbeeld HR, Inkoop, Facilitair, en soms de beleidsdomeinen), en dat deze afdelingen meer gericht zijn op de operatie dan op beleid en compliance. Het is daarom aan te bevelen een sterkere regierol in te richten ten aanzien van het 'i-beleidskader'. Begin 2023 is hier een goede eerste stap in gezet door hiervoor een specifiek project te starten. Ten eerste kan hiermee een beter overzicht worden gecreëerd ten behoeve van het kunnen aantonen dat wordt voldaan aan wet- en regelgeving. De sterkere regierol maakt het ook mogelijk om waar nodig te prioriteren in het implementatietraject. En *last but not least* kan vanuit de regierol ook de samenhang tussen de diverse met elkaar samenhangende beleidsonderwerpen in de i-kolom worden bewaakt. Onderliggend hebben de (nieuwe) beleidskaders namelijk allemaal hun weerslag op de informatiehuishouding van de PU in de breedste zin

van woord. Afstemming tussen de diverse trajecten is dus hoogst wenselijk vanuit het oogpunt van synergie, en noodzakelijk om in ieder geval geen strijdigheden tussen de trajecten te krijgen. Denk hierbij aan onderwerpen als de governance structuur van de data, samenhang in het applicatielandschap, compatibiliteit in de onderliggende architectuur, en eenduidige privacy- en informatieveiligheidsnormen (inclusief beheerafspraken en monitoring van naleving daarvan). Regie op en afstemming tussen de diverse beleidstrajecten is tot slot ook van belang om deze in lijn te laten zijn met het (nog te maken) informatieplan van de PU.

2.3. 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 tussen de bij het *Three Lines of Defense* model betrokken functionarissen die een rol spelen bij de bescherming van persoonsgegevens. Tijdens genoemde vergadering heeft GS ook besloten tot evaluatie van het Statuut.

De opdracht voor deze evaluatie is extern uitgezet. In december 2021 heeft het bureau Verdonck, Klooster & Associates 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 is het *Three Lines of Defense* model 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?

Het Statuut, inclusief de beschrijving van het *Three Lines of Defense* model en de rol van de FG daarbinnen, geeft volgens de uitkomsten van de evaluatie voldoende richting aan de governance van de privacy functie binnen de PU. Er zijn ook geen strijdigheden met de bepalingen in het privacybeleid, maar er is wel overlap. Dit zal in 2023 worden opgepakt bij de reeds geplande actualisering van het privacybeleid. In dat laatste beleid zullen de onnodige dubbelingen worden geschrapt, zodat het Statuut zich toespitst op de governance van de privacy functie binnen de PU, en het privacybeleid op de inhoudelijke aspecten ervan.

De evaluatie noemt de werking van het *Three Lines of Defense* model in de praktijk wel een belangrijk aandachtspunt. Een belangrijk voorbeeld dat wordt genoemd is dat de informatiestroom tussen de eerste lijn (de team(leider)s) en de tweede lijn (de PO's) nog niet optimaal is. Om adequaat te kunnen adviseren en toe te zien op naleving van de privacy wetgeving dienen de PO's tijdig bij dossiers betrokken te worden en afdoende informatie te hebben. Omdat er voor de PO's te veel teams zijn om zelf proactief betrokken te kunnen blijven, is er vanuit de teams ondersteuning nodig. Een eerste aanzet hiertoe is gegeven via het Netwerk IV&P Contactpersonen, maar deelname aan dit netwerk is te vrijblijvend en wordt niet organisatiebreed opgepakt (zie ook paragraaf 3.2). Een mooie kans op verbetering ligt in de aanstelling van IV&P medewerkers (IV&P kan ook onderdeel zijn van een breder taakpakket van die medewerkers) binnen de in oprichting zijnde stafbureaus. Daarbij is het dan wel van belang dat die stafbureaus zich uitstrekken over de hele organisatie (dus domeinen, maar ook projecten en opgaven) en dat de proactieve informatiestroom tussen de eerste en tweede lijn expliciet wordt opgenomen in het takenpakket van de genoemde medewerkers.

3. Bewustwording

Zoals aangegeven in het voorwoord is het waarborgen van voldoende privacy niet iets wat een privacy team *in splendid isolation* voor elkaar kan krijgen. In de digitale wereld waarin we leven heeft ieder team en iedere medewerker hierin ook een eigen verantwoordelijkheid. De AVG benoemt expliciet dat het voor organisaties belangrijk is om hun medewerkers hiervan bewust te maken (‘*awareness*’). Het IV&P team heeft in 2022 dan ook veel tijd besteed aan bewustwordingsactiviteiten en heeft daarmee bereikt dat veel medewerkers het belang van privacy beter begrijpen en hun kennis daarover is vergroot. Zo zijn (soms op verzoek) vrijwel alle managementteams bezocht, de ene keer om algemene uitleg te geven over privacy en een andere keer om specifieke onderwerpen toe te lichten, zoals het IV&P dashboard. Ook zijn specifieke momenten of thema’s (denk aan thuiswerken, veilig gebruik van mobiele telefoon en laptop op vakantie, en de Week van het Vertrouwen) aangegrepen om via bijvoorbeeld posters of berichten op Intranet gericht te communiceren over bepaalde onderwerpen. Hieronder worden de opleiding en het netwerk IV&P contactpersonen verder belicht.

3.1. Opleiding

Aan het begin van 2022 zijn voor alle medewerkers de e-learning modules over IV&P beschikbaar gesteld. Het maken van de modules is niet verplicht maar wordt wel sterk aangemoedigd. Het belang van bewustwording op medewerkersniveau kan niet genoeg benadrukt worden. Keer op keer blijkt uit onderzoeken dat (bewuste maar vooral ook onbewuste) menselijke fouten van medewerkers het belangrijkste risico zijn op het gebied van informatieveiligheid.

