NEDERLANDS
REGISTER
GERECHTELIJK
DESKUNDIGEN

Jaarverslag Privacy compliancy

Functionaris voor Gegevensbescherming

2020-2021

Ella Schepel
Functionaris voor Gegevensbescherming NRGD

Inhoud

1 Inleiding 3

2 Belangrijkste aandachtsgebieden privacy-compliancy 5

3 Privacy administratie 6

3.1 Privacybeleid en Governance 6

3.3 DPIA's en (pre)DPIA-register 6

3.4 Datalekken 8

4 Transparantie: privacyverklaring 8

5 Privacy by design en Privacy by default 8

6 Betrokken partijen 8

6.1 Verwerkers(register) en verwerkersovereenkomsten 8

6.2 Rechten van betrokkenen 9

6.3 Informatiebeveiliging en AVG 9

6.4 Awareness, training en opleiding 9

7 Belangrijkste aandachtspunten en aanbevelingen 9

1 Inleiding

Voor het NRGD en het Privacy Office waren 2020 en 2021 in meer dan een opzicht bijzondere jaren. Zo bestaat het NRGD al weer tien jaar! Tijd om daar gezamenlijk, op gepaste wijze bij stil te staan was er nauwelijks. Door de coronacrisis werd thuiswerken en (meer) digitaal werken de norm. Goed om te zien dat medewerkers en organisatie in staat waren om deze stap te maken.

Samenwerken met en leren van andere organisaties speelt in het denken en doen van het NRGD een belangrijke rol, ook waar het gaat om privacy-compliancy. Zo wordt gebruik gemaakt van handreikingen vanuit bijvoorbeeld het ministerie van Justitie en Veiligheid (JenV), ook al staat het NRGD als ZBO op enige afstand. Verder wordt veel kennis uitgewisseld binnen Kleinlef: een samenwerkingsverband van een 40-tal kleinere overheidsorganisaties. De aldus verkregen basis wordt waar nodig aangevuld met of vervangen door NRGD-maatwerk. Ook voor het inzetten van tools e.d. wordt goed gekeken naar het omliggende veld. Het NRGD hanteert gebruik van 'proven technology' als uitgangspunt.

Onder de noemer Informatiehuishouding weten de privacy en security deskundigen binnen het NRGD elkaar te vinden. Dit bevordert snel kunnen schakelen. Zo zag het NRGD zich tijdens de coronacrisis genoodzaakt om in een kort tijdsbestek een keuze te maken voor een communicatie tool (WebEx), om de bedrijfsvoering op het gewenste niveau voort te kunnen zetten.

Als kleine uitvoeringsorganisatie is het NRGD het gewoon om te balanceren met schaarste, schaarste m.n. wat betreft mensen en middelen. Medewerkers vervullen vaak meerdere functies/rollen en het beschikbare aantal uren is vaker dan je zou willen geringer dan het aanbod van werk. Dat geldt bijvoorbeeld voor het Privacy Office. Het betekent dat het NRGD zorgvuldig moet (af)wegen waarop wordt ingezet. Een beeld dat overigens ook bij andere (grotere) organisaties wordt herkend.

