Berenschot

RAPPORT

Inrichting rijksbrede privacy governance

68108 – openbaar – 18 oktober 2022

RAPPORT

Inrichting rijksbrede privacy governance

68108 – openbaar – 18 oktober 2022

Inhoudsopgave

Managementsamenvatting

Privacy en gegevensbescherming zijn de afgelopen jaren steeds belangrijkere thema's geworden binnen de (rijks)overheid en er bestaat een groeiende behoefte om privacy governance binnen de rijksoverheid eenduidiger in te richten, onder meer naar aanleiding van het ADR-rapport. Op verzoek van het CIO-office Rijk heeft Berenschot een onderzoek uitgevoerd naar de verschillende mogelijkheden om privacy governance beter in te richten. Op basis van een quickscan (bestaande uit interviews en desk study) heeft Berenschot verschillende scenario's voor de inrichting van een privacy governance uitgewerkt. Hieruit is één voorkeursscenario benoemd.

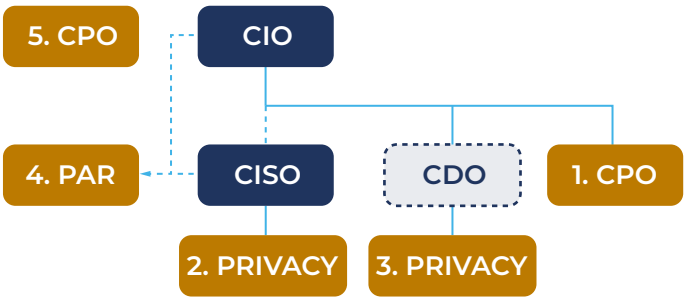
Tijdens de quickscan hebben we onderzocht welke behoeften er bestaan vanuit de bestuurlijke en politieke top, welke tekortkomingen en adviezen zijn gedeeld in eerdere rapporten en documenten, en hoe men vanuit de privacyfuncties binnen de verschillende ministeries (en rijksbreed) zelf kijkt naar de wijze waarop een (rijksbrede) inrichting vormgegeven is en in de toekomst vormgegeven kan worden. Uit de rapporten die we in het kader van ons onderzoek hebben gelezen, is meermaals het belang benoemd om privacy governance rijksbreed beter in te richten. Hierdoor kan een rijksbreed risicobeeld gevormd worden, kunnen kaders worden gesteld waarin kwaliteitseisen en standaarden zijn opgenomen, en kunnen parameters worden gedefinieerd die de rijksoverheid inzicht bieden in de rijksbrede borging van privacy van burgers (en ambtenaren). Het inrichten van deze privacy governance binnen het huidige CIO-stelsel lijkt daarbij een logische stap. We zien namelijk zowel in de toelichting van het CIO-besluit als in de I-strategie meerdere keren genoemd staan dat dit onderdeel is van het CIO-stelsel en de CIO(-Rijk)-functie. We constateren echter dat dit in het huidige besluit niet is vertaald in concrete taken, verantwoordelijkheden en bevoegdheden. In de departementale inrichting zien we een versnippering. Een belangrijk deel van de privacyfunctionarissen is gepositioneerd binnen het CIO-office, maar een deel van hen is ook geplaatst binnen andere afdelingen, zoals bijvoorbeeld bedrijfsvoering.

Uit gesprekken met de verschillende privacyfunctionarissen binnen de departementen blijkt dat ook zij meerwaarde zien in het versterken van rijksbrede samenwerking op bepaalde onderwerpen. Tegelijkertijd zijn er bij hen zorgen dat een rijksbrede inrichting leidt tot verminderde autonomie en onvoldoende aandacht voor uitdagingen en vraagstukken die specifiek voor hen gelden. Voldoende invloed en mandaat voor privacyfunctionarissen uit de ministeries is voor hen dan ook belangrijk.

Deze input heeft ertoe geleid dat we negen uitgangspunten hebben gedefinieerd waarin we belangrijke wensen en randvoorwaarden voor een rijksbrede privacy governance hebben vastgelegd. In deze uitgangspunten hebben we aspecten terug laten komen die voortbouwen op bestaande modellen en eisen rondom sturing, uitvoerbaarheid en draagvlak.

- Zet privacy hoger op de agenda.
- Bouw voort op bestaande rijksbrede structuren.
- Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties.
- Werk volgens het 3-LoD model en richt je daarbij op het inrichten van de tweede lijn.
- Voorkom dat het inrichten van een rijksbrede tweede lijn leidt tot het buitenspel zetten van de FG's.
- Zorg voor voldoende 'checks and balances'.
- Sluit aan bij functies die momenteel al door de meeste departementen worden ingericht, zoals de CPO.
- Zorg voor voldoende mandaat vanuit de departementen.
- Zorg voor een integrale aanpak.

Naast deze uitgangspunten, hebben we ook een profielschets gemaakt van de taken, verantwoordelijkheden en bevoegdheden die bij een tweedelijnsprivacyfunctionaris passen. Hierbij hebben we onder meer gekeken naar beleidstukken die we hebben ontvangen van verschillende departementen en de wijze waarop dit reeds is ingeregeld voor informatiebeveiliging.



Op basis van onze bevindingen hebben we vervolgens vijf scenario's uitgewerkt die we alle afzonderlijk hebben getoetst aan de eerder gedefinieerde uitgangspunten. De uitkomsten van deze toets hebben geleid tot een voorkeur voor scenario 1. In dit scenario wordt binnen het huidige CIO-stelsel een nieuwe functie toegevoegd van chief privacy officer (CPO). De inrichting van deze functie wordt naar analogie van het CISO-stelsel vormgegeven binnen het CIO-besluit. We denken dat dit scenario het beste tegemoetkomt aan de politieke en maatschappelijke wens om privacy hoger op de agenda te plaatsen, zorgt voor een meer integrale aanpak binnen de rijksoverheid en het beste aansluit bij de visie en inrichting van privacy governance binnen de ministeries. De aan te wijzen CPO zal in de uitvoering van zijn rol nauw samenwerken met andere functies binnen het CIO-office, zoals de CISO en de CDO. In de praktijk kunnen na te streven belangen en prioriteiten van deze functionarissen uiteenlopen of met elkaar conflicteren. Op zulke momenten is het van belang dat discussie en besluitvorming op het juiste niveau plaatsvindt. Naar onze mening dient de CIO in die gevallen een zorgvuldige belangenafweging te maken tussen de verschillende visies van CISO, CDO en CPO. In het kader van 'checks and balances' adviseren we om voor de CPO een escalatiemiddel in te regelen, vergelijkbaar met de CISO. Dit middel moet worden gezien als een uiterst middel.

Berenschot is gevraagd om tijdens het onderzoek ook specifiek te onderzoeken of een rijksbrede privacy governance vormgegeven zou kunnen worden binnen het op te richten CDO-stelsel. Op basis van ons onderzoek zien we hiervoor onvoldoende aanknopingspunten. Het belangrijkste argument hiervoor is dat de CDO-rol momenteel nog onvoldoende concreet is uitgewerkt en we daardoor dus niet kunnen beoordelen hoe de CDO zich verhoudt tot andere functionarissen binnen het CIO-stelsel. Bovendien bleek uit de interviews ook weinig draagvlak voor het integreren van privacy binnen een CDO-stelsel. Dit beperkte draagvlak bleek zowel uit de hoek van CDO's als vanuit de privacyfunctionarissen.

Tot slot hebben we enkele aanbevelingen geformuleerd die we adviseren bij de uitwerking van een rijksbrede privacy governance conform scenario 1 binnen het CIO-stelsel.

1. Richt het CPO-stelsel stapsgewijs in. Zorg er als eerste voor dat er binnen ieder ministerie een CPO aangesteld wordt en stem op hoofdlijnen een profiel af waarin de taken, de verantwoordelijkheden en de bevoegdheden worden vastgelegd. Pas vervolgens het CIO-besluit aan en richt een CPO-stelsel naar analogie van het CISO-stelsel in.
2. Waarborg de sterke positie van de FG in het nieuw op te richten stelsel. Voorkom dat rijksbrede kaders, standaarden en kwaliteitseisen ertoe leiden dat FG's buitenspel worden gezet. Betrek hen actief bij het vormgeven hiervan. Hiermee versterk je het draagvlak onder FG's.
3. Evalueer periodiek de wijze waarop de CPO en de CDO zich tot elkaar verhouden. We zien in de praktijk dat de invulling van de rol van CDO en CPO op veel vlakken potentieel overlappen. Zeker op het gebied van privacy-by-design, dataminimalisatie en andere concepten vullen de rollen elkaar mogelijk veel aan. Wanneer voor beide rollen een sterk fundament is gecreëerd, zou men er in de toekomst mogelijk voor kunnen kiezen om de rollen (deels) te integreren.
4. Houd bij het inrichten van een rijksbrede privacy governance voldoende rekening met de diversiteit van de ministeries en uitvoeringsorganisaties. Zorg ervoor dat een CPO-stelsel voldoende ruimte geeft om invulling te geven aan de wijze waarop zij een CPO-functie inrichten.
5. Tijdens verschillende interviews kwam naar voren dat een gebrek aan kennis en capaciteit een belangrijke drempel vormt bij het kwalitatief inrichten van een privacystelsel. We adviseren om gelijktijdig met het inrichten van privacy governance in te zetten op versterking van de kennis en capaciteit op het gebied van privacy rijksbreed, bijvoorbeeld door het inrichten van een flexibele schil of thematische werkgroepen.

HOOFDSTUK 1

Inleiding

De aandacht voor privacy is de afgelopen jaren flink toegenomen. Niet alleen door de komst van de Algemene verordening gegevens-bescherming (AVG), maar ook doordat het onderwerp steeds meer maatschappelijke en politieke aandacht krijgt. Dit maakt dat er behoefte is om richting te geven aan de governance op privacy binnen de (rijks)overheid. In dit hoofdstuk worden de aanleiding, vraagstelling en werkwijze van het onderzoek naar de rijksbrede governance op privacy beschreven.

De afgelopen jaren zijn we ons steeds meer bewust van de potentiële risico's die voortkomen uit onvoldoende bescherming van persoonsgegevens. In de afgelopen jaren hebben zich situaties voorgedaan waarin de bescherming van persoonsgegevens door de (rijks)overheid onvoldoende is gebleken of de gegevens van burgers op onrechtmatige wijze werden verwerkt. De toeslagenaffaire, inclusief de voortdurende nasleep daarvan, laat zien hoe complex problemen kunnen worden en wat voor enorme impact deze problemen kunnen hebben.

Bijvoorbeeld: Een groep gedupeerden van de toeslagenaffaire heeft aangegeven naar de rechter te stappen om een nieuw BSN-nummer aan te vragen. Als gevolg van de toeslagenaffaire zijn in een groot aantal systemen van (overheids)organisaties gedupeerden onterecht gemarkeerd als fraudeur. Omdat de overheid niet in staat lijkt te zijn om deze onterechte markeringen weg te halen, hebben gedupeerden een nieuw BSN verzocht.

Bron: *NOS - Gedupeerden toeslagenaffaire willen nieuw Burgerservicenummer (22 januari 2021)*

Ook wijzigingen in wet- en regelgeving hebben ervoor gezorgd dat het voldoen aan alle wettelijke normen steeds lastiger is geworden. Naast de reeds bestaande uitdagingen voor publieke organisaties om te voldoen aan de (abstracte en open) normen, zoals opgenomen in de AVG en UAVG, zien we tegelijkertijd steeds meer nieuwe wet- en regelgeving verschijnen, waarin specifieke eisen worden gesteld rondom de informatievoorziening binnen de rijksoverheid. Steeds vaker zien we dat overheden gegevens met elkaar uitwisselen, zodat zij beter in staat zijn om publieke waarde te creëren door de burger en de maatschappij van dienst te zijn. Hierdoor veranderen ook continu de risico's rondom het waarborgen van de privacy van burgers en zullen uitdagingen in de toekomst waarschijnlijk steeds vaker interdepartementaal van aard zijn.

Uiteraard ziet men deze veranderingen in het landschap ook binnen de (rijks)overheid. Vanuit de regering is een duidelijke tendens richting meer centrale coördinatie; dit zowel om een meer daadkrachtige overheid te stimuleren, alsook om een meer uniforme werkwijze voor de burger te bewerkstelligen. Zo heeft men met de benoeming van een staatssecretaris voor Digitale Zaken al een duidelijk signaal afgegeven dat de digitalisering binnen de rijksoverheid (deels) vanuit een centraal punt gecoördineerd moet worden. Onderwerpen als digitale weerbaarheid en privacy krijgen een steeds prominentere rol in de I-strategie. En in de hoofdlijnenbrief beleid voor digitalisering[1] van de staatssecretaris staat tevens benoemd dat naleving van de AVG een belangrijk onderwerp is.

Ook de roep van de politiek op dit gebied versterkt, bijvoorbeeld met de Motie Verhoeven waarin werd opgeroepen om chief privacy officers op hoog niveau aan te stellen bij uitvoeringsorganisaties naar aanleiding van de constatering dat de overheid structureel tekortschiet bij de bescherming van persoonsgegevens.

Toch zien we in de praktijk dat de bescherming van persoonsgegevens vrijwel volledig decentraal wordt aangevlogen. Met het CIO-besluit uit 2021 heeft men belangrijke stappen gezet rondom het versterken van de samenwerking tussen CIO's rijksbreed en het digitaliseren van de informatievoorziening, inclusief het waarborgen van de veiligheid daarvan door de CISO's. Die gelijke trend zien we niet binnen de privacy governance. Op het gebied van privacy bestaat onvoldoende mandaat om rijksbreed kaders te stellen die erop gericht zijn een interdepartementaal risicobeeld te vormen en deze risico's vervolgens te mitigeren.