Afgezet tegen het bovengenoemde belang, moet gesteld worden dat de deelname aan de e-learning modules ondermaats is. In de eerste helft van het jaar kwam het cumulatieve deelnamepercentage maar net boven de 10% uit. In het derde kwartaal was dit – mede na twee oproepen van de algemeen directeur – opgelopen naar iets boven de 30%. In het begin van het vierde kwartaal is op medewerker niveau gedeeld wie de e-learning heeft gevolgd, zodat teamleiders hier beter op kunnen sturen. Ook hebben domeinmanagers beter inzicht gekregen in de mate waarin de teams in hun domein aan de e-learning deelnemen. Eind 2022 is het percentage opgelopen tot iets boven de 50%, nog steeds te laag dus.

Onderdeel van de e-learning is ook dat er wekelijks een vraag naar alle medewerkers wordt gestuurd op het gebied van IV&P om dit onderwerp blijvend onder de aandacht te brengen. Ongeveer 50% van de medewerkers doet stabiel mee aan het beantwoorden van deze wekelijkse vraag, maar er is een aanzienlijk percentage van ongeveer 40% van de medewerkers die de wekelijkse vraag eigenlijk nooit beantwoordt.

De e-learning vraagt dus om blijvende aandacht. En ook om budget. Bestaande modules en wekelijkse vragen moeten immers up-to-date gehouden worden, en nieuwe modules moeten worden ontwikkeld om te blijven aansluiten bij de actualiteit. Als de deelnamepercentages ondanks alle inspanningen van IV&P en management ondermaats blijven, moeten wellicht ook manieren worden bedacht om het meer verplichtend te maken. Zo is onlangs het idee geopperd om de uitgifte van laptops te koppelen aan het doorlopen van de e-learnings.

3.2. Netwerk 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 IV&P ondersteunt daarin, maar kan vanzelfsprekend niet overal in de organisatie aanwezig zijn. Daarom is het programma IV&P in 2021 begonnen met het opbouwen van een netwerk van IV&P contactpersonen,

waarbij alle teams binnen de PU zijn uitgenodigd om hieraan deel te nemen. Via deze contactpersonen kan kennis en ervaring op het gebied van IV&P worden uitgewisseld. Dat werkt twee kanten op. Enerzijds kunnen contactpersonen meehelpen om de medewerkers uit te leggen wat van hen wordt verwacht. En anderzijds kunnen de contactpersonen aangeven welke onderwerpen er binnen de organisatie spelen en welke ondersteuning medewerkers nodig hebben om aan de genoemde verwachtingen te voldoen.

In 2022 is het netwerk 3 keer bij elkaar gekomen. Naast het bespreken van actuele onderwerpen (zoals de kwetsbaarheid log4j waar eind 2021/begin 2022 veel om te doen was) zijn o.a. het verwerkingsregister, de vertrouwelijkheidslabels, de e-learning en de grootste IV&P risico's besproken. Uit een korte evaluatie van de werking van het netwerk is naar voren gekomen dat het bijdraagt aan het vergoten van de bewustwording van dit onderwerp binnen de organisatie. Abstracte beleidsregels worden zo beter geoperationaliseerd, en mensen weten elkaar beter te vinden als er iets speelt. De effectiviteit van het netwerk heeft wel sterk te lijden onder de lage opkomst tijdens de bijeenkomsten (sommige teams hebben überhaupt geen contactpersoon aangewezen). Ook blijkt uit de evaluatie dat niet alle contactpersonen een terugkoppeling geven van het besprokene aan hun eigen teams. Wellicht dat de stafbureaus binnen de domeinen waarover thans wordt gesproken hierin een nuttige rol kunnen vervullen.

4. Privacy informatie

4.1. 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. In het bijbehorende beleidsdocument is uitgewerkt dat de teamleider verantwoordelijk is voor de juistheid van de verwerkingen in het register die zijn team uitvoert. Dit betekent dat nieuwe verwerkingen worden opgenomen, informatie over bestaande verwerkingen actueel wordt gehouden, en dat verwerkingen die niet meer actief zijn ook daadwerkelijk uit het verwerkingsregister worden verwijderd. De privacy officers doen het functioneel beheer van het verwerkingsregister, en ondersteunen teamleiders en medewerkers bij het actueel houden ervan, onder andere door voorlichting te geven, standaardformulieren te ontwikkelen, en periodiek uitvraag te doen naar de actualiteit van (onderdelen van) het verwerkingsregister.

Nadat de privacy officers eind 2021 zelf, op basis van de bij hen bekende informatie, een stevige actualisatieslag van het verwerkingsregister hadden gemaakt, hebben zij in het voorjaar van 2022 een brede oproep gedaan aan alle teamleiders en opgavemanagers om het Verwerkingsregister te controleren en eventuele noodzakelijke wijzigingen door te geven. Ondanks een ruime reactietijd (incl. de herinneringsemail had men 3 maanden de tijd) heeft slechts 50% gereageerd (met als positieve uitschieter BDV (89%) en negatieve uitschieter LLO (16%)). Door de lage respons heeft de PU geen actueel en volledig inzicht in haar processen waarbij persoonsgegevens verwerkt worden. Los van het feit dat dit een boetewaardige overtreding van de AVG is, betekent dit bijvoorbeeld ook dat (prioritering van) risicomanagement wordt bemoeilijkt en dat minder adequaat kan worden gehandeld bij incidenten (zoals datalekken).

De privacy officers zullen verdere gerichte uitvragen doen om het beeld (meer) compleet te krijgen, maar het verdient aanbeveling dat teamleiders meer proactief bewerkstelligen (al dan niet via hun IV&P contactpersonen of stafbureaus) dat het verwerkingsregister up-to-date is.

4.2. Rapportages

Ieder kwartaal stelt het privacy team een rapportage op, met daarin de belangrijkste informatie over de bestaande verwerkingen en een korte analyse daarvan. Deze rapportages worden ter informatie aan het CMT gestuurd, en worden vervolgens ook opgenomen op de Intranetpagina van het IV&P team.