KPI's

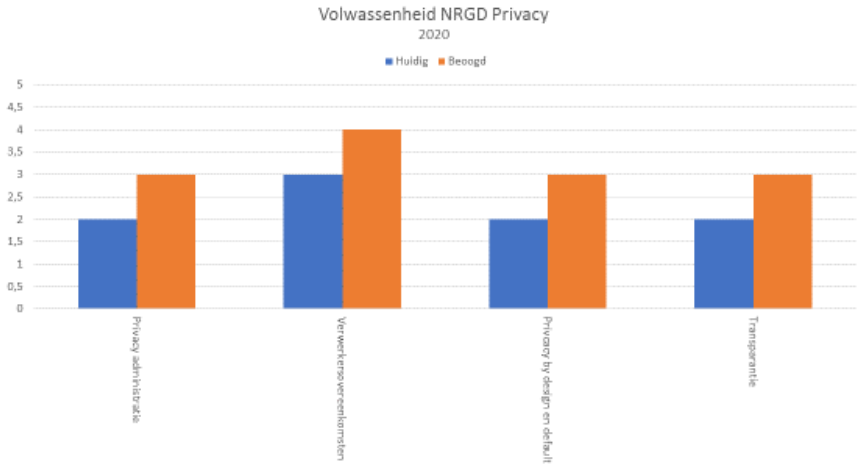
Wat betreft privacy-compliancy wordt binnen het ministerie van Justitie en Veiligheid gewerkt met zogenoemde KPI's. In 2020-2021 is hiermee geëxperimenteerd. De FG van het NRGD, tevens lid van de FG-pool KleinLef maakt deel uit van de schrijversgroep. Zoals uit onderstaande figuren valt af te leiden is in 2020 klein begonnen en is het aantal KPI's gaandeweg uitgebreid.

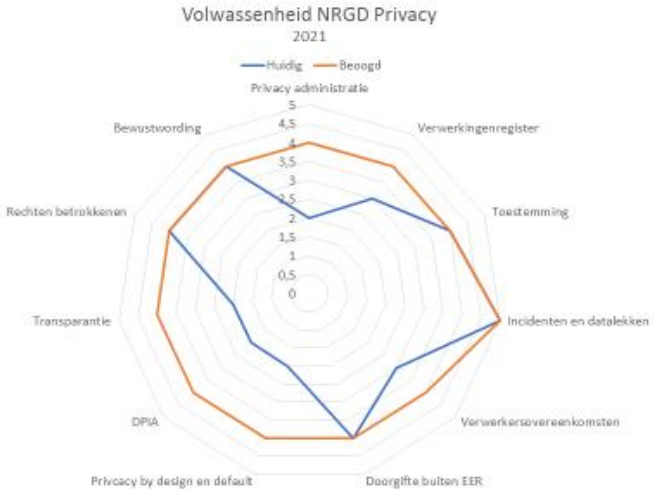
Met behulp van de KPI's maakt een organisatie zichtbaar waar zij zichzelf plot in de omgang met persoonsgegevens, of en zo ja welke groei is gepland en wat dat van de organisatie vraagt. De KPI's bieden inzicht in de wijze waarop vorm wordt gegeven aan de naleving van de privacy en maakt deze aantoonbaar. Deze sturingsinformatie biedt aanknopingspunten voor overleg, bijvoorbeeld tijdens het bureau-overleg of aan de bestuurstafel.

Er wordt gewerkt met vijf niveau's.[1] Voor de score van het huidige niveau van een KPI, wordt het niveau gekozen waarop de organisatie zich op het moment van invullen bevindt. Een hoger niveau wordt bereikt als *alle* elementen binnen een KPI zich op datzelfde hogere niveau bevinden. Binnen de overheid wordt niveau 3 gezien als het minimale volwassenheidsniveau voor privacy-compliancy. Belangrijker nog is dat het

[1] Privacymanagement KPI's JenV, versie november 2021.

NRGD vanuit de eigen missie en visie bepaalt wat het voor de organisatie passende volwassenheidsniveau is.





Het NRGD heeft de afgelopen twee jaar veel werk verzet wat betreft privacy-compliancy. In bovenstaand overzicht is dat niet altijd direct zichtbaar, vanwege het uitgangspunt dat een organisatie aan alle (onderliggende) elementen moet voldoen om een bepaald volwassenheidsniveau te scoren. Bij een aantal KPI's is het opvolgende niveau (3) al bijna bereikt. Zo wordt op korte termijn het beleidskader privacy (Privacy administratie) ter vaststelling aangeboden aan het College, waarna het binnen de organisatie verder kenbaar wordt gemaakt (KPI privacy administratie). In de ontwikkelfase van een verwerking is via de gecombineerde betrokkenheid van senior beleidsmedewerkers, CISO en PO structureel aandacht voor zorgvuldige omgang met persoonsgegevens en wordt de keuze voor privacyvriendelijke instellingen geborgd, aan vastlegging in werkprocessen en beleid wordt gewerkt (KPI Privacy by design en default). Bij ingebruikname van nieuwe tools en werkprocessen wordt standaard een DPIA uitgevoerd en risico's beoordeeld, de afronding en vastlegging behoeft aandacht (KPI DPIA).