Momenteel is een rijksbrede aanpak rondom privacy beperkt tot advisering bij vraagstukken over de rijksbrede bedrijfsvoering. Hiervoor heeft het ministerie van BZK in 2017 de functie van privacy adviseur Rijk (PAR) aangewezen. De PAR adviseert de Interdepartementale Commissie Bedrijfsvoering Rijksdienst (ICBR) en de Groepsondernemingsraad Rijk (GOR) bij interdepartementale bedrijfsvoeringsvraagstukken over aspecten rondom de bescherming van persoonsgegevens. Sinds 2021 is hier ook het opstellen van rijksbrede kaders, zoals bijvoorbeeld het Model DPIA Rijksdienst, bijgekomen. Verder vervult de PAR ook de rol als voorzitter van het informele interdepartementale privacyoverleg, waarbij de PAR vanuit een faciliterende en verbindende rol adviseert over rijksbrede privacyvraagstukken.

1 https://open.overheid.nl/repository/ronl-bbc2eeff7c47541f993ebd2f9b-61508f07750dd1/1/pdf/kamerbrief-hoofdlijnen-beleid-voor-digitalisering.pdf

In een extern evaluatieonderzoek uit 2020 heeft men onderzocht of de functie van de PAR meerwaarde biedt. In de conclusies van dit onderzoek werd dit bevestigd en werd bovendien aanbevolen dat de rol van de PAR in de toekomst verder versterkt zou mogen worden. Bijvoorbeeld door specifieke eisen te stellen aan de omgang met adviezen van de PAR, de PAR meer kaderstellende en coördinerende bevoegdheden toe te kennen en het verder stimuleren van de interdepartementale samenwerking.

Voorbeeld: Een goed voorbeeld van een 'best practice', (mede) geschreven door de PAR, is de ontwikkeling van het Model DPIA Rijksdienst. Dit model wordt breed binnen de rijksoverheid gebruikt en bevat een heldere uiteenzetting van de begrippen, beginselen en vragen die worden gesteld in het kader van de uitvoeriwng van een DPIA. Het Rijksmodel DPIA zorgt hiermee voor sterke kwaliteitswaarborgen en een integrale aanpak richting het identificeren van dreigingen en risico's, het betrekken van de juiste expertise en het waarborgen dat er voldoende effectieve maatregelen genomen worden.

Bron: *kcbr.nl - Model DPIA Rijksdienst (versie 2.0)*

Tot slot is men vanuit het CIO Rijk bezig met een verkenning naar het uitbreiden van het huidige CIO-stelsel met een rol van chief data officer (CDO). Hiermee wordt invulling gegeven aan de plannen zoals beschreven in de I-strategie. Hoewel de taken en verantwoordelijkheden van de CDO nog niet zijn vastgesteld, zal de CDO een sterke rol gaan vervullen rondom het op orde brengen van de informatiehuishouding binnen de rijksoverheid. Hij zal zich daarbij focussen op verdere ontwikkeling van datagedreven werken en daarmee bijdragen aan een verdere toename van de creatie van publieke waarde.

1.1 Vraagstelling

Nu het CIO-stelsel verder wordt uitgebreid met een CDO-stelsel, dient men opnieuw vast te stellen hoe de verschillende functies (en stelsels) binnen het CIO-stelsel zich tot elkaar verhouden. Onderwerpen als informatiemanagement, informatiebeveiliging, privacy en datamanagement zijn zeer nauw met elkaar verbonden en overlappen elkaar op diverse onderdelen. Door het toevoegen van een nieuwe functie binnen dit stelsel is het dan ook logisch dat men opnieuw moet bekijken hoe verschillende functionarissen zich tot elkaar verhouden. Dit vraagstuk speelt op zowel het overkoepelende rijksbrede niveau, als op het departementale niveau.

Daarbovenop wordt bekeken op welke wijze de rijksbrede (tweedelijns) privacy governance verder geformaliseerd en uitgebreid kan worden. Mede ingegeven door het onderzoek van de Auditdienst Rijk waarin wordt geconcludeerd dat de governance op het gebied van privacy versterkt moet worden binnen de rijksoverheid.

Voor het rijksbrede deel is hierbij een rol weggelegd voor de PAR die ook nu al een adviserende rol vervult bij inter-departementale bedrijfsvoeringsvraagstukken. Wanneer de privacy governance ingebed wordt in het CIO-stelsel, zal ook de PAR-functie hierbinnen een rol moeten krijgen. De PAR is formeel geen onderdeel van het CIO-stelsel, maar werkt hier in de praktijk nauw mee samen. Ook zijn de PAR's functioneel geplaatst in het IB&P-team. En deze inrichting is ook bij, in elk geval een aantal, departementen terug te vinden. Het hoofd IB&P binnen CIO-Rijk heeft tevens de rol van CISO Rijk.

Het voorgaande heeft ertoe geleid dat het ministerie van BZK advies heeft gevraagd over *de wijze waarop een privacy governance binnen de rijksoverheid het beste ingericht kan worden*. Hierbij is expliciet de vraag gesteld om in het onderzoek alternatieven voor de inbedding van privacy governance binnen het CIO-stelsel uit te werken. Bijvoorbeeld als apart onderdeel binnen het CIO-stelsel of als onderdeel van het (toekomstige) CDO-stelsel. Ten slotte is gevraagd om vanuit de geformuleerde alternatieven tot een onderbouwde voorkeursoplossing te komen. Het beantwoorden van deze vragen moet leiden tot een (gedragen) verdere professionalisering van de rijksbrede governance op het gebied van dit onderwerp.

1.2 Werkwijze

We hebben het onderzoek uitgevoerd in drie verschillende fasen:

1. **Quickscan huidige privacy governance.** We zijn gestart met het in kaart brengen van de huidige privacy governance binnen de diverse departementen en rijksbreed. Vanuit de departementen hebben we hiervoor met diverse stakeholders gesproken, waaronder (chief) privacy officers, FG's en CDO's. Daarnaast hebben we met verschillende rijksbrede functionarissen gesproken, onder meer vanuit het CIO-office en de PAR. Het doel van deze quickscan was enerzijds gericht op het inzichtelijk maken hoe de verschillende departementen de privacy governance hebben vormgegeven en welke voor- en nadelen zij zien in het intensiveren van de rijksbrede samenwerking in de toekomst. De volledige lijst van personen die we hebben gesproken, treft u in onze verantwoording.
2. **Inventariseren en beschrijven alternatieven.** De resultaten van de quickscan hebben we vervolgens gebruikt om een aantal uitgangspunten te definiëren die van belang zijn bij de inrichting van een rijksbrede privacy governance. Vervolgens hebben we vijf verschillende scenario's uitgewerkt die we ieder hebben getoetst aan een toetsingskader met de gedefinieerde uitgangspunten.
3. **Bepalen voorkeursoplossing.** In fase 3 hebben we conclusies en aanbevelingen gevormd, inclusief toelichting op welk scenario wij het meest geschikt achten. In dit rapport lichten we onze beweegredenen voor deze keuze expliciet toe. We ronden het onderzoek ten slotte af met een aantal aanbevelingen, zoals een stappenplan op hoofdlijnen en bepaalde aspecten waarvan we het van belang vinden om rekening mee te houden bij de verdere uitwerking van de rijksbrede privacy governance.

1.3 Leeswijzer

In hoofdstuk 2 bespreken we de kaders en het speelveld rondom de privacy governance. De uitkomsten van de quickscan zijn te vinden in hoofdstuk 3, de verschillende alternatieven in hoofdstuk 4 en de door ons geadviseerde oplossing met aanbevelingen in hoofdstuk 5. In de verantwoording (hoofdstuk 6) is een uitgebreidere beschrijving te vinden van de aanpak.

HOOFDSTUK 2

Context

Om een passend advies te geven over de wijze waarop de governance op privacy binnen de rijksoverheid ingericht zou moeten worden, is het noodzakelijk om het speelveld waarbinnen geopereerd wordt goed te begrijpen. In dit hoofdstuk beschrijven we kort de belangrijkste kaders waarbinnen ons advies plaatsvindt. Daar waar deze kaders leiden tot een uitgangspunt voor de nadere analyse en conclusies en aanbevelingen, benoemen we dit expliciet. We hebben in het kader van dit onderzoek de wettelijke kaders van AVG en UAVG niet opgenomen in de context. Dit onderzoek richt zich primair op de interne verantwoordelijkheid en niet zozeer op de wettelijke verantwoordelijkheid die organisaties hebben.

2.1 Besluit CIO-stelsel Rijksdienst

Het Besluit CIO-stelsel Rijksdienst 2021[2] beschrijft de organisatie-inrichting van het CIO-stelsel binnen de gehele rijksdienst. Het is het resultaat van een reeks stappen richting een grotere volwassenheid van digitalisering binnen de rijksoverheid. Dit is gestart in 2008 met het instellen van een CIO per departement, mede om grote ICT-projecten beter beheersbaar te maken. Uit het rapport van de Commissie Elias in 2014 bleek dit niet voldoende te zijn; de Commissie Elias concludeerde dat besluitvorming en verantwoordelijkheden op het gebied van ICT niet goed georganiseerd waren en dat er onvoldoende doorzettingsmacht was, mede vanwege het feit dat de rijks-CIO niet meer bevoegdheden had dan de departementale CIO's

In 2019[3] bleek het, in het licht van digitale ontwikkelingen, nodig om de sturing op alle aspecten van IV te versterken. Dit was onder meer op basis van een ABPTopconsult-rapport[4], dat concludeerde dat de groei rondom IV te ongecontroleerd was. Het advies was om de IV-functie op departementaal niveau te versterken, maar ook rijksbreed het nodige in te richten. Dit was de aanzet voor het CIO-besluit dat in 2020[5] is vastgesteld door de ministerraad. Hier staat tevens het CISO-stelsel in beschreven vanwege de toegenomen digitale dreigingen en de noodzaak om ook hier een stevige besturing op in te richten. Uit de nulmeting besluit CIO-stelsel[6] van mei 2021 bleek dat alle departementen bezig zijn met de implementatie van het besluit, maar dat er nog wel uitdagingen lagen in de implementatie van de benodigde veranderingen.

Het Besluit CIO-stelsel Rijksdienst 2021 beschrijft de taken en bevoegdheden van de CIO en CISO, op zowel departementaal als rijksbreed niveau. Het doel van het besluit is om de digitale transformatie te versterken en de CIO neer te zetten als digitaal leider binnen een departement. Op deze manier kunnen nieuwe ontwikkelingen naar een hoger niveau gebracht worden.

Een ander doel is het versterken van de samenwerking tussen de departementen. Dit vergroot de wendbaarheid om in te spelen op nieuwe ontwikkelen en te reageren op digitale dreigingen. Doordat alle CIO's en CISO's een vergelijkbaar takenpakket en bevoegdheden kregen, zou het samenwerken makkelijker moeten gaan en is er meer ruimte om van elkaar te leren. Het uitgangspunt blijft dat de minister verantwoordelijk is voor de informatievoorziening en in het besluit is nog ruimte om rekening te houden met de specifieke situatie van een departement.

Hoewel privacy geen expliciete inbedding binnen het CIO-besluit kent, die bijvoorbeeld informatiebeveiliging wel heeft, is uit de toelichting op het besluit duidelijk dat van de CIO verwacht wordt ook privacy mee te nemen in alle digitaliseringsvraagstukken. Zo staat er:

- 'De CIO moet kunnen adviseren en oordelen over alle aspecten van digitalisering en informatievoorziening, waaronder aspecten zoals informatiebeveiliging, privacy en de ontwikkeling en het beheer van informatiesystemen, in elk stadium van het uitvoeringsproces, de beleidsontwikkeling of het bedrijfsvoeringproces.'
- 'De kennis en ervaring stelt een CIO-office in staat om digitaliseringsvraagstukken en -beleid integraal te benaderen en daarmee het juiste evenwicht te vinden tussen beleidsdoelen enerzijds en onder meer informatievoorzieningsaspecten als informatiebeveiliging, privacy, openbaarheid en duurzame toegankelijkheid anderzijds.'
- 'De CIO is, in samenspraak met de CISO, belast met de continue vernieuwing van informatiesystemen op het gebied van informatiebeveiliging, privacy en de technologische ontwikkeling van functionaliteiten.'
- 'In samenspraak met de CIO is de CISO belast met de continue ontwikkeling van het rijksbrede beleid op het gebied van informatiebeveiliging en privacy van informatiesystemen en diensten.'

In dit onderzoek hebben we het CIO-besluit als een vaststaand feit beschouwd, in die zin dat er in de toekomst aanpassingen mogelijk zijn voor de CDO en eventueel een CPO-functie, maar we geen uitspraken doen over een wijziging van de beschrijving van de CIO- of CISO-functie. Met andere woorden, de beschreven scenario's in hoofdstuk 3 steunen op de beschrijving van de CIO- en CISO-functie zoals opgenomen in het CIO-besluit.

Bovendien merken we op dat de vorming van het huidige CIO-stelsel een lang proces is geweest met vele kleine stappen. Het is de verwachting dat het inrichten van de governance op privacy ook tijd nodig heeft om op zowel departementaal als rijksbreed niveau plek te krijgen in samenhang met de andere rollen. Aansluiten bij de stevigheid van een CIO-stelsel verkleint de implementatietijd.

2 https://wetten.overheid.nl/BWBR0044613/2021-01-01/0
3 https://zoek.officielebekendmakingen.nl/kst-26643-656.html
4 https://zoek.officielebekendmakingen.nl/blg-917402.pdf
5 https://zoek.officielebekendmakingen.nl/stcrt-2020-62488.html
6 https://www.rijksoverheid.nl/documenten/rapporten/2021/10/19/onderzoeksrapport-naar-uitkomsten-nulmeting-besluit-cio-stelsel-rijksdienst-mei-2021

2.2 I-strategie

Het ontwikkelen van een I-strategie Rijk en op dit moment in het bijzonder de I-strategie Rijk 2021-2025[7], is één van de taken van de CIO Rijk en de CISO Rijk. De I-strategie Rijk beschrijft de belangrijkste beleidsprioriteiten op het vlak van de digitale transitie. In tien thema's staat verwoord wat de gezamenlijke prioriteiten zijn van alle CIO's binnen de rijksoverheid op het gebied van informatievoorziening.