In 2022 heeft het programma IV&P samen met DKI het IV&P Dashboard ontwikkeld. Op basis van onderliggende data zoals met name het verwerkingsregister en het incidenten- en datalekregister is nu de belangrijkste informatie over de verwerking van persoonsgegevens beschikbaar, zoals aantallen verwerkingen en de daarin gebruikte persoonsgegevens, afgesloten verwerkersovereenkomsten, datalekken, uitgevoerde risicoanalyses en de e-learnings. Deze informatie kan gefilterd worden naar bijvoorbeeld team, domein en/of periode. Het Dashboard is in vele MT's gepresenteerd en is inmiddels ook toegankelijk voor de business controllers. In de komende periode kan mede door de interactie met gebruikers het Dashboard verder uitgebreid en verfijnd worden.

Naast het bieden van inzicht kunnen rapportages vooral van toegevoegde waarde zijn als deze worden gebruikt in de planning- en control cyclus, dus in het goede gesprek en de managementgesprekken, waarbij informatie uit de rapportages kan worden gebruikt om afspraken te maken en de voortgang daarvan te monitoren en waar nodig bij te sturen. Ervaringen met deze gespreksrondes kunnen dan vervolgens ook weer goede input bieden voor uitbreiding en/of verdere verfijning van de rapportages. Het is daarbij goed voorstelbaar dat de kwartaalrapportages en het Dashboard – die in verschillende periodes en separaat zijn ontwikkeld en vrij veel overlap vertonen – op den duur op elkaar worden afgestemd of geïntegreerd worden tot één geheel.

5. Organisatie

In 2019 is de PU gestart met het programma Informatieveiligheid & Privacy (hierna IV&P). Het doel van het programma IV&P was het niveau van informatieveiligheid en privacy structureel te verbeteren en in te bedden in de provinciale organisatie. Het programma IV&P is niet gestart omdat informatieveiligheid en privacy een tijdelijk karakter hebben, maar omdat een intensieve aanpak nodig was om de organisatie te laten groeien. Dit mede in het licht van de in de inleiding reeds genoemde toenemende digitalisering en de door GS geformuleerde ambities op dit terrein. De organisatie heeft een stevige verantwoordelijkheid te vervullen richting onze burgers, samenwerkingspartners en andere stakeholders om de aspecten informatieveiligheid en privacy (en overigens ook digitale toegankelijkheid) voldoende te betrekken in de digitale ontwikkelingen.

Mede door het programma IV&P zijn een aantal belangrijke successen geboekt, zoals in de diverse paragrafen van deze rapportage naar voren komt. Maar er is ook nog veel te doen. Op basis van de meeste recente self-assessments kan worden geconcludeerd dat de provincie voor privacy weliswaar nagenoeg op het gewenste procesvolwassenheidsniveau zit, maar dat het vasthouden van dit niveau voortdurende aandacht vergt en dat de laatste stapjes om het gewenste niveau 3 te bereiken weerbarstig blijken. Voor informatieveiligheid moet de organisatie nog een stevige groei doormaken, zoals ook aangegeven in paragraaf 7 van deze rapportage.

Op het moment van schrijven van deze rapportage vinden de laatste voorbereidingen plaats voor het afronden van het programma IV&P en het daarmee overdragen van IV&P 'naar de lijn'. Het is belangrijk om stil te staan bij dat moment, omdat deze overdracht de *governance* structuur van privacy (de AVG spreekt van 'de toewijzing van verantwoordelijkheden') binnen de PU voor de komende tijd vastlegt en daarmee bepalend is voor met welke intensiteit en vanuit welk perspectief de diverse privacy onderwerpen in de toekomst zullen worden opgepakt.

Een eerste aspect wat ik hierbij zou willen belichten is het feit dat privacy officers niet alleen advies geven en meewerken bij het regelen van allerlei privacy zaken, maar dat zij tegelijkertijd ook vanuit hun 2^{e} lijns rol erop moeten toezien dat een en ander binnen de wettelijke kaders gebeurt. Het Statuut voor Gegevensbescherming spreekt bijvoorbeeld van het stellen van kaders, signaleren en rapporteren, toetsen van naleving van verwerkersovereenkomsten, monitoren van risicobeheersingsmaatregelen, etc. Het is logisch dat in de afgelopen periode (de 'opbouwfase') het accent grotendeels op advies en ondersteuning

heeft gelegen. Zaken moeten worden ingeregeld, kennis opgebouwd en bewustzijn gecreëerd, en aanjagen en opbouwen kosten nu eenmaal veel tijd. Maar nu de opbouwfase grotendeels is afgerond en de 1e lijn ook een flink aantal zaken zelf (proactief) kan oppakken (daarbij waarschijnlijk gesteund door de stafbureaus waar nu over wordt gesproken), ligt het in de rede dat – naast het advies dat natuurlijk gewoon blijft doorgaan – er een accentverschuiving plaats gaat vinden naar de toezichtsactiviteiten. In lijn daarmee verdient het dan ook aanbeveling om de privacy officers onder te brengen op een relatief onafhankelijke en herkenbare plek die recht doet aan deze 2e lijns rol (kaderstelling, advies, ondersteuning en monitoring).

Een tweede aspect dat ik zou willen belichten is dat het werk van de privacy officers (net als van veel andere 'i-medewerkers', waaronder de information security officers) en de wijze waarop zij dit in lijn met de brede organisatiedoelstellingen moeten invullen zeer nauw verweven is met en afhankelijk is van de (invulling van de) brede 'i-visie' van de organisatie (datagedreven en digitaal werken en de invulling van de compliance aspecten daarvan). Mark Vermeer, sinds 1 november 2022 Directeur Digitale Overheid van het ministerie van BZK, zegt het volgende over die integraliteit van de ICT-functie: 'Vroeger regelde de afdeling ICT alles wat met de computer te maken had. Maar ondertussen heeft al het werk van de overheid een digitaal aspect. De scheidslijn tussen ICT als bedrijfsvoeringsfunctie en ICT als onderdeel van het primair proces begint te vervagen. Basiskennis van digitalisering is belangrijk om je tent goed te kunnen runnen.' In dat licht bezien moeten de IV&P activiteiten dan ook in een bredere context worden gemanaged, waarbij op basis van een 'i-visie' kaders worden gesteld (en afgedwongen), activiteiten geprioriteerd, voortgang en risico's worden gerapporteerd, en waarbij op basis van de voortgang ook kan worden bijgestuurd (inclusief mogelijke budgetwijzigingen indien nodig). Die integrale i-managers-rol was binnen de PU voorzien voor de CIO, en deze is in 2022 (overigens zonder effectief mandaat) ook actief geweest, maar het CMT heeft eind 2022 besloten niet in te stemmen met zijn plan van aanpak voor het vervolg. Het verdient aanbeveling dat de noodzakelijke integrale aanpak van de i-functie op een andere manier alsnog wordt geborgd, en dat de privacy functie daarin wordt ondergebracht.