Leeswijzer

Het jaarverslag beschrijft de belangrijkste aandachtsgebieden wat betreft privacy-

compliancy en de stand van zaken van andere AVG-verplichtingen. Afgerond wordt met de aandachtspunten en aanbevelingen.

2 Belangrijkste aandachtsgebieden privacy-compliancy

Informatiehuishouding

Informatiehuishouding ziet op vragen als hoe lang mag het NRGD welke data bewaren, welke data mag op welke manier worden gedeeld en hoe de kwaliteit van de ontvangen en bewaarde data wordt geborgd. Met het finaliseren van het Basisselectiedocument, de Selectielijst heeft het NRGD een belangrijke stap gezet in het op orde brengen van de informatiehuishouding. Wat betreft het delen van data heeft het NRGD tijdig de risico's van de op handen zijnde Wet open overheid zowel bedrijfsmatig als wat betreft bescherming van persoonsgegevens onderkend. De inzet is succesvol te noemen, zo worden op verzoek van het NRGD de persoon gerichte beoordelingsformulieren van individuele toetsingen uitgezonderd. Ook andere ontwikkelingen als archiefwetgeving en de geïntensiveerde aandacht voor de informatiehuishouding bij overheidsorganen als gevolg van de toeslagenaffaire laten zien dat het op orde hebben/ brengen van de informatiehuishouding noodzakelijk is.

Bewaartermijnen

Met het vorderen der jaren groeit het (digitale) geheugen van het NRGD en groeit het belang van het hebben van vastgestelde bewaartermijnen en ingerichte processen om tijdig te komen tot vernietiging van data. De afgelopen periode is een groot deel van de beschikbare capaciteit van de Privacy Officer gestoken in het finaliseren van het Basisselectiedocument, de Selectielijst. In 2021 zijn belangrijke slagen gemaakt in de uitvoering/ naleving. Het papierenarchief is opgeruimd, waar nodig zijn documenten gedigitaliseerd. Verder zijn er voorbereidingen getroffen voor jaarlijks opschonen van digitale documenten.

Uitbreiding werkterrein

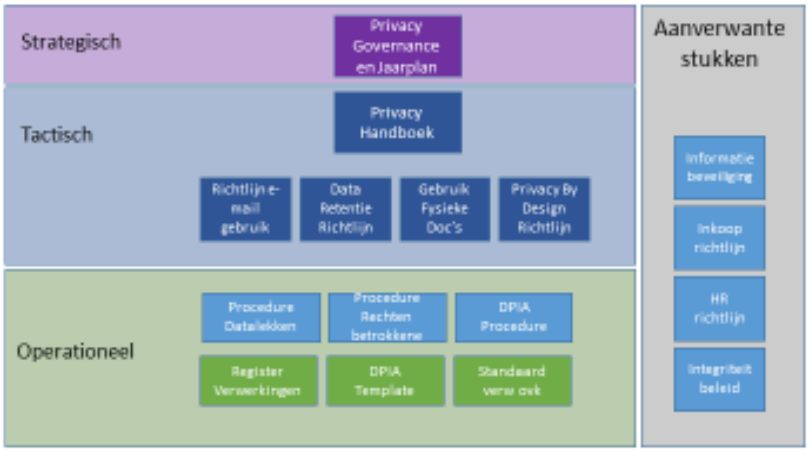
Langs meerdere wegen wordt gewerkt aan uitbreiding van het werkterrein van het NRGD naar het civiel- en bestuursrecht. In 2020 is het wettelijke traject hiervoor opgestart en er is een convenant gesloten met de NVMSR. Een deel van de hierbij betrokken data ziet op persoonsgegevens. Insteek is het Privacy Office (PO en FG) een vaste gesprekspartner te laten zijn bij, in ieder geval planvorming, informatievraagstukken en het aanknopen van nieuwe relaties/ samenwerkingsvormen. Zo kan toepassing van de privacybeginselen het best worden geborgd en krijgen privacy professionals ruimte om mee te denken in hoe data (wel) kan stromen.