Niet onopgemerkt blijft het feit dat men doordrongen lijkt te zijn van een goede basis voor informatiebeveiliging en privacy. In vele thema's staat een samenhang benoemd met deze onderwerpen. Zo wordt in thema 2 tot en met 7 op zijn minst binnen elk thema een notie over privacy gemaakt. Bijvoorbeeld binnen *thema 2 - Digitale weerbaarheid*, waar benoemd staat dat (1) de aanpak van privacy nog niet op orde is, (2) privacy van belang is voor digitale weerbaarheid en dat (3) risicoafwegingen rondom informatievoorziening, inclusief privacy, chef-sache zijn. Ten aanzien van dat laatste staat expliciet benoemd dat privacy een vast onderwerp op de agenda van de bestuursraad en directieteam is. Een ander thema waarin privacy een duidelijk belangrijk onderwerp is, is *thema 6 - Data en algoritmen*. Hierin staat het belang beschreven van kansen op het gebied van data die weer leiden tot uitdagingen aan de andere kant, zoals op het gebied van privacy. Belangrijke notie hier is tevens dat verkokering van vakgebieden, zoals informatiebeveiliging, archivering en privacy niet helpt bij de sturing op data.

Tot slot staat in de I-strategie beschreven dat er een voorstel zal komen voor een nieuw in te richten CDO-rol binnen het CIO-stelsel. Over deze functie staat alleen de volgende toelichting: *'Waar de CIO zich vooral richt op de functionele informatievoorziening, houdt de CDO zich bezig met het inhoudelijke gebruik van data en het beheersen van risico's.'*

7 https://www.digitaleoverheid.nl/document/i-strategie-rijk-2021-2025/

2.3 Three lines of defense model

Het three lines of defense model[8], ook wel genoemd 3-LoD, wordt gebruikt om de governance rondom risicomanagement in te richten. Het model beschrijft een methode voor organisaties om op verschillende lagen in control te zijn, door bijvoorbeeld de juiste checks en balances in te richten en de verantwoordelijkheden op de juiste plek neer te leggen.

De verschillende verdedigingslinies binnen een organisatie, vertaald naar privacy risicomanagement, zijn als volgt te omschrijven:

- In de *eerste lijn* gaat het om business-/lijnmanagement, die verantwoordelijk is voor zijn eigen processen en de keuzes en risico's die het hierin maakt. Het correct omgaan met privacy hoort hierbij, maar ook bijvoorbeeld het accepteren van bepaalde restrisico's in afweging met andere waarden binnen de organisatie, zoals de realisatie van de beleids- en uitvoeringsdoelstellingen.
- De *tweedelijnsfunctie* (zoals een privacy officer of -coördinator) ondersteunt hierbij, zodat het lijnmanagement deze verantwoordelijkheid kan pakken. Een CPO hoort, net als een CIO als CISO, in de tweede lijn thuis. De tweede lijn voert onder andere taken uit als het adviseren, coördineren en monitoren/bewaken van specifieke risico's. Onder meer de ontwikkeling van privacybeleid en het controleren of de eerste lijn binnen deze kaders werkt horen hierbij.
- De *derde lijn* controleert en houdt toezicht. Deze richt zich specifiek op het samenspel tussen eerste en tweede lijn en of dit goed verloopt. En in geval van privacy betekent dit ook dat dit toezicht in de gaten houdt of de organisatie zich houdt aan de Algemene Verordening Gegevensbescherming (AVG). Primair vormt de functionaris gegevensbescherming (FG) de derde lijn. Daarnaast zijn onafhankelijke interne audits en bijvoorbeeld een Auditdienst Rijk (ADR) ook vormen van derdelijnstoezicht, al wordt extern toezicht als de ADR ook wel benaderd als vierdelijnstoezicht.

Noodzakelijk bij het three lines of defense model is dat het een integrale aanpak betreft, waarbij binnen een goed ingericht stelsel de verschillende lijnen op elkaar kunnen steunen en elkaar versterken. Het goed verdelen van de verantwoordelijkheden voorkomt dat er risico's gemist worden of dat er dubbel werk gedaan wordt. Het blijft echter van belang dat het lijnmanagement zich verantwoordelijk blijft voelen voor risico's.

8 Zie onder andere Het three lines of defense model van het IIA", The Institute of Internal Auditors (IIA), 2020

In het CIO-besluit staat dat een departementale CIO belast is met het inrichten van het CIO-stelsel voor het ministerie en de onder haar ressorterende dienstonderdelen. Het lijnmanagement is integraal verantwoordelijk en de departementale CIO heeft onder andere als taak om het lijnmanagement te adviseren over informatievoorziening en digitalisering. De departementale CISO moet bijvoorbeeld een departementaal risicobeeld bijhouden en kan hier lijnmanagement gevraagd en ongevraagd over adviseren. Rijksbreed wordt er volgens dezelfde principes gewerkt. In dat geval zijn de overheidsinstanties de eerste lijn, ligt een tweede lijn bij het ministerie van BZK (bijvoorbeeld in het opstellen en toezien van rijksbrede uitgangspunten en kaders) en is een derde lijn een onafhankelijke toezichthouder.

Kortom, de taken, verantwoordelijkheden en bevoegdheden van de functies binnen het CIO-stelsel richten zich expliciet op de tweede lijn.

Op basis daarvan hanteren we voor dit onderzoek als uitgangspunt dat als gesproken wordt over een inrichting van privacy governance binnen CIO Rijk dit alleen de tweede lijn kan betreffen en niet de derdelijns FG's.

2.4 Rijksbreed AVG-onderzoek Auditdienst Rijk

De Auditdienst Rijk (ADR) heeft in 2021 en 2019 haar rijksbrede AVG-onderzoek[9] uitgebracht. Het onderzoek heeft als doel om inzicht te krijgen in de maatregelen rondom de inzage van gegevens, de kwaliteit van registers rondom verwerkingsactiviteiten en de activiteiten die ondernomen zijn naar aanleiding van het voorgaande AVG-onderzoek. Het gaat hierbij om het stelsel van maatregelen voor de naleving van de AVG per departement.

Op basis van de bevindingen per departement is een rijksbreed beeld opgesteld. In het onderzoek over 2021 wordt onder andere geconstateerd dat de departementen zich in verschillende stadia van volwassenheid bevinden, dat verschillende processen zeer divers zijn ingericht en bijvoorbeeld wijzigingsverzoeken niet eenduidig worden afgehandeld. Ze constateren dat verbetertrajecten beperkt zijn opgestart, onder andere door gebrek aan privacycapaciteit en prioritering.

De uiteindelijke bevinding is *dat 'Inrichting privacymanagement en privacy governance binnen de rijksoverheid nog in ontwikkeling (is)'*. Hierbij wordt aangegeven dat een meer uniforme en eenduidige aanpak rondom privacy wenselijk zou zijn en dat *'de verdere inbedding van privacymanagement binnen de rijksoverheid noodzakelijk is'*. Op deze manier kan het niveau van privacybescherming omhoog.

Hierin wordt ook een koppeling gemaakt met het Besluit CIO-stelsel Rijksdienst, waarin privacy nog geen expliciete rol speelt. De onderzoekers geven aan dat de precieze rol van privacy in dit stelsel nog niet bekend is, maar het wel kan bijdragen aan *'een meer gelijke aanpak en een gedeelde visie over de invulling van privacymanagement'*. Ze benadrukken ten slotte dat de rijksbrede privacy governance moet worden geformaliseerd.

2.5 Motie Verhoeven

Op 3 februari 2021 is een motie in de Tweede Kamer aangenomen over het aanstellen van een chief privacy officer bij uitvoeringsorganisaties[10]. In deze motie wordt geconstateerd dat *'de overheid structureel tekortschiet op AVG-dataveiligheidsprincipes (...)'* en een chief privacy officer op hoog niveau *'kan toezien dat privacy en informatieveiligheid al bij het ontwerp en de uitrol van IT-systemen gewaarborgd worden'*. Mede uit deze motie blijkt dat de Tweede Kamer privacy in toenemende mate als zeer belangrijk onderwerp ziet. Hoewel de minister de motie ontraadde, ingegeven door het feit dat reeds alle organisaties een FG en een CIO hebben, nam de Kamer de motie aan met 96 stemmen voor.

Op 29 april 2022 stuurde de minister van BZK een brief aan de Kamer[11]. Hier staat te lezen dat de minister mede naar aanleiding van de Motie Verhoeven voornemens is om volgend jaar met een voorstel te komen om het interne toezicht op de informatiehuishouding te verstevigen binnen het CIO-stelsel.

9 In onder andere het Rijksbreed AVG Onderzoek (2021)

10 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z02217&did=2021D04899

11 https://open.overheid.nl/repository/ronl-fe6243dd99be2e6dc212a90f5390f-3580fd8c36f/1/pdf/kamerbrief-over-monitoring-sociale-media-en-naleving-avg-door-overheden.pdf

2.6 Onderzoek ICTU CDO-functie

In februari 2021 heeft ICTU een onderzoek dat zij uitvoerden in opdracht van BZK naar de rol en positie van de CDO gepubliceerd.[12] Het is een eerste verkenning naar de (ontwikkeling van de) rol van CDO binnen de overheid. Het rapport geeft aan dat er een passende data governance moet worden opgesteld, *'gelet op de Europese ontwikkelingen, Nederlandse ambities en de behoeften uit de praktijk'*.

Het doel van de CDO-rol is om de uitvoering van een datagedreven overheid te bevorderen, met inachtneming van publieke waarden. Het rapport stelt dat een CDO duidelijk de aansluiting moet zoeken met het primaire proces, zonder hiervoor de verantwoordelijkheid over te nemen. Met andere woorden, ook hier wordt een tweedelijnsfunctie beschreven conform het three lines of defense model.

Uit het onderzoek zijn er vier verschillende typen CDO te onderscheiden:

- Verandermanager en aanjager van innovatie, richting een datagedreven organisatie.
- Beheerder van data, waarbij het vooral gaat over het inrichten van de governance rondom data.
- Uitvoerder van data-analysestrategie.
- Beheerder en beheerser van kwaliteit en risico's.

Uit het onderzoek van ICTU blijkt dat de rol bij verschillende organisaties anders ingericht is: *'Geen van de geïnterviewde CDO's in deze verkenning delen dezelfde portefeuille van verantwoordelijkheden, aangezien elke CDO de rol heeft aangepast aan de unieke behoeften en het volwassenheidsniveau van zijn of haar organisatie'*. Een CDO kan een CDO-team inrichten voor de uitvoering van de werkzaamheden, afhankelijk van de aard en ambitie van een organisatie. Een expert privacy, beveiliging en ethiek is één van de mogelijke rollen: *'Expert op het gebied van ethiek, beveiliging en/of privacy, ondersteunt de organisatie met de focus op deze aspecten. Hij/zij helpt daarnaast bij het opstellen van een privacyimpactassessment en overige privacy- en/of ethiekstukken'*.

Het rapport betreft de meest uitgewerkte beschrijving van de CDO-rol binnen de overheid en beschouwen we daarmee als belangrijke basis om uitspraken te doen over een mogelijke integratie tussen de governance op privacy en het CDO-stelsel.

12 https://privacy-web.nl/wp-content/uploads/po_assets/560652.pdf

HOOFDSTUK 3

Huidige inrichting privacy governance

We hebben de huidige situatie in kaart gebracht door middel van een quickscan. We hebben hiervoor gesproken met (concern/ chief) privacy officers, CDO's en betrokken functionarissen van CIO Rijk (voor een volledig overzicht van geïnterviewde functionarissen zie paragraaf 6.2). Tezamen met de documentatie die we reeds bekeken hadden en de aanvullende documentatie die we kregen in de interviews, geven we hieronder de zaken weer die we belangrijk achten voor de verdere uitwerking.

3.1 Inrichting privacy governance departementen

3.1.1 Inrichting privacy per departement

Op dit moment is de inrichting voor privacy niet rijksbreed geformaliseerd. Dit betekent dat binnen elk departement op eigen wijze invulling gegeven wordt aan privacy. Op hoofdlijnen zien we overeenkomsten binnen de inrichtingen. Zo heeft elk departement dat we spraken, op een na, een functie van privacy officer ingericht. Bij het ene departement is dit een chief privacy officer (hierna: CPO) met eventuele decentrale privacy officers, bij het andere departement werkt men juist weer alleen met privacy officers. De grotere departementen met een hogere volwassenheid en meer taak- en uitvoeringsorganisaties, zoals het Ministerie van Justitie en Veiligheid (min JenV), werken hierbij vaker met een CPO en maken daarbij vaker gebruik van een decentraal stelsel van privacyfunctionarissen. In algemene zin kunnen we in elk geval stellen, op basis van de interviews, dat er een beweging richting het instellen van een CPO lijkt te zijn.

Een andere overeenkomst tussen vrijwel alle departementen is het feit dat er gewerkt wordt langs de lijnen van het three lines of defense model. Zie hiervoor ook de toelichting in het vorige hoofdstuk. De wettelijk verplichte Functionaris Gegevensbescherming (hierna: FG) is hierbij, mede op basis van de wettelijke verantwoordelijkheden die een FG heeft, de derde lijn binnen het departement. Het lijnmanagement is primair verantwoordelijk voor privacy binnen de eigen processen en vormt daarmee de eerste lijn. En de (C)PO is gepositioneerd in de tweede lijn. Van daaruit ondersteunt de (C)PO het lijnmanagement in het geven van uitvoering aan de eerstelijnsverantwoordelijkheid, maar de (C)PO vormt ook een belangrijk controlerende of bewakende functie op de afspraken en het geschreven beleid binnen de eigen organisatie. Het verschil met de controlerende functie van de FG zit vooral in het feit dat de (C)PO controleert of men zich houdt aan de interne regels, terwijl de FG toetst of de juiste waarborgen voor betrokkenen zijn ingericht conform de AVG en of het spel tussen eerste en tweede lijn op een juiste manier verloopt.