> 'De scheidslijn tussen ICT als bedrijfsvoeringsfunctie en ICT als onderdeel van het primair proces begint te vervagen. Basiskennis van digitalisering is belangrijk om je tent goed te kunnen runnen.'
>
> Mark Vermeer, Directeur Digitale Overheid bij Ministerie van BZK, in Publiek Denken 40-2023

Ik zou deze paragraaf willen afsluiten met de notie dat met het einde van het programma IV&P en de onderbrenging van de privacy officers in de lijn, de hoeveelheid taken van de privacy officers niet afnemen (eerder toenemen gelet op de uitdijende digitale agenda), maar vooral, zoals toegelicht, van aard veranderen. Daarnaast blijft van belang om te beseffen dat het vasthouden (en waar nodig groeien) van de volwassenheid ten aan zien van privacy (en informatieveiligheid) alleen gerealiseerd kan worden wanneer dit onderwerp door de hele organisatie heen wordt omarmd. Iedere medewerker maakt dagelijks gebruik van de digitale infrastructuur van de PU en kan die infrastructuur, inclusief de daarin gebruikte persoonsgegevens, beïnvloeden, bijv. door gebruik van apparaat en wifiverbindingen, het creëren en delen van documenten en andere (persoons)gegevens, het opzetten van een website of het aangaan van een samenwerkingsovereenkomst; voldoen aan de privacyregels begint met gezond verstand (hoe zou ik willen dat een organisatie met mijn persoonsgegevens omgaat), (een minimum aan) kennis, en een juiste antenne (al dan niet afgedwongen door processen) om op gepaste momenten advies in te winnen bij een collega, leidinggevende of het IV&P team. Ik doe daarbij een oproep aan het management om te sturen op deze verantwoordelijkheid, daarbij ondersteund door de deskundigen op dit gebied.

6. Risicomanagement

Risicomanagement van (persoons)gegevens is een continu proces dat (privacy)risico's signaleert, beoordeelt, waar nodig verkleint en bewaakt. Het begint met het uitvoeren van een Quickscan (voorheen de Business Impact Analyse – BIA – genoemd), waarin de betrokken (persoons)gegevens worden geanalyseerd met behulp van de criteria beschikbaarheid, integriteit (kwaliteit) en vertrouwelijkheid. Op basis van deze analyse wordt onder andere bepaald of een DPIA noodzakelijk is (als er een hoog risico is voor de betrokken om wier persoonsgegevens het gaat) en ook of een aanvullende risicoanalyse noodzakelijk is (als de gegevens cruciaal zijn voor de PU en/of haar belanghebbenden).

6.1. DPIA's

Op grond van de AVG is het noodzakelijk dat voor verwerkingen met een hoog risico voor de betrokkenen een DPIA wordt uitgevoerd. Deze DPIA moet worden uitgevoerd voordat de verwerking van start gaat. In de loop van 2022 is de relatief grote achterstand die was opgelopen bij het uitvoeren van DPIA's significant weggewerkt. Waar aan het eind van 2021 nog sprake was van 9 uit te voeren DPIA's (dus verwerkingen die toch al zonder benodigde DPIA van start waren gegaan), was dit aantal eind 2022 terug gelopen naar 1.

Ondanks het wegwerken van de achterstand, wat een belangrijke prestatie in 2022 genoemd mag worden, is er toch een belangrijk aandachtspunt te noemen bij het proces van DPIA's. Zoals gezegd dienen deze te worden afgerond vóórdat de verwerking van start gaat. Het komt voor dat een DPIA onder hoge tijdsdruk afgerond moet worden omdat de verwerking snel van start moet gaan. Dit komt de zorgvuldigheid niet ten goede en kan bijvoorbeeld afbreuk doen aan het benodigde proces van *privacy by design* zoals genoemd in artikel 25 van de AVG. Het komt helaas ook nog wel eens voor dat de DPIA wordt ingepland terwijl de verwerking al gestart is. Dit is niet alleen een boetewaardige overtreding van de AVG (dat de AP niet schroomt om boetes uit te delen bij het ontbreken van noodzakelijke voorafgaande risicoanalyses, blijkt uit de in de inleiding genoemde boete voor de Gemeente Rotterdam), maar veel belangrijker is dat hierdoor potentieel grote risico's voor de betrokkenen ontstaan doordat onrechtmatig of onzorgvuldig met hun persoonsgegevens wordt omgegaan.

Zowel de verplichting om een Quickscan alsook – onder omstandigheden – een DPIA uit voeren is opgenomen in het Algemeen Privacybeleid, maar wordt verder niet procesmatig afgedwongen. Het verdient aanbeveling om dat wel te doen, bijvoorbeeld in een '*New Product Approval Process*' en/of door systematische bespreking van de '*i-portfolio*' in een periodiek overleg met voldoende mandaat.