Beheerprocessen

Onderhoud en beheer wordt vaak gezien als sluitstuk, niet zelden stopt een project of klus bij de oplevering. Onderhoud en beheer als onderdeel zien van een cyclische beweging, de zogenaamde plan-do-check-act cyclus helpt hierbij. Het op orde brengen èn houden van de (werk)processen vraagt om gezamenlijke inzet van organisatie en Privacy Office. Daarbij dient aandacht gegeven te worden aan een duidelijke afhechting en vastlegging van (werk)afspraken en adviezen.

3 Privacy administratie

3.1 Privacybeleid en Governance



Samenhang beleidsdocumenten

Het privacybeleid volgt op dit moment grotendeels het beleid van het ministerie, hierdoor beschikt het NRGD over een prima basis. Het afgelopen jaar is gewerkt aan een eigen beleidskader voor privacy, het stuk zal begin 2022 ter vaststelling worden aangeboden.

3.2 Verwerkingenregister

Het verwerkingenregister is een belangrijk fundament onder de privacy administratie, voor organisatie, FG èn AP. Het is de manier om aan te tonen dat je als organisatie grip hebt op privacy en de verwerking van persoonsgegevens: grondslag, doelbinding, dataminimalisatie etc. Bijna alles komt erin samen, of hangt ermee samen. Is bijvoorbeeld een (pre-)DPIA uitgevoerd of herijkt, dan vormt dat aanleiding om het verwerkingenregister te toetsen op juistheid en volledigheid. Dat geldt ook voor wijzigingen in werkprocessen op opstarten van nieuwe. Bij wijzigingen of aanvullingen in het register zal vervolgens ook de in- en/of externe privacyverklaring aangepast moeten worden.

Het NRGD heeft besloten om gebruik te maken van de EZK-tool. Een groot deel van de verwerkingen is hierin al opgenomen, de rest volgt het komend jaar.

Toestemming

Binnen het NRGD wordt alleen voor de toezending van de nieuwsbrief gebruik gemaakt van de grondslag toestemming.

3.3 DPIA's en (pre)DPIA-register

Om goed grip op privacy te krijgen moet privacy vanaf de start worden meegenomen, of het nu gaat om een nieuw project, wetgeving of een ICT-inkooptraject. Dat kan op verschillende manieren. Bijvoorbeeld door Privacy by design/default toe te passen, maar ook door voorafgaand aan iedere nieuwe verwerking van persoonsgegevens een risico-analyse uit te voeren, een zogenoemde pre-DPIA (Data Protection Impact Assessment). Volgt daaruit een waarschijnlijk hoog risico voor de rechten en vrijheden van betrokkenen, dan moet er een reguliere DPIA uitgevoerd worden. De (pre)DPIA wordt

aan de voorkant van een traject ingezet, afhankelijk van de ontwikkelingen binnen het traject kan tussentijdse bijstelling plaatsvinden. Zo heeft de organisatie (vroeg)tijdig eventuele risico's in beeld en kan (vroeg)tijdig mitigerende maatregelen meenemen/ implementeren. Ook het werken volgens de beginselen van Privacy by design komt hierdoor beter tot z'n recht. Een late uitvoering van de (pre)DPIA vergroot de kans op extra kosten en/of vertraging, omdat eerdere besluiten eventueel aangepast of teruggedraaid moeten worden.