Grote verschillen zien we in de verschillende functies die betrokken zijn bij privacy binnen de departementen. Waar in sommige departementen alleen (C)PO('s) en een FG aanwezig zijn, zien we bij anderen ook privacyjuristen, privacycoördinatoren en CISO's die een expliciete rol binnen de privacytaken hebben gekregen.

3.1.2 Rol en positionering departementale CPO

De departementale CPO-functie dan wel -rol is zeer verschillend ingericht. In brede lijnen heeft de CPO in elk geval een rol bij de ondersteuning van het lijnmanagement. Waarbij dient opgemerkt te worden dat de CPO in het ene departement nadrukkelijk gesprekspartner is van het hoger management, terwijl in andere departementen de CPO meer een adviseur is die benaderd wordt bij vraagstukken die leven bij het lager management of in de meer operationele sfeer. Ook heeft de CPO veelal een belangrijke rol in het opstellen van het privacybeleid. Vaak gebeurt dit in overleg met de FG, maar is het onderdeel van de taken en verantwoordelijkheden van de CPO. Ook levert de CPO aan de lijn ondersteuningsproducten die enerzijds de lijn helpen bij het invullen van de privacyverantwoordelijkheid en anderzijds zorgen voor een eenduidige wijze van de uitvoering van het beleid binnen een organisatie. Met name dit laatste aspect zorgt ook voor het verhogen van de kwaliteit. De mate waarin een CPO ook een vorm van controle of bewaking op het beleid mag of kan uitvoeren, verschilt bij de departementen en is ook sterk afhankelijk van de eigen invulling van de functie. Er zijn ook CPO's die dit onderdeel geheel bij de FG laten liggen. We zien ook dat hier een grijs gebied is tussen beide functies. Oorzaken die hiervoor naar voren zijn gekomen is het ontbreken van een heldere taakafbakening, capaciteitsgebrek in de tweede lijn en de wijze waarop informele samenwerking tussen FG en CPO bij de met name wat kleinere departementen gegroeid is. Tot slot zien we als zeer belangrijke taak van de CPO bij vrijwel alle organisaties het vergroten van de bewustwording op het gebied van privacy bij alle medewerkers. De mate waarin dit gebeurt verschilt vervolgens wel weer aanzienlijk.

Of een CPO een volwaardige functie of een rol bij een functionaris is, verschilt. Hierin zien we in elk geval dat de grotere uitvoeringsorganisaties die we gesproken hebben een hogere mate van volwassenheid lijken te hebben dan veel kerndepartementen als het gaat om de inrichting van de privacyfunctie. In gesprek met enkele van hen is hierbij de uitleg naar voren gekomen dat de uitvoering ook al langer nadrukkelijk vraagt om een goede privacyfunctie en er daardoor eerder ruimte was voor een goede inrichting van de privacyorganisatie.

We zien verder dat de positionering van de CPO verschilt. Zo zijn er CPO's gepositioneerd onder de CIO, onder bestuursondersteuning of in de SG-kolom. Veelal hebben we hier ook teruggekregen dat men nog zoekende is naar de juiste plek binnen het departement. Ook is men op verschillende plekken nog zoekende naar hoe het samenspel met de CISO verloopt. Hier zien we wel veel verschillen in tussen de departementen. We zien niet direct een verband tussen de mate van effectiviteit van invulling en de positie van de CPO, maar dit is ook een vraagstuk op zichzelf en niet mee te nemen als klein aspect binnen dit onderzoek.

Bij de meeste departementen is er een stevige samenwerking tussen FG en CPO. Bij de meeste departementen, bijvoorbeeld heel expliciet bij ministeries van JenV, EZK en LNV, zien we een organisatorische scheiding tussen tweede en derde lijn. Op andere plekken zien we echter meer vermenging tussen tweede en derde lijn. Zo zien we op enkele plekken dat de FG binnen een typische tweedelijnsafdeling als de CIO-office gepositioneerd is. De mate waarin dit als problematisch wordt ervaren ligt vooral aan de praktische invulling die men zelf geeft aan de functie. We hebben hierbij ook voorbeelden gezien waarin met name het voordeel van een stevige samenwerking benut wordt door een dergelijke positionering van de FG.

Tot slot wordt binnen één departement aangegeven dat de FG- en de CPO-functie door elkaar heen lopen, doordat het stelsel van privacy officers bij het kerndepartement geen CPO-functie heeft en dit in grote mate wordt ingevuld door de FG zelf. Een betrokken functionaris die we spraken bij dit departement ervaart dit als lastig in de praktijk en heeft behoefte aan een strakkere inrichting van de three lines of defense.

3.1.3 Afstemming en samenwerking privacygerelateerde taken

Buiten de reeds hierboven vermelde samenwerking tussen FG en CPO, zien we ook dat de samenwerking tussen de (overige) verschillende privacyfunctionarissen enorm verschilt. Dit hangt vaak nauw samen met de grote van een departement. Immers, wanneer meer functionarissen betrokken zijn bij privacy, ontstaan vaak ook meer gerichte overlegstructuren. Bij de grotere departementen zien we overlegstructuren die geformaliseerd zijn in beleidsstukken. Bijvoorbeeld privacyboards, privacyplatforms, kennisgroepen, juridische netwerken data en privacy of privacyoverleggen. Bij kleinere departementen, in dit geval zijn de ministeries OCW, AZ en BuZa hier voorbeelden van, zien we vooral informele overlegstructuren. In algemene zin constateren we dat de overleggen veelal geen enkel mandaat hebben en vooral gericht zijn op het doorspreken van lopende zaken en/of op kennisuitwisseling.

Evenals de formalisatie van overleggen verschilt, verschilt ook de frequentie van overleggen enorm. Van wekelijkse overleggen tot halfjaarlijkse overleggen. De grote lijn is dat in elk geval per één tot twee maanden een overleg met privacyfunctionarissen plaatsvindt binnen de organisatie. In algemene zin merken we dat bij departementen waar minder reguliere en frequente overlegstructuren zijn ook benoemd wordt dat er een gebrek aan adequate afstemming is.

Verder zien we in de meeste gevallen een vorm van samenwerking met de CISO en andere functionarissen op het gebied van informatiebeveiliging. In een enkel geval is de functie gecombineerd, maar over de gehele lijn kun je stellen dat op het gebied van informatiebeveiliging en privacy binnen het Rijk goed samengewerkt wordt. Vaak werd aangegeven in de interviews dat men dit ook als versterkend ervaart voor beide vakgebieden. Op sommige zaken is er sprake van 'gedeelde belangen en samen staan we sterker', bij andere issues is functionele samenwerking noodzakelijk vanuit beide disciplines (denk bijvoorbeeld aan datalekken). Waar belangen uiteenlopen tussen informatiebeveiliging en privacy, is men, aldus de interviews waarin dit naar voren kwam, goed in staat om samen het juiste gesprek hierover te voeren.

In een enkel geval horen we in de interviews dat er afstemming tussen CDO en CPO plaatsvindt. Oorzaak dat dit nog weinig naar voren komt is onder meer dat de CDO-rol relatief nieuw is en bij nog lang niet alle departementen is ingericht op het moment van het onderzoek. Ook ziet niet elke CDO (op dit moment) een verbinding met privacy in zijn of haar werk.

Voorloper: Ministerie van Justitie en Veiligheid
In veel interviews is aangegeven dat men de huidige inrichting binnen JenV als zeer sterk ervaart. Waarbij JenV niet het enige genoemde departement is (ook EZK, LNV en OCW werden genoemd), maar wel het vaakst benoemd is als sterk voorbeeld. Meerdere departementen hebben er dan ook voor gekozen om elementen van deze inrichting over te nemen. De elementen van JenV die als sterk worden ervaren, hebben met name te maken met de organisatorische inrichting en de betrokkenheid van het management. Derhalve beschrijven we hier kort de wijze waarop JenV het georganiseerd heeft.

We zien dat bij JenV de CPO-functie een volwaardige functie binnen het CIO-office vervult, naast een CDO en CISO. Ook zien we dat er een functionerend stelsel van privacy officers/medewerkers met privacy in de portefeuille gerealiseerd is sinds 2017. De privacy officers komen twee keer per maand bij elkaar. Ook is er een formeel privacyboard. Hiermee is JenV verder in formalisering van de privacyfunctie dan menig ander departement.

JenV geeft hierbij aan dat de grotere departementen met uitvoeringsorganisaties kunnen leren van deze wijze van werken, maar dat kleinere departementen (stafministeries) weinig hiervan kunnen leren aangezien de uitdagingen waar zij voor staan geheel anders zijn. De focus van de kleinere (beleids)departementen zit meer op zaken als rechten van betrokkenen en waarborgen van privacy binnen beleid, terwijl bij de grotere departementen met veel uitvoeringsorganisaties ook daadwerkelijk veel gegevensverwerkingen plaatsvinden.

3.1.4 Borging privacy

Hoewel privacywetgeving al van ver voor de AVG in 2018 is, komt in de meeste gesprekken nadrukkelijk naar voren dat privacy pas vanaf de invoering van de AVG echt aandacht heeft gekregen. Daardoor is de privacyorganisatie veelal rond die tijd pas steviger geworden. Men vindt overwegend dat de borging van privacy aanzienlijk is toegenomen in de afgelopen vier jaar. Tegelijkertijd wordt geconstateerd dat privacy vaak nog vooral gedreven wordt vanuit de compliancegedachte en niet als onderdeel van organisatiebreed risicomanagement. Daar waar de Autoriteit Persoonsgegevens juist vanuit risico's voor de betrokkenen privacy in ogenschouw neemt.

De aanwezigheid van de benodigde capaciteit, kennis en kunde is een zorgpunt bij een groot aantal geïnterviewden. Het is momenteel lastig om goed opgeleide medewerkers te vinden. Hierdoor is de capaciteit beperkt en is er geen grote vijver van hoogopgeleide privacyprofessionals om uit te vissen. Het behouden en vergroten van die capaciteit en kennis ziet men als een randvoorwaarde om een volgende stap in volwassenheid te zetten. Dit wordt ook benadrukt door een aantal FG's; zij zien een sterke tweedelijnsfunctie op privacy als een vereiste om als organisatie de juiste dingen en de dingen juist te doen. Daar waar capaciteitsgebrek aanwezig is in de tweede lijn, komt naar voren dat de FG soms (te) veel in een adviserende tweedelijnsfunctie moet opereren. Dit bemoeilijkt de toetsende rol niet alleen, maar leidt potentieel ook tot de onwenselijke situatie dat de slager zijn eigen vlees keurt.

In algemene zin onderschrijft men de constatering van de ADR dat verdere inbedding van privacymanagement binnen het Rijk noodzakelijk is. De visie op de wijze waarop dit moet gebeuren loopt sterk uiteen bij de gesprekspartners. Oplossingen die worden aangedragen betreffen bijvoorbeeld het verstevigen van de centrale en rijksbrede privacycoördinatie, of het creëren van meer uniformiteit met kaders, hulpmiddelen en kennisdeling; waar anderen het zien als een oproep om de capaciteit voor privacy te intensiveren.

Ten slotte is het opvallend te noemen dat men kansen ziet in het rijksbreed ontwikkelen van hulpmiddelen die CPO's in hun eigen departement kunnen inzetten, maar we tegelijkertijd juist ook een zeer intern gerichte werkwijze naar voren horen komen. Dit wordt deels verklaard doordat in interviews vaak verwezen wordt naar het feit dat privacy een ministeriële verantwoordelijkheid is, terwijl men ondertussen ook de noodzaak ziet om meer als één overheid te opereren richting burgers op het vlak van privacy. Door de rijksbrede samenwerking vooral te beperken tot hulpmiddelen, wordt een stap richting het opereren als één overheid geformuleerd, terwijl men ondertussen de vrijheid behoudt om privacy op eigen wijze te besturen.

3.2 Rijksbrede privacy governance

3.2.1 Huidige rijksbrede privacy governance

In aansluiting op het three lines of defense model, ligt de verantwoordelijkheid voor privacy volledig bij de departementen. Dit is logisch, want elk departement is eerstelijns verantwoordelijk voor privacy binnen de eigen processen. Ook op de tweede lijn is er echter geen formele rijksbrede verantwoordelijkheid. Hoewel privacy in minder expliciete mate benoemd wordt in het CIO-besluit, wordt ervaren dat privacy geen formele borging kent binnen CIO Rijk.

Ook merken we in de gesprekken dat er onduidelijkheid en onvrede is over hetgeen wel ingericht is rondom privacy. De PAR zelf ervaart dat momenteel geen invulling gegeven kan worden aan een rijksbrede coördinerende rol, mede vanwege het feit dat hiervoor formele gronden (mandaat) ontbreekt. Vanuit de departementen wordt opgemerkt dat het voor lang niet iedereen duidelijk is waar de PAR nu wel en niet over gaat. En dit werkt twee kanten op. We horen hierdoor onvrede over waar de PAR wel zichtbaar is, maar ook over waar de PAR niet zichtbaar is. Wel merken we op dat over het algemeen de CPO's positiever gestemd zijn over de functie van de PAR dan de FG's. De FG's laten zich in meerdere interviews kritisch uit over situaties waar zij menen vanuit hun wettelijke verantwoordelijkheid een rol te moeten spelen en zich niet voldoende gekend voelen door de PAR hierin. We concluderen hieruit vooral dat er behoefte is aan een goede beschrijving en vaststelling van de verschillende functies rondom privacy.