6.2. PDCA

De PU bevindt zich vooral nog in de fase waarin Quickscans en DPIA's voor de eerste keer worden uitgevoerd. Voorkomen moet worden dat de organisatie de DPIA ziet als 'het zetten van een vinkje'. Immers, als de DPIA is afgerond begint vaak pas het echte werk. Met de DPIA is slechts in kaart gebracht waar risico's zich bevinden en welke maatregelen deze risico's kunnen mitigeren. Er is in de praktijk nog te weinig aandacht voor het concreet maken van maatregelen, het implementeren van deze maatregelen, en het beoordelen van de effecten van de geïmplementeerde maatregelen. Ook dient nog een stap gezet te worden naar een werkwijze waarbij Quickscans en DPIA's periodiek worden uitgevoerd. Zowel gewijzigde omstandigheden als de beoordeling van de effecten van de eerder geïmplementeerde maatregelen kunnen immers aanleiding zijn om de DPIA te herijken. De hele cyclus van het uitvoeren van een risicoanalyse (DPIA), het implementeren van mitigerende maatregelen, het beoordelen van de effectiviteit van die maatregelen, en het waar nodig aanpassen van die maatregelen wordt ook wel de *plan, do, check, act* (PDCA) cyclus genoemd, en vormt de basis van een daadwerkelijk privacy management systeem (PMS). Vaak wordt het IT-systeem dat een dergelijk continu proces ondersteunt ook een PMS genoemd,

maar een echt PMS is dus het hele beschreven continue proces en niet alleen het ondersteunende IT-systeem.

Het verdient aanbeveling om zowel de herijking van Quickscans en DPIA's als de monitoring van de daarin voorgestelde maatregelen meer structureel vorm te geven in een PDCA-cyclus.

7. Informatieveiligheid

Informatieveiligheid is een zelfstandige discipline met ook een veel breder aangrijpingsgebied dan alleen persoonsgegevens, maar het wordt hier toch beschreven omdat het veel invloed heeft op het volwassenheidsniveau van privacy. De AVG stelt immers dat voldoende technische en organisatorische maatregelen moeten worden getroffen om persoonsgegevens te beschermen.

Uit de Assessment Informatiebeveiliging 2021, uitgevoerd onder regie van CCO, blijkt dat de laatste tijd weliswaar op onderdelen goede vooruitgang is geboekt (bijvoorbeeld ten aanzien van bewustwording, kaderstelling, crisismanagement en het inrichten van en oefenen met een bijbehorend CERT, en het uitvoeren van Quickscans bij applicaties en processen om de IV&P risico's in beeld te brengen), maar dat de ontwikkeling naar een hoger volwassenheidsniveau zeer moeizaam verloopt en achterblijft bij de ambities (minimaal 2 en gewenste doorgroei naar 3). Dit is zorgelijk, omdat een vergelijkbaar beeld ook al uit de voorgaande Assessment uit 2019 naar voren kwam. De kern is een governance probleem: onduidelijk eigenaarschap van de (informatieveiligheidsrisico's van de) I-assets. Hierdoor is er geen overkoepelend beeld van de informatieveiligheidsrisico's, wordt er maar in beperkte mate over gerapporteerd, en dus ook niet (in samenhang met de I-ambities) op gestuurd. Daar waar de risico's wel in beeld zijn (bijvoorbeeld na de uitvoering van een Quickscan, DPIA of risicoanalyse) wordt niet procesmatig afgedwongen dat de voorgestelde beheersingsmaatregelen ook daadwerkelijk worden geïmplementeerd en wordt niet gemonitord of deze effectief zijn. Ook ten aanzien van leveranciers (verwerkers) is er onvoldoende monitoring van IV&P risico's, terwijl bekend is dat IV&P-gerelateerde incidenten vaak bij (de systemen van) leveranciers plaats vinden. Tot slot is tekenend dat al geruime tijd bekend is dat de PU niet voldoet aan de verplichte BIO, maar dat eind 2022 nog niet inzichtelijk is wat hiervoor allemaal moet gebeuren en wie er stuurt op de voortgang daarvan.

Zoals hierboven gezegd is het niet aan mij als FG om gedetailleerde aanbevelingen te doen op het gebied van informatiebeveiliging. Gelet op het belang van dit onderwerp van privacy wil ik wel de algemene aanbeveling doen om de managementaandacht voor de noodzakelijke versterking van de informatiebeveiliging van de PU te intensiveren, met bijzondere aandacht voor de governance van de I-assets en de rapportage aan en sturing door of namens het CMT.

8. Datalekken

Van een datalek is sprake (de AVG spreekt van een 'inbreuk in verband met persoonsgegevens') wanneer een inbreuk op de beveiliging leidt tot het verlies, of het ongeoorloofd wijzigen, verstrekken, inzien of anderszins verwerken van persoonsgegevens. Kort gezegd is er bij een datalek dus iets gebeurd met de persoonsgegevens wat niet de bedoeling was.

In 2022 zijn 18 datalekken gemeld bij de privacy officers. 2 van deze meldingen zijn vervolgens door de PU gemeld bij de AP vanwege de risico's voor betrokkenen. Deze meldingen zijn beide gedaan binnen de gestelde termijn van 72 uur na ontdekking. De AP heeft geen contact opgenomen voor nadere informatie of verder onderzoek.

Naast een melding bij de AP moeten in sommige omstandigheden ook de betrokkenen worden geïnformeerd, en wel als er sprake is van een hoog risico voor de betrokkenen. In 1 van de 2 bij de AP gemelde

datalekken zijn ook de betrokkenen geïnformeerd, onder andere omdat er bijzondere (medische) gegevens in het spel waren. In 2 andere gevallen was melding aan de betrokkenen juridisch gezien niet noodzakelijk, maar is dit uit zorgvuldigheidsoverwegingen toch gedaan.

In voorgaande jaren was bij de PU – net als bij veel andere organisaties – vaak verkeerd geadresseerde post of email de belangrijkste oorzaak van de datalekken. Dit jaar zien we een andere categorie als belangrijkste oorzaak, te weten de categorie 'Per ongeluk gepubliceerd, ten onrechte verwerkt, of te ruime autorisaties'. De in deze categorie gemelde datalekken zijn terug te voeren op de volgende gedragingen:

- te snel verleende autorisatie voor een nieuw account voordat het gehele benodigde proces was doorlopen;
- onbedoelde potentiële toegang tot een netwerkschijf ten tijde van een technische migratie (hier stonden ook de eerdergenoemde medische gegevens);
- te ruime toegang tot sollicitatiegegevens ten tijde van de uitrol van een nieuw personeelsadministratiesysteem;
- te ruime toegang tot HR-data voor de afdeling waar zogenoemde 'informatie dashboards' worden gemaakt;
- abusievelijke publicatie van persoonsgegevens op internet;
- onzorgvuldig gebruik van login gegevens bij het omwisselen van een laptop.