Aanhaken van het Privacy Office vraagt blijvend aandacht. Een project dat er in positieve zin uitspringt is het Ad hoc project. Voor OurMeeting geldt dat de DPIA nog niet officieel is afgerond. De tool is in gebruik is genomen op basis van een, door de CISO opgestelde, concept DPIA met risicobeoordeling door de directeur van het Bureau NRGD. Om privacybescherming beter te borgen is ingezet op het vaststellen van het DPIA-proces.

Het uitvoeren van een DPIA kan bewerkelijk zijn. Op dit punt dan ook aandacht gevraagd voor de beperkte capaciteit bij het Privacy Office. Het kan nodig zijn dat de organisatie middelen ter beschikking moet stellen om een DPIA extern uit te laten voeren. Bij de opstelling van het jaarplan en de begroting kan hier rekening mee worden gehouden. De afgelopen jaren is een aantal keren van gebruik gemaakt van externen.

Verder is het afhechten, vastleggen van de DPIA en het aansluitend monitoren van risico's en maatregelen nog een aandachtspunt. Gekeken zou kunnen worden naar een risicoregister dat zowel door de CISO als door de Privacy Officer valt te gebruiken.

Videoconferentietool

Zoals gemeld moest als gevolg van de coronacrisis in korte tijd een besluit worden genomen over de inzet van een videoconferentietool. Vanuit het ministerie van Justitie en Veiligheid is WebEx als enige betrouwbare videoconferentietool voorgeschreven. SSC-ICT heeft conform dit standpunt WebEx als enige videoconferentietool uitgerold en ondersteund, andere tools worden niet toegelaten. Het NRGD is als uitvoeringsorganisatie onder het ministerie van JenV verplicht gebruik te maken van diens faciliteiten en infrastructuur en is alleen zo in staat de continuïteit van de bedrijfsvoering tijdens de corona-periode te garanderen.

Om zich een oordeel te kunnen vormen van mogelijke risico's bij gebruik van de tool en inzicht in de verwerking van persoonsgegevens van gebruikers en gasten binnen de tool heeft het NRGD het ministerie om een DPIA verzocht. Ondanks dat de tool al langere tijd binnen de rijksoverheid wordt gebruikt, is tot op heden geen (afgeronde) DPIA aangeleverd.

Het NRGD heeft, voor zover mogelijk, beleid opgesteld voor het gebruik van WebEx. Hoewel Webex door JenV en SSC-ICT als veilig wordt aangemerkt voor overleggen tot departementaal vertrouwelijk, heeft het NRGD niet alleen de door hen voorgestelde maatregelen en adviezen in acht genomen. Het NRGD heeft vanuit de eigen verantwoordelijkheid aanvullende maatregelen getroffen. Zoals het niet noemen van namen (spreken over aanvrager A), het bespreken van rapportages aan de hand van 'rapportage A', werd toegang tot digitale vergaderingen beperkt door alleen uitgenodigde personen toe te laten en met een wachtwoord te werken. Verder is er bij mondelinge en schriftelijke toetsingen een moderator aanwezig geweest om er zeker van te zijn dat onbevoegden geen toegang hadden tot de vergadering. Opslaan of opnemen van communicatie is geblokkeerd. De genomen maatregelen en afstemming zijn vastgelegd. Tussentijds overleg en evaluatiemomenten van het beleid zijn nog niet schriftelijk vastgelegd. Dit is een aandachtspunt voor de toekomst.

3.4 Datalekken

In de periode 2020 - 2021 zijn er geen datalekken gemeld. Wel kreeg het NRGD in die periode te maken met datalekken bij derden waarbij persoonsgegevens van medewerkers van het NRGD waren betrokken. Goed te merken dat de in- en externe contacten ook in deze gevallen snel zijn gelegd en de inzet erop is gericht om betrokkenen zo snel en zo goed mogelijk te informeren.