Er zijn twee belangrijke privacygremia op dit moment. Dat is de CPO-raad, waarin privacy officers van elk departement zitting hebben. Het is een niet-geformaliseerd gremium en heeft daarmee ook geen status van een formeel voorportaal richting CIO-beraad. Het kenmerkt zich vooral door het bespreken van casuïstiek met elkaar, het delen van rijksbrede ontwikkelingen en het uitwisselen van best practices.
Het is onbekend wat de precieze relatie is met het tweede gremium, het rijksbreed overleg met FG's (RPFG) is tevens een niet-geformaliseerd gremium. In dit gremium zijn de FG's van de departementen vertegenwoordigd. In rijksbrede bedrijfsvoeringsprojecten adviseren zij de PAR. De PAR adviseert op zijn beurt de Groepsondernemingsraad Rijk (GOR) en de interdepartementale coördinerende overlegorganen, zoals het CIO-beraad, conform de PAR-procedure. Naast deze formelere functie, worden ook hier casuïstiek en best practices uitgewisseld.

3.2.2 Rijksbreed inzicht in privacy (huidige situatie)

Er is geen formele noodzaak om vanuit de departementen inzicht te verschaffen in de stand van zaken op het gebied van privacy en de risico's aan CIO Rijk. In de interviews wordt aangegeven dat men terughoudend is met het proactief delen van deze informatie, omdat onbekend is wat er met die informatie gebeurt, vanuit welk mandaat dit dan zou gebeuren en omdat er al veel andere informatie aangeleverd moet worden.

Een gevolg hiervan is dat er geen mogelijkheid is om uniform te rapporteren over privacy, bijvoorbeeld aan de Tweede Kamer. Dit is opmerkelijk als we naar het CIO-besluit kijken waarin privacy als onderdeel van de informatiehuishouding staat benoemd en daarmee onderdeel uitmaakt van het takenpakket van de CIO.

3.3 Rol CDO

In het afgelopen jaar is men binnen CIO Rijk gestart met het inrichten van een CDO-stelsel. Het inrichten van het CDO-stelsel gaf mede aanleiding tot dit onderzoek, aangezien er onduidelijkheid bleek te zijn over of privacy wel of niet tot het takenpakket van de CDO behoort. We hebben dan ook expliciet met de geïnterviewden gesproken over de mogelijkheid tot integratie van privacy binnen de CDO-rol.

De belangrijkste constatering op dit vlak is dat er nog veel onduidelijkheid is over de CDO-rol en iedereen er zijn of haar eigen beelden bij heeft. We zien ook dat op basis van die eigen beelden soms stevige conclusies getrokken worden over de rol. Wat we niet gezien hebben is een uitgewerkte beschrijving van de CDO-rol, anders dan wat er, relatief hoog over, beschreven staat in het onderzoek van ICTU over de rol en positie van de CDO. We hebben namelijk geen documenten ontvangen met een feitelijke omschrijving van de taken, verantwoordelijkheden en bevoegdheden van deze functie, net als de scope en/of het werkgebied. Tegelijkertijd is men al wel gestart met het inrichten van een CDO-functie binnen elk departement.

Hoewel we onderschrijven dat het starten en samen verder inrichten een goede tactiek kan zijn voor het creëren van draagvlak en snelheid erin houden, concluderen we ook dat de CDO's die we spraken bij de verschillende departementen een behoorlijk uiteenlopende blik hadden op de functie. Waar bij het ene departement de CDO zich richt op het benutten van kansen op het gebied van datagedreven werken, is men bij andere departementen juist vooral gericht op het op orde brengen van de basis. We hebben drie CDO's gesproken, dit beperkt het beeld enigszins. Tegelijkertijd constateren we dat deze drie gesprekken geleid hebben tot drie verschillende beelden en de verwachting niet is dat bij een bredere toetsing onder CDO's dit leidt tot zeer andere conclusies.

Er is een duidelijk verschil tussen de manier waarop de CDO's bij de departementen aankijken tegen privacy binnen hun rol en de manier waarop dit vanuit het team Informatiehuishouding – Data en Algoritmen bekeken wordt, die zich bezighoudt met de oprichting en het inrichten van de CDO-functie (hierna: CDO Rijk i.o.) bij CIO Rijk. Bij de CDO Rijk i.o. wordt nadrukkelijk gesproken over een tweeledige taak van de CDO, te weten het aanjagen van datagedreven werken en het voldoen aan wet- en regelgeving. De CDO's binnen de departementen zien echter vooral de component datagedreven werken nadrukkelijk naar voren komen. Daarmee constateren zij ook meer dan eens dat belangenverstrengeling kan ontstaan indien privacy binnen hun taakgebied wordt belegd en geven zij aan dat ze checks and balances van groot belang vinden en daarmee privacy buiten hun directe verantwoordelijkheid wensen te beleggen.

Dit is in lijn met de beelden van de meeste CPO's en FG's die benadrukken dat privacy in het kader van checks and balances een eigen positie nodig heeft en niet onderdeel kan zijn van dezelfde rol die juist datagedreven werken moet aanjagen. Kansen versus risico's en deze gebalanceerd bekijken en afwegen, maakt dat checks and balances goed georganiseerd moeten worden aldus de privacyfunctionarissen. Kortom, het is geen breed gedragen beeld dat CDO en privacy samen georganiseerd moeten worden.

3.4 Toekomstige inrichting privacy governance

Naast de quickscan over de huidige situatie, hebben we de geïnterviewden ook gevraagd naar kansen, belemmeringen, pluspunten en minpunten als het gaat om het rijksbreed organiseren van de privacy governance. Een aantal zaken die meermaals naar voren kwamen, nemen we hier expliciet op.

Men wil ook in de toekomstige inrichting vasthouden aan het three lines of defense model. Met name vanuit de FG's wordt benadrukt dat de eerstelijnsverantwoordelijkheid en het derdelijnstoezicht niet rijksbreeds georganiseerd kunnen worden. Wij beamen dat rijksbrede governance vooral over de tweedelijnsinrichting gaat. Rijksbrede governance vermindert op geen enkele wijze de ministeriële verantwoordelijkheid die bij elk departement ligt.

Men vindt het belangrijk om ruimte te hebben voor departementale bijzonderheden en is angstig voor een te grote focus op een eenduidige inrichting. Ook dit signaal begrijpen wij volledig. Er zit veel verschil tussen kleine beleidsdepartementen versus grote departementen met veel en grote uitvoeringsorganisaties. Dit vraagt om een andere focus qua taken vanwege de aard van de informatiehuishouding en een andere inrichting passend bij de wijze waarop het departement is ingericht.

Maak taken, verantwoordelijkheden en bevoegdheden van privacyfunctionarissen en -overleggen inzichtelijk en formaliseer deze, zodat er ook op het gebied van privacy mandaat en bevoegdheid is.

Waak voor een inrichting met many chiefs, but not enough indians. De zorg is dat er te veel functies op C-level ontstaan en hierdoor aan slagkracht wordt ingeleverd. Deze zorg is met name vanuit CIO Rijk geuit. Bij de departementen is immers veelal reeds gekozen voor de inrichting van een CPO-functie.

HOOFDSTUK 4

Scenario’s inrichting privacy governance

In dit hoofdstuk beschrijven we vijf verschillende scenario’s om de rijksbrede privacy governance in te richten (paragraaf 4.3). Voorafgaand aan het uitwerken van de verschillende scenario’s hebben we een profiel geschetst van de privacyfunctie en een toetsingskader gedefinieerd waaraan we de verschillende scenario’s toetsen (paragraaf 4.2).

4.1 Toetsingskader

Voorafgaand aan de uitwerking van de verschillende scenario's, hebben we uitgangspunten gedefinieerd en een profielschets van de taken en verantwoordelijkheden rondom privacy geschetst.

Deze uitgangspunten vormen een kader waaraan we de verschillende scenario's kunnen toetsen. Daarnaast hebben we een profiel geschetst waarin we op hoofdlijnen hebben uitgewerkt welke taken en verantwoordelijkheden (C)PO's zouden moeten hebben en welke kennis en vaardigheden daarvoor vereist zijn.

Om de verschillende scenario's te kunnen vergelijken, hebben we een toetsingskader opgesteld. Dit toetsingskader bestaat uit negen uitgangspunten die we hebben opgesteld op basis van de resultaten van de quickscan (desk study en interviews). Met andere woorden, deze uitgangspunten zijn zowel door ons, als belangrijke stakeholders en gesprekspartners die onderdeel waren van dit onderzoek, benoemd als belangrijke elementen waar rekening mee gehouden moet worden bij de uitwerking van de scenario's.

Uitgangspunt	
Zet privacy hoger op de agenda	We zien een brede wens vanuit de maatschappij, de politiek en het openbaar bestuur om privacy actiever en beter op de agenda te zetten. Zo wordt in de I-strategie expliciet benoemd dat rapportages over de aanpak van tekortkomingen en implementatie van privacymaatregelen zowel qua inhoud als timing verder moeten groeien.[13] Ook vanuit het parlement zien we eenzelfde beweging (zie bijvoorbeeld Motie Verhoeven[14]) en de recente brief vanuit minister en staatssecretaris.[15]
Bouw voort op bestaande rijksbrede structuren	Bij het uitwerken van verschillende scenario's hebben we voornamelijk gekeken naar mogelijkheden die passen binnen de bestaande structuren. De reden hiervoor is tweeledig. Ten eerste vinden we het van belang dat wijzigingen binnen de bestaande privacy governance voldoende realistisch moeten zijn en herkenbaar voor de medewerkers die erbinnen en eronder moeten werken. Daarnaast vinden we het van belang dat alternatieve scenario's ook binnen afzienbare tijd moeten kunnen worden geïmplementeerd.
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties	Tijdens de interviews is veelvuldig naar voren gekomen dat de verschillende departementen en uitvoeringsorganisaties erg van elkaar verschillen in mate van volwassenheid, complexiteit van verwerkingsactiviteiten, gevoeligheid van gegevens en positionering van privacyfunctionarissen. De grootste verschillen zitten (logischerwijs) tussen beleidsdepartementen en uitvoeringsorganisaties. Echter, ook de positionering van privacy varieert binnen organisaties, tussen positionering binnen het CIO-office, Bedrijfsvoering (BDV) en Bestuursorganisatie en Advies (BOA). We nemen daarom mee in hoeverre er binnen een scenario ruimte is om invulling te geven aan deze diversiteit.
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model	Alle gesprekspartners hebben aangegeven te werken volgens het three lines of defense model (3-LoD). Dit model legt de verantwoordelijkheid voor de processen primair bij het lijnmanagement (eerste lijn). Het inrichten van privacy governance binnen de rijksoverheid richt zich binnen ons onderzoek primair op het inrichten van de tweede lijn.
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's)	Ieder departement (en uitvoeringsorganisatie) heeft een eigen FG aangesteld die verantwoordelijk is voor het toezicht houden op de naleving van de geldende privacywetgeving binnen die desbetreffende organisatie. Wanneer men besluit om (een deel van) de tweedelijnstaken rijksbreed in te richten, is het van belang om te waarborgen dat dit niet onbedoeld leidt tot het beperken van de invloed van de FG's.
Zorg voor voldoende checks and balances tussen de verschillende functionarissen	Het waarborgen van het bestaan van voldoende 'checks and balances' kwam in veruit de meeste interviews als kernpunt naar voren. Deze term vertalen we als het principe om te waarborgen dat de taken en bevoegdheden van verschillende functionarissen voldoende gescheiden moeten zijn, en er voldoende mechanismen moeten bestaan om te waarborgen dat belangenafwegingen op de juiste wijze worden gemaakt en er voldoende macht en tegenmacht bestaat om hierin de juiste balans te vinden.
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/worden ingericht, zoals chief privacy officer (CPO)	Verschillende ministeries en uitvoeringsorganisaties hebben inmiddels de functie van CPO intern belegd en vastgelegd in het interne privacybeleid. Daarnaast zijn er nog enkele ministeries waar een dergelijke rol momenteel informeel vervuld wordt door een privacy officer, maar men wel bezig is om deze functie formeler te beleggen in een privacybeleid.
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries	Tijdens de interviews is verschillende keren benoemd dat er behoefte is om een breder rijksbreed mandaat te hebben om besluiten te kunnen nemen rondom het stellen van kaders en het nemen van maatregelen. Daarbij is expliciet benoemd dat de huidige PO-raad geen mandaat heeft en slechts een vrijblijvende adviserende rol vervult. Het huidige mandaat van de PAR is formeel beperkt tot een adviserende rol over rijksbrede kaders en voorzieningen.
Zorg voor een integrale aanpak	Veel vraagstukken raken niet alleen privacy, maar zijn breder. De business moet niet overladen worden met compliance gedreven adviezen vanuit elke hoek (CDO, CFO, CIO, CISO, CPO) en bijbehorende verantwoording, maar er moet een integrale aanpak zijn. Een genoemde oplosrichting is dat ervoor gezorgd wordt dat alle vraagstukken samenkomen bij de CIO en in het rijksbrede speelveld bij het CIO-beraad.

13 Zie I-strategie Rijk 2021 – 2025, p. 26
14 Motie Verhoeven c.s. over een chief privacy officer bij uitvoeringsorganisaties - Informatie- en Communicatietechnologie (ICT) in de Zorg, https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vlg0qsukr4zj
15 Brief regering, Monitoring sociale media en naleving AVG door overheden, 29 april 2022, 32761-224

Ieder scenario wordt op alle uitgangspunten getoetst. Op basis van onze toets hebben we een beoordeling gegeven door middel van een kleur. In de navolgende tabel geven we weer wat de betekenis van deze kleuren is.