Naar aanleiding van de gemelde datalekken wordt altijd gekeken wat hiervan kan worden geleerd om het risico op herhaling te verkleinen. Dit wordt zowel met de betrokken proceseigenaar en medewerker alsook organisatiebreed opgepakt. Bovengenoemde datalekken onderstrepen onder andere nog eens het belang van een goede autorisatiestructuur, zowel op papier als in de praktijk. Bij implementatie van nieuwe systemen en processen moet er voldoende tijd worden ingebouwd om de autorisatiestructuur op te stellen en ook te testen voordat deze in productie wordt genomen. Het belang hiervan kan sterk toenemen als er meerdere afdelingen en/of derde partijen bij betrokken zijn. Ook na de implementatie zal de werking van de autorisatiestructuur systematisch (risicogebaseerd) moeten worden getest.

9. Derde partijen

Als de PU met een derde partij persoonsgegevens uitwisselt, moeten de belangen van betrokkenen voldoende gewaarborgd blijven. Vaak zal het noodzakelijk zijn om daarvoor een privacyovereenkomst met die derde partij te sluiten. Er zijn drie soorten privacyovereenkomsten, en welke gebruikt moet worden hangt met name af van wie het doel en de middelen bepaalt van de verwerking. Als dat de derde partij is, denk bijvoorbeeld aan een logistieke dienstverlener die adressen van de PU nodig heeft om een zending te kunnen verzorgen, dan kan een Gegevensleveringsovereenkomst worden afgesloten. De derde partij is dan primair verantwoordelijk voor een zorgvuldig gebruik van de persoonsgegevens, en met het opstellen van de Gegevensleveringsovereenkomst wordt die verantwoordelijkheid vastgelegd voordat de PU overgaat tot levering van de persoonsgegevens. In de meeste gevallen zal de PU zelf het doel en de middelen van de verwerking bepalen. Denk bijvoorbeeld aan een dienstverlener die de salarisadministratie voor de PU uitvoert, een softwarebedrijf dat een specifieke applicatie bouwt en/of onderhoudt voor de PU, een onderzoeksbureau dat interviews of enquêtes afneemt of anderszins persoonsgegevens verzameld in opdracht van de PU, of een beveiligingsbedrijf dat camerabeelden maakt in opdracht van de PU. In die gevallen is en blijft de PU primair verantwoordelijk voor een zorgvuldig gebruik van de persoonsgegevens. De derde partij is in dit geval een verwerker, en daarmee dient, voorafgaande aan de start van de dienstverlening, een verwerkersovereenkomst te worden opgesteld. Een derde soort van privacyovereenkomst is de Onderlinge Regeling. Deze moet worden opgesteld wanneer het doel en de middelen van de verwerking gezamenlijk worden bepaald door de PU en de derde partij. Beide partijen dragen dan gezamenlijk verantwoordelijkheid voor het zorgvuldig gebruik van de persoonsgegevens, en in de Onderlinge Regeling kunnen dan afspraken gemaakt worden wie voor welk onderdeel de primaire verantwoordelijkheid draagt en hoe dat wordt ingevuld.

9.1. Verwerkers

Van de genoemde privacyovereenkomsten is binnen de PU de verwerkersovereenkomst verreweg de meest voorkomende overeenkomst. De bekendheid binnen de PU om een verwerkersovereenkomst te moeten afsluiten is groot, maar toch gebeurt dit nog niet altijd, of in ieder geval niet op tijd, dat wil zeggen vóórdat de dienstverlening door de verwerker van start gaat. Eind 2022 waren 61 van de 68 noodzakelijke verwerkersovereenkomsten afgesloten. Het ontbreken van 7 verwerkersovereenkomsten is een zeer onwenselijke situatie en het verdient aanbeveling dat deze zo spoedig mogelijk alsnog worden opgesteld. 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 maken over het veilig verwerken van de persoonsgegevens is niet alleen een wettelijke verplichting, maar gelet op de genoemde risico's ook noodzakelijk vanuit het oogpunt van een zorgvuldige bedrijfsvoering.

Er is weliswaar bewustzijn over de verplichting om verwerkersovereenkomsten af te sluiten, maar een geborgd en gecontroleerd proces ontbreekt. De privacy officers kunnen ondersteunen bij het opstellen van deze overeenkomsten, maar de teamleiders zijn er verantwoordelijk voor dat de overeenkomst tijdig wordt afgesloten. Het team Inkoop wordt vaak genoemd als borging voor het afsluiten van verwerkersovereenkomsten, maar niet alle verwerkingen lopen via team Inkoop, en bovendien geeft dit team aan wel te wijzen op de verplichting van het afsluiten van een verwerkersovereenkomst, maar dat zij niet verantwoordelijk zijn voor de nakoming daarvan. Gelet op het genoemde belang verdient het aanbeveling om het tijdig afsluiten van een verwerkersovereenkomst procesmatig af te dwingen.

Voor een daadwerkelijke risicobeheersing is het niet alleen belangrijk *dat* verwerkersovereenkomsten worden opgesteld, maar ook dat hiervan *gebruik* wordt gemaakt. Het verdient daarom aanbeveling dat een bepaalde vorm van monitoring van de afspraken wordt georganiseerd, bij voorkeur als onderdeel van het bredere leveranciersmanagement. Deze monitoring kan uiteraard risicogebaseerd plaats vinden, en kan dus afhankelijk van de risico's variëren in periodiciteit (van continu tot eens in de zoveel jaar) en zwaarte (van een uitgebreide audit tot een eenvoudig e-mailtje of belletje met een aantal simpele vragen). In 2022 is door de privacy officers reeds een voorstel voor dergelijke risicogebaseerde monitoring gedaan, maar dit is blijven steken in een discussie over maatvoering en verantwoordelijkheid.