In 2021 is de vergadertool OurMeeting in gebruik genomen. Via deze tool heeft het NRGD meer grip op datastromen. Zo kan het delen van documenten met bijvoorbeeld leden van het College of toetsers, de duur van inzage en het al dan niet kunnen downloaden van documenten worden ingeregeld. De kans op datalekken is hierdoor sterk verkleind en de accountability toegenomen.

Het is aan te raden om in de bewustwordingssessies aandacht te besteden aan: wanneer spreek van je van een datalek en hoe te handelen. Het NRGD heeft het op zich genomen om eventuele datalekken van ingezette toetsers te melden. In intervisiebijeenkomsten met de toetsers wordt daarom de nodige aandacht besteed aan privacybescherming.

4 Transparantie: privacyverklaring

De privacyverklaring is een middel om aan betrokkenen te tonen hoe het NRGD met persoonsgegevens omgaat. Het NRGD heeft een externe privacyverklaring, gepubliceerd. Een interne privacyverklaring ontbreekt, daar staat tegenover dat het merendeel van de verwerkingen van interne betrokkenen via P-direkt loopt. De Privacy Board van JenV heeft onderzoek gedaan naar privacyverklaringen, een van de aandachtspunten daaruit is het aanbrengen van meer gelaagdheid in de privacyverklaring.

Ook is onderhoud en (versie)beheer hier een aandachtspunt. Dat er proceseigenaren zijn vastgesteld van de interne en externe privacyverklaring zal hierbij zeker helpen.

5 Privacy by design en Privacy by default

Privacy by design betekent dat privacy vanaf het begin meegenomen wordt, en dat kan zowel organisatorisch als technisch worden opgevat. Dit aandachtspunt betreft vooral de organisatorische aspecten van privacy by design. Privacybescherming vraagt blijvende aandacht in (besluitvormings)processen. Het is belangrijk dat het Privacy Office vroegtijdig bij pilots, wijzigingen en projecten wordt betrokken. Zie ook eerdere opmerkingen bij het onderdeel DPIA.

6 Betrokken partijen

6.1 Verwerkers(register) en verwerkersovereenkomsten

Het NRGD maakt gebruik van een standaardmodel voor verwerkersovereenkomsten. Het NRGD heeft de onderlinge verhoudingen: verwerkersverantwoordelijke/ verwerker uitgezocht in het kader van AVG onderzoek toetsers. Er is een actueel overzicht van verwerkers.

De situatie rond de Brexit is door het Privacy Office nauw gemonitord. In juni 2021 heeft de Europese Commissie (EC) een tweetal adequaatheidsbesluiten genomen. Daarmee oordeelt de EC dat het niveau van bescherming van persoonsgegevens in het Verenigd Koninkrijk gelijkwaardig is aan dat in de Europese Unie. Het NRGD hoeft daardoor geen aanvullende maatregelen te treffen.

6.2 Rechten van betrokkenen

Het NRGD heeft in 2021 voor het eerst een verzoek tot inzage ontvangen. Het verzoek is tijdig afgehandeld.

Het is aan te raden om in de bewustwordingssessies aandacht te besteden aan de rechten van betrokkenen, en hoe je een AVG-verzoek herkent en behandelt.

6.3 Informatiebeveiliging en AVG

Het NRGD is verantwoordelijk voor het nemen van passende technische en organisatorische maatregelen om te kunnen waarborgen en aan te tonen dat de verwerkingen van persoonsgegevens in overeenstemming zijn met de AVG. Steeds verdergaande digitalisering maakt dat op dit punt van de overheid veel wordt verwacht.

Het NRGD voldoet aan de Baseline Informatiebeveiliging Overheid (BIO), heeft autorisaties vastgesteld en heeft een cookieverklaring gepubliceerd. Verder maakt het NRGD gebruik van de door de rijksoverheid opgestelde Gedragsregeling voor de digitale werkomgeving en van het door JenV opgestelde Afwegingskader Cloud JenV. Het NRGD is voornemens om op termijn eigen beleid voor de Cloud te ontwikkelen. Dat geldt ook voor het informatiebeveiligingsbeleid en een risico-register. Dit is voor een belangrijk deel het gevolg van de beperkt beschikbare capaciteit bij het Security Office.