Markering	Betekenis
	Het scenario geeft op een goede wijze invulling aan dit uitgangspunt.
	Het scenario voldoet op zichzelf niet volledig aan het uitgangspunt. We voorzien met het nemen van de juiste maatregelen echter geen onoverkomelijke problemen.
	Het scenario is niet in staat om op de juiste wijze invulling te geven aan dit uitgangspunt. Zelfs als er aanvullende maatregelen worden genomen om deze risico's te mitigeren, wordt alsnog onvoldoende voorzien in de politieke, bestuurlijke en maatschappelijke wensen.
	Dit uitgangspunt is in dit scenario niet van toepassing en dus niet toetsbaar aan het kader.

4.2 Profielschets

In ons onderzoek richten we ons op het inrichten van privacy governance binnen de tweede lijn van het 3-LoD model. In dat kader hebben we een profiel geschetst waarin we (i) algemeen beschrijven wat een tweedelijnsprivacyfunctionaris inhoudt, (ii) welke taken en verantwoordelijkheden deze functionaris hoort te hebben en (iii) met welke andere functies hij of zij veel zal samenwerken en afstemmen bij de uitoefening van zijn rol.

Tot slot hebben we er bewust voor gekozen om in deze fase de taken en verantwoordelijkheden nog niet te koppelen aan een specifieke functie, omdat deze taken en verantwoordelijkheden in ieder scenario toegepast moeten kunnen worden.

4.2.1 Omschrijving tweedelijnsrol/-functie

De tweedelijnsprivacyfunctionaris is primair belast met de ontwikkeling en coördinatie van het privacybeleid. Daarnaast ondersteunt hij de directie en het lijnmanagement van de betreffende organisatie met de implementatie en naleving van het privacybeleid. Afhankelijk van de organisatorische positionering van de functionaris wordt de omvang en scope van zijn functie bepaald.

4.2.2 Taken en verantwoordelijkheden

De tweedelijnsprivacyfunctionaris binnen de departementen is in ieder geval verantwoordelijk voor:

- Het ontwikkelen en actueel houden van een risicobeeld met betrekking tot privacy.
- Het bijdragen aan het opstellen en beheren van het meerjarig informatieplan voor de organisatie met betrekking tot de privacy.
- Het inrichten van een privacy governance voor het departement of dienstonderdeel en het toezien op de werking van deze privacy governance binnen dit departement of dienstonderdeel.
- Het zorgdragen voor het privacybeleid als onderdeel van het digitaliserings- en informatievoorzieningsbeleid. Dit houdt onder meer het opstellen, onderhouden en implementeren van privacybeleid in.
- Het ontwikkelen en coördineren van gegevensbeschermingsactiviteiten, -projecten en het zorg dragen voor een projectportfolio voor privacy.
- Het gevraagd en ongevraagd adviseren van de bestuursdirectie en het verantwoordelijk lijnmanagement over de privacy en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleids-en uitvoeringstrajecten, informatieprocessen en informatiesystemen.
- Het coördineren van de ADR- en AP-onderzoeken over privacy binnen het departement.
- Het monitoren en controleren van het privacybewustzijn binnen de organisatie, het adviseren van de organisatie hierover en het zorg dragen voor het vergroten van het bewustzijn over privacy binnen het ministerie of organisatieonderdeel.

Daarnaast vervult een tweedelijnsprivacyfunctionaris, afhankelijk van de positie van zijn functie, ook een rol richting de (departementale) CIO. In dat geval omvatten zijn taken en verantwoordelijkheden in ieder geval:

- Het bijdragen aan CIO-oordelen en kwaliteitstoetsen met betrekking tot privacy.
- Het toezien op naleving van de kaders en het informeren en adviseren van de leden van de departementale CIO-raad, de leden van de bestuursraad en de PAR en CISO Rijk over het toezien op naleving van deze kaders.
- Het gevraagd en ongevraagd adviseren van de CIO over privacy en de risico's daarvoor van voorgenomen wet- en regelgeving, investerings-, beleids- en uitvoeringstrajecten, informatieprocessen en informatiesystemen als onderdeel van het digitaliserings- en informatievoorzieningsbeleid.

Tot slot kan men ook rijksbreed een aantal taken en verantwoordelijkheden definiëren die behoren tot zijn of haar functie, zoals:

- Het in samenwerking met de CPO's en functionarissen gegevensbescherming opstellen en actueel houden van het rijksbrede risicobeeld met betrekking tot de bescherming van persoonsgegevens.
- Het inrichten van een rijksbreed CPO-stelsel en het toezien op de werking van dit CPO-stelsel.
- Het ontwikkelen, coördineren en monitoren van de implementatie en naleving van rijksbreed privacybeleid en -kaders, en de wijze waarop de gegevens over de bescherming van persoonsgegevens door de ministeries worden verstrekt.
- Het zorg dragen voor het rijksbrede privacybeleid als onderdeel van het rijksbrede digitaliserings- en informatievoorzieningsbeleid.
- Adviseren over de bescherming van persoonsgegevens en de risico's daarvoor van (voorgenomen) wet- en regelgeving, investeringen, beleid, uitvoeringstrajecten, informatieprocessen en informatiesystemen, voor zover deze betrekking hebben op de rijksdienst.
- Het gevraagd en ongevraagd uitbrengen van rijksbrede adviezen en verstrekken van informatie, inzake de bescherming van persoonsgegevens en het risicomanagement daarvan.
- Het toezien op naleving van de kaders en het informeren en adviseren van de leden van de departementale CIO-raad, de leden van de bestuursraad en de PAR en CISO Rijk over het toezien op naleving van deze kaders.
- Het bijdragen aan het opstellen van rijksbrede privacybeleidsstukken, rijksbrede DPIA's en andere rijksbrede privacyactiviteiten.
- Het coördineren van de samenwerking bij interdepartementale privacyvraagstukken.
- Het coördineren van de aanpak van rijksbrede inbreuken in verband met persoonsgegevens (dan wel datalekken) en calamiteiten.

4.2.3 Samenwerking

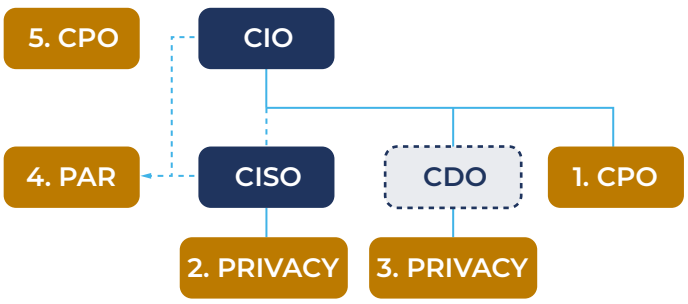
We zien dat de tweedelijnsfunctionarissen in de praktijk veel samenwerken met diverse medewerkers met verschillende achtergronden en uit verschillende lagen binnen de organisatie. Zo zal de tweedelijnsprivacyorganisatie moeten schakelen met de directie en het lijnmanagement, inzake het opstellen en implementeren van privacybeleid, het adviseren van beleidsmedewerkers en medewerkers uit de I-kolom over risico's in concrete gevallen, en dient deze zijn adviezen af te stemmen met andere functionarissen uit de tweede lijn, waaronder de medewerkers in het CIO-office ('departementale' CISO, CDO, CIO) en functionarissen uit de derde lijn, zoals bijvoorbeeld de FG en de ADR. Daarnaast zien we in het kader van interdepartementale vraagstukken een groeiende behoefte om ook met andere CPO's af te stemmen.

4.3 Scenario's

Op basis van de resultaten van de documentstudie en de input die we hebben opgehaald tijdens de interviews, hebben we vijf scenario's beschreven die de basis kunnen vormen van de ontwikkeling van een rijksbrede privacy governance, namelijk:

- **Scenario 1.**
  Privacy governance als aparte pijler binnen het CIO-stelsel.
- **Scenario 2.**
  Privacy governance onder de CISO binnen CIO-stelsel.
- **Scenario 3.**
  Privacy governance in nieuw CDO-stelsel.
- **Scenario 4.**
  Geen wijzigingen privacy governance.
- **Scenario 5.**
  Privacy governance in afzonderlijk CPO-stelsel.

We beschrijven de verschillende scenario's in subparagrafen die hierna volgen. Daarnaast toetsen we de verschillende scenario's aan het eerder beschreven toetsingskader (zie paragraaf 4.1). In onderstaande tabel is het totaaloverzicht van die toetsing weergegeven. De toelichting op het gegeven oordeel staat beschreven in de tabellen bij de verschillende scenario's in de opvolgende subparagrafen.



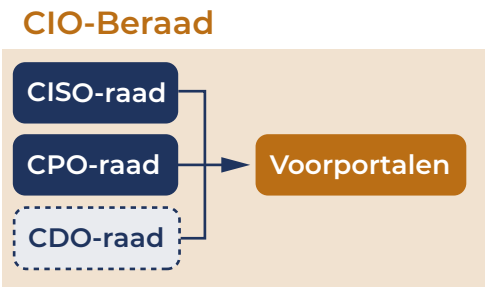
Figuur 1. **Overzicht scenario's**

Uitgangspunt	1. CPO onder CIO	2. Privacy onder CISO	3. Privacy onder CDO	4. Geen wijzigingen	5. Separaat CPO-stelsel
Zet privacy hoger op de agenda					
Bouw voort op bestaande rijksbrede structuren					
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties					
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model.					
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's).					
Zorg voor voldoende checks and balances tussen de verschillende functionarissen					
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/worden ingericht, zoals chief privacy officer (CPO)					
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries					
Zorg voor een integrale aanpak					

4.3.1 **Scenario 1.** Privacy governance als aparte pijler binnen het CIO-stelsel

In scenario 1 wordt een rijksbreed CPO-stelsel ingericht binnen het bestaande CIO-stelsel (zie Figuur 3. Organogram scenario 1).

Scenario 1 is erop gericht om zo veel mogelijk aan te sluiten bij bestaande principes en modellen waar volgens wordt gewerkt, zoals deze al reeds uitgewerkt zijn binnen het bestaande CIO-stelsel. In dit scenario wordt het huidige CIO-besluit gewijzigd en wordt een aparte privacy governance opgenomen in dit besluit. De privacy governance kan worden ingericht naar analogie van het CISO-stelsel. In deze paragraaf verwijzen we naar deze privacy governance middels de term CPO-stelsel.



Figuur 2. **Overlegstructuren scenario 1**

Figuur 3. **Organogram scenario 1**

Wat betekent dit voor de departementen?

Allereerst wordt het huidige CIO-besluit aangepast en uitgebreid door het toevoegen van de rol chief privacy officer (CPO). Ieder ministerie is verplicht om deze rol in te vullen. De omschrijving van deze rol, evenals de daarbij horende taken en bevoegdheden, worden beschreven naar analogie van de CISO.[16] Voor de omschrijving van deze rol, taken en verantwoordelijkheden van de CPO verwijzen we naar de profielschets in paragraaf 4.2.

In de praktijk betekent dit dat de CPO onderdeel wordt van het CIO-office, waardoor verdere samenwerking met de CIO, CISO en (toekomstig) CDO wordt vergroot. Om voldoende rekening te kunnen houden met de diversiteit van de verschillende ministeries, inclusief de daaronder ressorterende dienstonderdelen, raden we aan om in het CIO-besluit de minister ook de bevoegdheid te bieden om vanuit het departementaal CIO-stelsel binnen verschillende dienstonderdelen een aparte CPO aan te wijzen.[17]

Voor zover noodzakelijk worden voor de CPO een aantal formele bevoegdheden vastgelegd die de CPO, in acute gevallen, de mogelijkheid bieden om zich de secretaris-generaal of het verantwoordelijke lijnmanagement rechtstreeks van informatie te voorzien. Deze maatregel draagt bij aan het waarborgen van de 'checks and balances' tussen verschillende functionarissen.

Wat verandert er rijksbreed?

In dit scenario zijn we ook uitgegaan van het beleggen van de rol van CPO Rijk. Ook deze rol richten we in naar analogie van de CISO Rijk.[18] Dit betekent dat de CPO Rijk functioneel onder de CIO Rijk wordt gepositioneerd. De CPO Rijk is belast met de coördinatie van de maatregelen en het beleid voor de bescherming van de privacy (dan wel persoonsgegevens) voor zover deze betrekking hebben op de rijksoverheid. De huidige coördinatie- en adviesfunctie van de PAR rondom rijksbrede bedrijfsvoeringsvraagstukken vallen in de toekomst ook onder de PAR.

Voor zover noodzakelijk worden voor de CPO Rijk een aantal formele bevoegdheden vastgelegd die de CPO Rijk, in acute gevallen, de mogelijkheid biedt om zich rechtstreeks tot de secretaris-generaal of het verantwoordelijke lijnmanagement van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties te wenden en van informatie te voorzien. Deze maatregel draagt bij aan het waarborgen van de *'checks and balances'* tussen verschillende functionarissen.

Tot slot wordt er rijksbreed nog een CPO-raad ingericht. Deze vervult de functie als voorportaal van het CIO-beraad op het gebied van privacybeleid. Deze raad wordt voorgezeten door de CPO Rijk en alle departementale CPO's zijn leden van deze raad. De CPO-raad richt zich op een (eventueel toekomstig) privacybeleid van de rijksdienst en bespreekt het onderdeel privacy/gegevensbescherming van de meerjarige I-strategie. De CPO-raad vervangt het huidige overleg van privacy officers.

16 Zie hiervoor artikelen 6 tot en met 8 van het CIO-besluit
17 Zie artikel 9 CIO-besluit.
18 Zie hiervoor de artikelen 10, 13 en 14 van het CIO-besluit

Hoe verhoudt dit scenario zich tegenover de uitgangspunten in het toetsingskader?