9.2. Samenwerkingsverbanden

In 2022 heeft het privacy team bijgedragen aan een project waarbij de belangrijkste risico's van bestaande samenwerkingsverbanden zijn geïnventariseerd en benodigde acties zijn bepaald om deze risico's te adresseren. Dit heeft als resultaat opgeleverd dat een beter inzicht bestaat in de aard en de omvang van de samenwerkingsverbanden, en dat in een aantal gevallen ook reeds nieuwe of aanvullende privacy bepalingen zijn opgenomen. Nog niet alle samenwerkingsverbanden zijn gecheckt op noodzakelijke acties, en het privacy team zal deze exercitie in 2023 verder afronden.

Uit het hierboven genoemde project blijkt dat in het verleden lang niet alle documentatie 'privacy-proof' is opgesteld, en dat herstelwerkzaamheden dus noodzakelijk (en in gang gezet) zijn. Om te voorkomen dat in de toekomst weer zo'n project nodig is, verdient het aanbeveling dat procesmatig wordt geborgd dat bij het aangaan van samenwerkingsverbanden vooraf wordt gecheckt of en zo ja welke privacy bepalingen moeten worden opgenomen.

10. Rechten van betrokkenen en klachtenprocedure

Volgens de AVG heeft een betrokkene het recht om een organisatie die zijn of haar persoonsgegevens verwerkt te vragen om deze persoonsgegevens in te zien, te verkrijgen, te rectificeren en/of te verwijderen. De provincie heeft – in tegenstelling tot bijvoorbeeld gemeenten – relatief weinig rechtstreeks contact met burgers. Hierdoor is het aantal inzageverzoeken de afgelopen jaren zeer laag geweest. In 2022 heeft de PU 1 verzoek ontvangen betreffende inzage in de persoonsgegevens. Dit verzoek is binnen de wettelijke termijn afgedaan.

Betrokkenen en andere belanghebbenden kunnen, als zij van mening zijn dat de verwerking van 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 deze klachten. In 2022 heeft de PU geen klachten als hiervoor bedoeld ontvangen.

BIJLAGE - CIP Self Assessment

Hieronder zijn de resultaten per onderdeel uitgewerkt, met een extra toelichting voor de 5 onderdelen die een score lager dan 3 hadden.

Score >= 3.0 is voldoende *Score tussen 2.0 en 2.9 is matig* *Score < 2.0 is onvoldoende*

Privacy Beleid: het beleidsdomein

B.01 Privacy Beleid geeft duidelijkheid en sturing (voldoende)
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 15-12-2022 : 3.2
Score 29-11-2021 : 3.5

B.02 Organieke inbedding (voldoende)
De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld.
Score 15-12-2022 : 3.3
Score 29-11-2021 : 3.7

B.03 Risicomanagement, Privacy by Design en de GEB (onvoldoende)
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 15-12-2022 : 1.0
Score 29-11-2021 : 1.1

Risicomanagement is een continu proces dat de (privacy)risico's signaleert, beoordeelt en risico's verkleint en bewaakt.

Onderbouwing/verklaring voor het nog niet behalen van volwassenheidsniveau 3:
- Vertraging in de aanpak voor risicomanagement voor Informatieveiligheid.
- DPIA's: Het initiatief om een DPIA uit te voeren ligt vooral nog bij IV&P. Het bewustzijn voor eigenaarschap van informatie en bijbehorende risico's is nog niet voldoende ingebed. De PU bevindt zich vooral nog in de fase waarin DPIA's voor de eerste keer worden uitgevoerd. De PU dient de stap te zetten naar een werkwijze waarbij DPIA's periodiek worden uitgevoerd/herijkt. Er is in de praktijk nog te weinig aandacht voor het concreet maken van maatregelen, het implementeren van deze maatregelen, en het beoordelen van de effecten van de geïmplementeerde maatregelen.
- Privacy by Design: De taken en verantwoordelijkheden voor Privacy by Design zijn nog onvoldoende uitgewerkt en belegd. Vanuit privacy is er beperkte en/of te late aansluiting op nieuwe ontwikkeling binnen de organisatie; nieuwe processen, programma's/projecten, aanschaf van applicaties/Cloud oplossingen en initiatieven op het gebied van data.

Privacy Uitvoering: het uitvoeringsdomein

U.01 Doelbinding gegevensverwerking (matig)
Doeleinden en rechtvaardigingsgronden van alle verzamelingen en verwerkingen van persoonsgegevens zijn tijdig, welbepaald en uitdrukkelijk omschreven.
Score 15-12-2022 : 2.4
Score 29-11-2021 : 2.4

Het vastleggen van het doel van de gegevensverwerkingen zorgt ervoor dat voor ieder persoonsgegeven de keuze om te verwerken weloverwogen en te rechtvaardigen wordt gemaakt. Het doel moet daarvoor welbepaald en uitdrukkelijk omschreven zijn vóórdat de verwerking begint en er moet getoetst worden of de verwerking van de gegevens noodzakelijk is voor het bereiken van het doel en er geen privacyvriendelijk(er) alternatief voorhanden is.

Input voor het bepalen van het doel zijn: het privacybeleid inclusief de geldende wet- en regelgeving, en overzicht op de verwerkingen, samen met de bijdrage vanuit gegevensmanagement. Het resultaat van de vastlegging vormt een belangrijk instrument voor de informatieverstrekking aan betrokkenen en de processen binnen het control domein.

Onderbouwing/verklaring voor het nog niet behalen van volwassenheidsniveau 3:

- Het doel is niet altijd bepaald en omschreven vóórdat de verwerking begint en dus wordt niet altijd vooraf bepaald of de verwerking gerechtvaardigd is.
- Er wordt niet altijd getoetst of de verwerking van de gegevens noodzakelijk is voor het bereiken van het doel en of het doel ook met minder persoonsgegevens kan worden bereikt, c.q. er een ander privacy-vriendelijk(er) alternatief voorhanden is.