6.4 Awareness, training en opleiding

Bewustzijn op het gebied van privacy en security vraagt om voortdurende aandacht en zorg. Het is belangrijk dat door leidinggevenden het belang ervan wordt gezien en vooral wordt uitgedragen en benadrukt.

Het ministerie is in 2020 gestart met het programma Weerbaar JenV, zo wordt het mogelijk om aan te tonen dat medewerkers daadwerkelijk worden getraind. Het NRGD heeft besloten hierop aan te sluiten. Het afgelopen jaar hebben medewerkers de AVG-cursus Brons gehaald. Controle op naleving ligt bij de directeur. De Privacy Officer en de CISO bevragen periodiek ‘medewerkers’ niet in loondienst op hun activiteiten om kennis van privacybescherming actueel te houden.

Onder het motto ‘never waste a good crisis’ vormen in de media uitgemeten beveiligingsincidenten en datalekken aanknopingspunten voor (korte) awareness sessies via mail en/of tijdens (bureau) overleggen.

Via het samenwerkingsverband KleinLef nemen medewerkers van het NRGD deel aan de AVG-werkgroep en de CIO/CISO-werkgroep. Het NRGD maakt gebruik van een FG uit de pool van KleinLef. De groepen delen in toenemende mate kennis en informatie met elkaar. Voor kleinere organisaties als het NRGD zijn dergelijke vormen van samenwerking onontbeerlijk. Ook hier doet de beschikbare capaciteit zich gelden.

7 Belangrijkste aandachtspunten en aanbevelingen

Onderstaand de belangrijkste aandachtspunten en aanbevelingen op een rij.

- *Privacy en security*
  Privacy en security hangen nauw met elkaar samen. Zet in op (verdergaande) integratie zowel beleidsmatig als in de uitvoering, maak zoveel mogelijk efficiënt gebruik van gezamenlijke instrumenten. Bevorder efficiënte samenwerking.
- *Facilitering*
  Houd bij opstellen van het jaarplan (incl. begroting) van het NRGD rekening met impact op capaciteit en middelen voor de informatiehuishouding (privacy en security).

- *Informatiehuishouding*
  Er is een goede start gemaakt met het implementeren en handhaven van de Selectielijst. Belangrijk dat dit wordt voorgezet.
- *Beheerprocessen en accountability*
  Door organisatie en Privacy Office dient blijvend gewerkt te worden aan het verder op orde brengen van de (werk)processen en het consequent toepassen ervan. Hecht processen af, leg e.e.a. goed vast en zorg voor 'onderhoud en beheer'. Dit geldt bijvoorbeeld voor de DPIA's en het monitoren van de daaruit voortvloeiende risico's en maatregelen.
- *Gesprekspartner/ adviseur*
  Het afgelopen jaar is er een nieuwe Privacy Officer gestart. Goed moment om de onderlinge afspraken en overlegmomenten met directeur, FG, CISO en Privacy Officer te actualiseren. Betrek hier ook de geplande bureau-activiteiten voor het komend jaar bij.
- *Volwassenheidsniveau*
  Stel periodiek in samenspraak met het Privacy Office de geambieerde volwassenheidsniveaus vast. Maak 'SMART'-afspraken[2] over hoe dit te bereiken dan wel te behouden.

Conclusie

Uitdagingen zullen er altijd zijn. Met blijvende aandacht voor een goede balans, kan het NRGD binnen afzienbare tijd doorgroeien naar bij de organisatie passende volwassenheidsniveaus.

Ella Schepel
Functionaris voor Gegevensbescherming NRGD

[2] SMART : specifiek, meetbaar, acceptabel, realistisch en tijdgebonden.