Uitgangspunt	Toets	Toelichting
Zet privacy hoger op de agenda		Het formaliseren van de rol van CPO (Rijk) in het CIO-stelsel zorgt er vrijwel zeker voor dat het onderwerp actiever op de agenda komt. Het formaliseren van de rol van CPO binnen het CIO-stelsel biedt (kwalitatieve) waarborgen in het kader van taken, verantwoordelijkheden en bevoegdheden. Bovendien wordt ook een duidelijk signaal afgegeven en een extra functionaris aangesteld die kan waarborgen dat interdepartementale vraagstukken op de juiste wijze aangevlogen kunnen worden. Door hierbij gebruik te maken van de kennis en ervaring die al is opgedaan bij het vormgeven van het CIO-stelsel, heeft dit naar ons inzicht de potentie voor een vliegwieleffect.
Bouw voort op bestaande rijksbrede structuren		Het huidige CIO-stelsel bevat al een sterk fundament om een rijksbrede privacy governance in vorm te geven. Zowel de CIO als CISO hebben de afgelopen jaren stappen gezet om het bereik en de invloed te vergroten. Een functie van CPO kan profiteren van de kennis en ervaring die zijn opgedaan door de CIO en CISO Rijk.
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties		Binnen het huidige CIO-stelsel is rekening gehouden met de diversiteit en complexiteit van de diverse departementen en uitvoeringsorganisaties. Zo bestaat er de mogelijkheid om een departementaal CIO-stelsel in te richten als de aard en de complexiteit van de inrichting van het departement en betrokken uitvoeringsorganisatie hierom vraagt. Wel merken we op dat de huidige privacy governance binnen de verschillende ministeries en uitvoeringsorganisaties varieert. Zo hebben niet alle departementen de privacy officers binnen het CIO-office gepositioneerd, we zien ze ook binnen bedrijfsvoering of BOA. Door het opnemen van de rol van CPO in het CIO-stelsel worden ministeries geforceerd de interne governance en het privacybeleid aan te passen.
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model		Het huidige CIO-stelsel is volledig ingericht als tweedelijnsfunctie binnen het 3-LoD model. Door het toevoegen van de rol van CPO aan deze functie, kan ook deze functie volledig binnen deze tweede lijn opereren en daarbij gebruikmaken van de kennis en ervaring die al is opgedaan binnen deze gremia.
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's)		Door een CPO(Rijk)-rol in te richten en dit te formaliseren in een mandaat dat vergelijkbaar is met dat van de CISO Rijk, bestaat er de kans dat beleidsmatige keuzes worden gemaakt die buiten de departementale scope van de FG's om gaat. Dit is in potentie een risico wanneer dit zou leiden tot een beperking van de toezichthoudende functie van de FG's. Zorg er bij de eventuele inrichting van een CPO-stelsel dan ook voor dat de FG's ook toezicht kunnen houden op en advies geven over rijksbrede privacyvraagstukken.
Zorg voor voldoende checks and balances tussen de verschillende functionarissen		Het CIO-stelsel bevat verschillende mechanismen en maatregelen om te waarborgen dat betrokken functionarissen voldoende mandaat hebben om beleid op te stellen en te adviseren rondom de informatievoorziening, en zorgt er tegelijkertijd voor dat er voldoende 'checks and balances' zijn tussen de verschillende functies en bewindslieden. Een nieuw aan te wijzen CPO zou op dezelfde wijze gebruik kunnen maken van deze mechanismen en maatregelen, en zodoende voldoende mandaat krijgen.
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/ worden ingericht, zoals chief privacy officer (CPO)		Zoals eerder beschreven hebben de meeste ministeries en uitvoeringsorganisaties inmiddels een rol van CPO ingericht, of zitten in het proces om een dergelijke rol te formaliseren. Door deze functie in het CIO-stelsel te verankeren, wordt meer eenduidigheid gecreëerd. Ook ten opzichte van andere 'C-level'-rollen wordt aansluiting gezocht. Zo wordt een CPO in het hart van de informatievoorziening gepositioneerd en bovendien dicht tegen de CISO. Dit maakt het ook voor hen makkelijker om samen te werken en de onderwerpen integraal aan te pakken.
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries		Door het inrichten van de rol van CPO binnen het CIO-stelsel naar analogie van de rol van CISO krijgt de CPO formele bevoegdheden en daarmee ook mandaat. Onder leiding van een CPO Rijk kunnen in een CPO-raad onderwerpen worden besproken en beleidskaders worden gevormd die ingebracht worden in bestaande besluitvormingsprocessen, zoals het CIO-beraad.
Zorg voor een integrale aanpak		De inbedding van de rol van CPO binnen het CIO-stelsel biedt veel mogelijkheden voor een integrale aanpak. Zo zorgt de positionering van een CPO binnen het CIO-stelsel ervoor dat de CISO, CPO en (toekomstig) CDO dicht tegen elkaar gepositioneerd zijn en zij eenvoudig met elkaar kunnen afstemmen. Door een CPO-raad in te richten als voorportaal voor het CIO-beraad, op een gelijke wijze als de andere voorportalen, wordt de CIO bovendien in staat gesteld om een afgewogen advies te geven aan lijnmanagement, de SG, staatssecretaris, of minister. Hiermee denken we ook dat voldoende rekening gehouden wordt met het dilemma van: 'Too many chiefs, no indians', dat verlamming van de besluitvorming kan veroorzaken, doordat binnen besluitvormingsprocessen statistisch gezien een van de 'gelijkwaardige' altijd een negatief advies zal geven.

4.3.2 **Scenario 2.** Privacy governance binnen het CIO-stelsel onder de CISO

In scenario 2 worden de taken, verantwoordelijkheden en bevoegdheden rondom privacy belegd in het CISO-stelsel binnen het bestaande CIO-stelsel.

In scenario 2 werken we zo veel mogelijk volgens bestaande principes en modellen, maar kiezen we ervoor om hier geen nieuwe (formele) functie/rol voor in te richten. We passen het huidige CIO-besluit aan en breiden daarbinnen het takenpakket van de CISO uit om ook de bescherming van persoonsgegevens dan wel privacy op een juiste wijze in te richten.

Wat betekent dit voor de departementen?

De belangrijkste wijziging voor de departementen in dit scenario is dat de tweedelijnstaken op het gebied van privacy onder de eindverantwoordelijkheid van de (departementaal) CISO komen te vallen.

In de praktijk zal dit waarschijnlijk leiden tot een situatie waarin een of meerdere privacy officers worden aangewezen om zich onder de CISO te richten op het opstellen en uitwerken van richtlijnen en beleidskaders op het gebied van privacy.

De CISO kan dit vervolgens integraal meenemen in zijn beleidskaders, adviezen en visie richting de CIO, secretaris-generaal en het lijnmanagement.

Wat verandert er rijksbreed?

Ook rijksbreed wordt de rol van CISO aangepast en uitgebreid met de taken, verantwoordelijkheden en bevoegdheden zoals deze zijn beschreven in de profielschets in paragraaf 4.2.2.

In beginsel betekent dit dat de reeds bestaande gremia, zoals de CISO-raad in de toekomst ook worden ingezet om een (toekomstig) privacybeleid van de rijksdienst in te richten en privacy en gegevensbescherming expliciet mee te nemen als onderdeel van de meerjarige I-strategie. De wijze waarop privacy expliciet wordt meegenomen in de CISO-raad valt te bezien. Hier kan gedacht worden aan het laten bestaan van het huidige overleg van privacy officers en een adviserende rol richting de CISO-raad te geven. Hetzelfde geldt voor de PAR-functie voor rijksbrede bedrijfsvoeringsvraagstukken. In de formalisatie van de rollen zien we deze functie ondergebracht worden bij de CISO.

Hoe verhoudt dit scenario zich tegenover de uitgangspunten in het toetsingskader?

Uitgangspunt	Toets	Toelichting
Zet privacy hoger op de agenda		Door taken en bevoegdheden rondom de inrichting van privacy governance te formaliseren onder de rol van CISO, wordt privacy in ieder geval explicieter op de agenda gezet dan momenteel het geval is. Toch vragen we ons af of dit in de praktijk ook het geval zal zijn als deze taken en verantwoordelijkheden bij de CISO worden belegd. Praktisch gezien betekent dit dat een CISO zijn aandacht zal moeten gaan verdelen tussen privacyvraagstukken en informatiebeveiligingsvraagstukken. Digitale weerbaarheid is op zichzelf al een vraagstuk dat uitdagend genoeg is voor CISO's. Dit niet alleen uit het groeiende aantal meldingen van aanvallen en het snel veranderende (internationale) politieke landschap, maar ook uit de stijgende budgetten die worden vrijgemaakt om de digitale weerbaarheid te vergroten. Daarnaast zien we ook een stijgend aantal privacyvraagstukken en zorgvuldig gebruik van persoonsgegevens door de rijksoverheid. Het onderbrengen van beide onderwerpen onder de CISO, leidt in de praktijk naar ons idee dan ook vooral tot vermindering van aandacht voor beide onderwerpen.
Bouw voort op bestaande rijksbrede structuren		Door het borgen van taken en verantwoordelijkheden op het gebied van privacy onder de CISO, wordt er voortgebouwd op bestaande structuren binnen de rijksoverheid. De formalisering van de rollen van CIO en CISO binnen het CIO-stelsel vormen inmiddels een sterk fundament voor de informatievoorziening binnen de rijksoverheid. Door de privacy governance hierop voort te bouwen, kan op dit onderwerp een 'vliegwieleffect' ontstaan. De huidige positionering van de PAR zorgt er bovendien voor dat de lijn met de CISO kort is.
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties		Binnen het huidige CIO-stelsel is expliciet rekening gehouden met de diversiteit en complexiteit van de diverse departementen en uitvoeringsorganisaties. Zo bestaat er de mogelijkheid om een departementaal CIO-stelsel in te richten als de aard en de complexiteit van de inrichting van het departement en betrokken uitvoeringsorganisatie hierom vraagt. Wel merken we op dat ministeries de positie van privacy en informatiebeveiliging geregeld op verschillende plekken binnen de organisatie beleggen. Door het opnemen van de privacytaken bij de CISO worden ministeries geforceerd de interne governance en het privacybeleid aan te passen.

Uitgangspunt	Toets	Toelichting
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model		Het huidige CIO-stelsel is volledig ingericht als tweedelijnsfunctie binnen het 3-LoD model. Door het toevoegen van de taken en bevoegdheden op het gebied van privacy aan deze functie, kunnen ook deze taken volledig binnen deze tweede lijn opereren en daarbij gebruikmaken van de kennis en ervaring die al is opgedaan bij het opbouwen van deze gremia.
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's)		Door het uitbreiden van de rol van CISO (Rijk) op het gebied van privacy, bestaat er de kans dat beleidsmatige keuzes worden gemaakt die buiten de departementale scope van de FG's om gaat. Dit is in potentie een risico wanneer dit zou leiden tot een beperking van de toezichthoudende functie van de FG's. Zorg bij de eventuele inrichting van de privacy governance binnen het CIO-stelsel dan ook dat de FG's ook toezicht kunnen houden op, en advies geven over, rijksbrede privacyvraagstukken.
Zorg voor voldoende checks and balances tussen de verschillende functionarissen		Het CIO-stelsel bevat verschillende mechanismen en maatregelen om te waarborgen dat betrokken functionarissen voldoende mandaat hebben om beleid op te stellen en te adviseren rondom vraagstukken op het gebied van informatiebeveiliging en privacy binnen de informatievoorziening. Het stelsel zorgt er tegelijkertijd voor dat er voldoende 'checks and balances' zijn tussen de verschillende functies en bewindslieden. Door taken en bevoegdheden op het gebied van informatiebeveiliging en privacy in één rol te voegen, ontstaan er risico's dat er onvoldoende checks and balances tussen beleid en maatregelen rondom informatiebeveiliging en privacy blijven. We kunnen ons voorstellen dat er diverse situaties zijn waarbij de belangen die worden nagestreefd vanuit informatiebeveiligingsperspectief anders zijn dan die van de bescherming van persoonsgegevens. Een goed voorbeeld hiervan is de informatieverstrekking aan betrokkenen/burgers bij een groot datalek, waarbij vanuit IB een belang kan bestaan om informatie niet te delen, terwijl dit vanuit gegevensbescherming juist wel gedaan moet worden. Een ander voorbeeld kan zijn het verzamelen van (logging)gegevens, waarbij vanuit IB een belang bestaat om logginggegevens te verzamelen en voor langere tijd te bewaren, terwijl dit vanuit de bescherming van persoonsgegevens niet te rechtvaardigen is.
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/worden ingericht, zoals chief privacy officer (CPO)		Zoals eerder beschreven hebben de meeste ministeries en uitvoeringsorganisaties inmiddels een rol van CPO ingericht, of zitten in het proces om een dergelijke rol te formaliseren. Hoewel meerdere privacy officers of andere functionarissen ook onder de CISO kunnen worden aangesteld, vinden we het onlogisch om een CPO onder een CISO te positioneren. De functie zou voor wat betreft takenpakket weliswaar niet veel hoeven af te wijken van een CPO-takenpakket, maar realistisch gezien wordt een dergelijke functie dan toch minder zwaar ingericht. De bevoegdheden en verantwoordelijkheden zullen dan toch minder zwaar worden vormgegeven. Het betekent ook dat de reeds gepositioneerde CISO's hun kennis en kunde moeten uitbreiden op het gebied van privacy om deze rol waar te kunnen maken. Het is lastig om de specialistische kennis die nodig is om een dergelijke functie inhoudelijk goed uit te kunnen voeren op zowel privacy als informatiebeveiliging in één persoon te vinden.
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries		Het expliciteren van taken, verantwoordelijkheden en bevoegdheden onder de CISO zal bijdragen aan een breder mandaat vanuit de ministeries.
Zorg voor een integrale aanpak		Het integreren van taken, verantwoordelijkheden en bevoegdheden binnen de rol van de CISO in het CIO-stelsel draagt bij aan een integrale aanpak. Adviezen rondom informatiebeveiliging en privacy kunnen al afgewogen worden door de CISO (of CISO-raad) voorafgaand aan het delen met de CIO (of CIO-beraad).