U.02 Register van verwerkingsactiviteiten (voldoende)

Gegevens over de gegevensverwerkingen zijn 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 15-12-2022 : 3.5

Score 29-11-2021 : 3.5

U.03 Kwaliteitsmanagement (voldoende)

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 15-12-2022 : 3.1

Score 29-11-2021 : 2.6

U.04 Beveiligen van verwerking van persoonsgegevens (onvoldoende)

De organisatie treft technische en organisatorische maatregelen voor verwerking van persoonsgegevens op een passend beveiligingsniveau.

Score 15-12-2022 : 1.2

Score 29-11-2021 : 2.3

Informatiebeveiliging heeft tot doel om de dans op en de eventuele gevolgen van beveiligingsincidenten te beperken. De maatregelen bestaan uit organisatorische, technische en fysieke maatregelen die gebaseerd zijn op een (organisatieafhankelijke) risicoanalyse, wettelijke verplichtingen (waaronder de (U)AVG) en branche specifieke standaard voor informatiebeveiliging (de BIO). Informatiebeveiliging is een van de instrumenten voor privacybescherming. Daar waar maatregelen voor informatiebeveiliging en privacybescherming overeenkomsten vertonen, kunnen taken en verantwoordelijkheden worden gedeeld en kunnen taken gecombineerd worden uitgevoerd.

Onderbouwing/verklaring voor het nog niet behalen van volwassenheidsniveau 3:

- Er is een beveiligingsplan, maar dat is niet actueel, niet afgestemd op beveiligingsrisicobeoordelingen, en de verantwoordelijkheden voor het uitvoeren van het beveiligingsplan zijn onvoldoende ingebed binnen de organisatie, waardoor adequate implementatie achterblijft.
- De PU voldoet nog niet aan de BIO, en er is geen overzicht wie wat moet doen.

- De PU beschikt nog niet over een werkend informatiebeveiligingsmanagementsysteem (ISMS).
- Er is (nog) geen vastgestelde organisatie brede wijze voor beveiligingsrisicoanalyses. Er is een beoogde partij en methode geselecteerd. De methode (SRAM) hangt samen met de gekozen partijen (Strict). Deze werkwijze is nog niet formeel vastgesteld. Beveiligingsrisicoanalyses worden niet periodiek uitgevoerd, en zijn ook nog niet uitgevoerd voor alle verwerkingen met verhoogde risico's. Beveiligingsrisico's zijn niet altijd duidelijk toegewezen aan verantwoordelijken.

U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens (matig)
Bij elke verzameling van persoonsgegevens wordt tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar gesteld.
Score 15-12-2022 : 2.3
Score 29-11-2021 : 2.4

Het verstrekken van informatie dient ervoor transparant te zijn naar betrokkenen over het verzamelen en het verwerken, inclusief eventuele doorgifte, van de persoonsgegevens over betrokkene. Om dit te kunnen doen moet een actueel overzicht bekend en inzichtelijk gedocumenteerd zijn van waar, hoe en door wie de gegevens worden verwerkt.

Onderbouwing/verklaring voor het nog niet behalen van volwassenheidsniveau 3:
- Er is geen eenduidig vastgelegde en bewaakte wijze waarop wordt bepaald welke informatie de betrokkenen ontvangt bij de verzameling van persoonsgegevens. Veelal wordt per verwerking bepaald of informatie wordt verstrekt aan de betrokkene, welke informatie wordt verstrekt en op welke wijze de informatie wordt verstrekt.
- Vooraf wordt niet altijd bepaald of er een informatieplicht is aan betrokkenen.
- Eisen die aan de informatieverstrekking aan betrokkenen wordt gesteld, worden niet gecommuniceerd aan de organisatie. Deze informatie is niet beschikbaar op intranet.

U.06 Bewaren van persoonsgegevens (voldoende)
Door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.
Score 15-12-2022 : 3.4
Score 29-11-2021 : 2.7

U.07 Doorgifte persoonsgegevens (voldoende)
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 strikte criteria gehanteerd.
Score 15-12-2022 : 3.0
Score 29-11-2021 : 3.0

Privacy Control: het control- of beheerdomein

C.01 Intern toezicht (onvoldoende)
Door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.
Score 15-12-2022 : 1.3
Score 29-11-2021 : 1.4

Het toezicht binnen de eigen organisatie heeft tot doel vast te stellen of de gegevensverwerkingen rechtmatig zijn en of daarvoor de juiste maatregelen zijn getroffen, zodat voldaan wordt aan de eisen van de AVG, sectorspecifieke wetgeving en/of een (eventuele) Gedragscode.

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.

Onderbouwing/verklaring voor het nog niet behalen van volwassenheidsniveau 3:

- De PU is vooral nog bezig met opzetten/implementeren van beleid, kaders en richtlijnen voor privacy waardoor er nog weinig aandacht is geweest voor monitoren en houden van toezicht.
- Richtlijnen en werkwijze voor het houden van toezicht conform het *Three Lines of Defence* model zijn nog onvoldoende uitgewerkt. Het is onvoldoende duidelijk wat er gecontroleerd dient te worden, op welke wijze en aan wie gerapporteerd dient te worden.
- Rapportage/afleggen van verantwoording vanuit de uitvoering is nog niet ingericht.
- Binnen de PU is er (nog) onvoldoende sprake van een cultuur gericht op meten, evalueren en (continue) verbeteren.
- Binnen de reguliere managementprocessen (planning en control cyclus) is er onvoldoende aandacht en ruimte voor een onderwerp als (informatieveiligheid en) privacy.

C.02 Toegang tot gegevensbewerking voor betrokkenen (voldoende)

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 15-12-2022 : 3.3
Score 29-11-2021 : 3.5

C.03 Meldplicht Datalekken (voldoende)

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 15-12-2022 : 3.1
Score 29-11-2021 : 3.5