4.3.3 **Scenario 3.** Privacy governance onder CDO binnen CIO-stelsel

In scenario 3 beleggen we de taken, verantwoordelijkheden en bevoegdheden rondom privacy in het (toekomstige) CDO-stelsel als onderdeel van het CIO-stelsel.

In dit scenario worden de taken en verantwoordelijkheden van de tweedelijnsprivacyfunctie(s) opgenomen en geïntegreerd in het CDO-stelsel als onderdeel van het CIO-stelsel. Het CDO-stelsel wordt momenteel nog vormgegeven. De impact die dit zal hebben voor de departementen is op dit moment dan ook lastig in te schatten.

Wat betekent dit voor de departementen?

Het meest voor de hand liggende gevolg voor ministeries is allereerst dat zij verplicht zullen worden om een CDO aan te stellen. Deze CDO zal in dit scenario over een zeer breed takenpakket beschikken, dat zich in één zin het best laat omschrijven als: *de aanjager van datagedreven werken met als doel het vergroten van de creatie van publieke waarde.*

Departementen zullen er in dit geval dan ook rekening mee moeten houden dat de CDO in staat is om een integraal beeld te vormen van de risico's en kansen die het gebruik van data met zich meebrengen en daarin een zorgvuldige belangenafweging moeten maken.

In de praktijk zal dit logischerwijs leiden tot het positioneren van één of meerdere privacy officers onder de verantwoordelijkheid van de CDO.

Wat verandert er rijksbreed?

Ook rijksbreed zullen de taken, verantwoordelijkheden en bevoegdheden die wij hebben opgenomen in de profielschets onder de verantwoordelijkheid van de CDO (Rijk) komen te vallen.

Daarnaast zien we voor ons dat ook te verwachten gremia, zoals een CDO-raad als voorportaal van het CIO-beraad, zodanig worden ingericht dat onderwerpen op het gebied van privacy worden meegenomen in deze overlegstructuren.

Hoe verhoudt dit scenario zich tegenover de uitgangspunten in het toetsingskader?

Uitgangspunt	Toets	Toelichting
Zet privacy hoger op de agenda		Uit de interviews met verschillende (kwartiermaker) CDO's kwam naar voren dat zij momenteel nog in een vroege fase van de inrichting van hun rol zitten. Uit de interviews hebben we dan ook geen eenduidig beeld gekregen van de wijze waarop zij hun rol vervullen en hoe zij zich verhouden tot andere rollen, zoals bijvoorbeeld een CIO, CISO, (C)PO of FG. Ze beschikken zelf ook niet over de juiste kennis en kunde op dit vlak. Door in deze vroege fase al taken en verantwoordelijkheden op het gebied van privacy onder te brengen bij de CDO, geeft (grote) risico's op dit gebied.
Bouw voort op bestaande rijksbrede structuren		De rol van CDO is momenteel nog niet formeel ingericht binnen alle departementen en het CIO-stelsel. Hoewel men van plan is om de rol van CDO te borgen binnen een CDO-stelsel (als onderdeel van het CIO-stelsel) is dit nog geen vaststaand feit. Door privacy binnen CDO te borgen, gaan we een nieuwe positionering binnen een vernieuwing, anders gezegd, nog niet bestaande structuur, aanbrengen. Hierdoor ontstaan dermate grote onzekerheden, dat we dit als een voor nu niet geschikte situatie beschouwen.
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties		Binnen het huidige CIO-stelsel is expliciet rekening gehouden met de diversiteit en complexiteit van de diverse departementen en uitvoeringsorganisaties. Zo bestaat er de mogelijkheid om een departementaal CIO-stelsel in te richten als de aard en de complexiteit van de inrichting van het departement en betrokken uitvoeringsorganisatie hierom vraagt. Ervan uitgaande dat dit ook het geval zal zijn bij het inrichten en vormgeven van het CDO-stelsel, voorzien we hier geen problemen in. Wel merken we op dat de huidige privacy governance binnen de verschillende ministeries en uitvoerings-organisaties varieert. Zo hebben niet alle departementen de privacy officers binnen het CIO-office gepositioneerd, maar bijvoorbeeld binnen bedrijfsvoering of BOA. Door het opnemen van de privacytaken in het CDO-stelsel, worden ministeries geforceerd de interne governance en het privacybeleid aan te passen.
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model		Het huidige CIO-stelsel is volledig ingericht als tweedelijnsfunctie binnen het 3-LoD model. Door het toevoegen van de rol van CDO aan deze functie, kan ook deze functie volledig binnen deze tweede lijn opereren en daarbij gebruikmaken van de kennis en ervaring die al is opgedaan bij het opbouwen van deze gremia.

Uitgangspunt	Toets	Toelichting
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's)		Door privacy onder te brengen bij de CDO en dit te formaliseren in een mandaat dat vergelijkbaar is met dat van de CISO (Rijk), bestaat er de kans dat beleidsmatige keuzes worden gemaakt die buiten de departementale scope van de FG's om gaat. Dit is in potentie een risico wanneer dit leidt tot een beperking van de toezichthoudende functie van de FG's. Zorg bij de inrichting van rijksbrede privacy governance er dan ook voor dat de FG's ook toezicht kunnen houden op, en advies geven over, rijksbrede privacyvraagstukken.
Zorg voor voldoende checks and balances tussen de verschillende functionarissen		Het CIO-stelsel bevat verschillende mechanismen en maatregelen om te waarborgen dat betrokken functionarissen voldoende mandaat hebben om beleid op te stellen en te adviseren rondom vraagstukken op het gebied van informatiebeveiliging en privacy binnen de informatievoorziening. Het stelsel zorgt er tegelijkertijd voor dat er voldoende 'checks and balances' zijn tussen de verschillende functies en bewindslieden. Echter, doordat taken en bevoegdheden van de beoogd CDO en tweedelijnsprivacyfunctie in één rol worden gevoegd, ontstaan er risico's dat er onvoldoende 'checks and balances' tussen beleid en maatregelen rondom de CDO en privacyfunctie zijn. Momenteel zien we dat bij de invulling van de rol van CDO's veel belangen worden nagestreefd die potentieel op gespannen voet staan bij het waarborgen van een goede omgang met persoonsgegevens. De meerderheid van de (kwartiermaker) CDO's benoemden dit allemaal ook expliciet gedurende de interviews. Daarbij spraken zij ook expliciet de behoefte uit om op dit onderdeel voldoende tegenmacht te ontvangen, om een zorgvuldige omgang met persoonsgegevens te waarborgen. Bij het integreren van privacy binnen het CDO-stelsel ontbreekt deze formele tegenmacht die bij het positioneren van een CPO op gelijke voet wel aanwezig is. In geval van het laatste geldt immers dat op niveau van de CIO bij tegenstrijdige belangen een besluit genomen wordt, waardoor de 'machten' in balans blijven en de uiteindelijke integrale aanpak gewaarborgd blijft. We zijn van mening dat de CDO, in deze vroege fase van het vormgeven van de rol, onvoldoende in staat is om deze zorgvuldige afweging zelfstandig te maken.
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/worden ingericht, zoals chief privacy officer (CPO)		Tijdens de quickscan zijn we geen enkele departement of uitvoeringsorganisatie tegengekomen die de privacy governance volledig heeft geïntegreerd in de CDO-rol. Sterker nog, ook de CDO's zelf zien weinig draagvlak voor deze oplossing. Zo zijn zij bang onvoldoende in staat te zijn om de belangen op het gebied van digitale transformatie na te streven indien zij ook (deels) verantwoordelijkheid dragen voor het borgen van de privacy binnen de organisatie.
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries		Door taken en verantwoordelijkheden op het gebied van privacy governance te expliciteren in de rol van CDO, zal een breder mandaat worden gecreëerd dan momenteel het geval is. Daarbij gaan we ervan uit dat de borging van de rol van CDO plaatsvindt naar analogie van de rol van CISO.
Zorg voor een integrale aanpak		Het integreren van taken, verantwoordelijkheden en bevoegdheden binnen de rol van de CDO in het CIO-stelsel draagt niet bij aan een integrale aanpak. Door privacy onder de verantwoordelijkheid van een CDO te plaatsen, zal deze al een belangenafweging kunnen maken ten aanzien van vraagstukken die zowel de digitale transformatie als privacy raken, zonder dat hier tevens integraal informatiebeveiliging in meegenomen wordt. Hierdoor ontstaat in onze optiek dan ook een risico dat juist de CIO (of CIO-beraad) onvoldoende in staat is om een integraal advies uit te brengen.

4.3.4 **Scenario 4.** Geen wijzigingen privacy governance

In scenario 4 gaan we uit dat er niets wordt veranderd ten opzichte van de huidige (rijksbrede) privacy governance.

In dit scenario blijven de departementen zelfstandig verantwoordelijk voor het inrichten van een privacy governance. Bestaande (informele) overlegstructuren, zoals de PO-raad blijven hetzelfde.

De scope van de PAR blijft formeel beperkt tot advisering rondom rijksbrede thema's op het gebied van bedrijfsvoering en adviseur van de GOR.

Wat betekent dit voor de departementen?

In beginsel betekent dit uiteraard dat er voor de departementen niets verandert. Tegelijkertijd merken we wel dat er binnen diverse departementen de behoefte bestaat om meer samen te werken.

Als men er dus voor kiest om rijksbreed geen wijzigingen door te voeren, dan kan men er alsnog voor kiezen om binnen bestaande structuren te zoeken naar oplossingen om rijksbrede privacyonderwerpen beter integraal aan te sturen.

Wat verandert er rijksbreed?

Dit betekent dat er rijksbreed in principe dus geen wijzigingen worden doorgevoerd. Het mandaat van de PAR voor advisering en kennisdeling blijft gelijk en de PO-raad zal hetzelfde informele karakter behouden.

Hoe verhoudt dit scenario zich tegenover de uitgangspunten in het toetsingskader?

Uitgangspunt	Toets	Toelichting
Zet privacy hoger op de agenda		Door geen enkele wijziging door te voeren in het inrichten van de rijksbrede privacy governance, is het lastig te voorspellen of het waarborgen van privacy actiever op de agenda wordt gezet, maar wordt het niet waarschijnlijk geacht dat privacy actiever op de agenda komt. De huidige inrichting van het CIO-stelsel biedt weliswaar al (beperkte) mogelijkheden om hier invloed op uit te oefenen, maar toch lijkt een duidelijk expliciet mandaat te ontbreken. Uit de interviews met de privacy officers en andere medewerkers, maar ook uit stukken zoals de I-strategie, Kamerbrieven en moties komt naar voren dat er een behoefte is aan (meer) prioriteit aan het borgen van privacy.
Bouw voort op bestaande rijksbrede structuren		Momenteel zijn er geen interdepartementale structuren waarop voortgebouwd kan worden. Ieder departement maakt een eigen afweging rondom het inrichten van een privacy governance.
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties		De huidige inrichting biedt volledige vrijheid aan de departementen om de privacy governance in te richten.
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model		Momenteel is er geen rijksbrede tweedelijns privacy governance ingericht. Desalniettemin werken alle departementen zelfstandig volgens eenzelfde structuur. Wel merken we op dat hier rijksbreed dus geen invloed op uitgeoefend kan worden in dit scenario.
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's)		Doordat in dit scenario geen rijksbrede privacy governance is ingericht, is de invloed vanuit de rijksoverheid zeer beperkt. Er verandert hiermee dus niets aan de huidige situatie. Dit betekent overigens niet dat daarmee de verhoudingen tussen FG's en (C)PO's altijd op de juiste manier ingericht zijn.

Uitgangspunt	Toets	Toelichting
Zorg voor voldoende checks and balances tussen de verschillende functionarissen		Uit de interviews kwam naar voren dat binnen een aantal departementen en uitvoeringsorganisaties de FG niet altijd het gevoel heeft zijn taken uit te kunnen voeren naar de letter van de wet. Redenen die hiervoor werden gegeven waren bijvoorbeeld een onvoldoende sterke informatiepositie om tijdig geïnformeerd te worden over zaken die naar het inzicht van de FG prioriteit verdienen. Of dat de functiescheiding tweede lijn versus derde lijn onvoldoende kon worden bewaakt, bijvoorbeeld vanwege onderbezetting. Bovendien hebben niet alle departementen de tweedelijnsfunctie op dezelfde wijze ingericht, waardoor kennis, ervaring en kwaliteiten uiteenlopen. Hierdoor ziet men dat ook in relatie tot bijvoorbeeld een CISO in de praktijk onvoldoende checks and balances bestaan.
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/worden ingericht, zoals chief privacy officer (CPO)		In dit scenario kunnen we geen toets uitvoeren op dit aspect omdat dit niet aan de orde komt.
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries		Een van de meest gedeelde zorgen tijdens de interviews is dat men graag meer rijksbreed zou willen samenwerken, maar dat dit momenteel onvoldoende mogelijk is vanwege een gebrek aan mandaat.
Zorg voor een integrale aanpak		Vanuit het perspectief van de rijksoverheid kiest men in dit scenario niet voor een integrale aanpak en kan men hier, behoudens door middel van informele adviezen, niet op sturen. Uiteraard zijn de departementen vrij om binnen het eigen departement een integrale aanpak te kiezen.

4.3.5 **Scenario 5.** Privacy governance in afzonderlijk CPO-stelsel

Het laatste scenario beschrijft de situatie waarin een volledig (onafhankelijk) stelsel wordt ingericht waarin privacy governance wordt opgenomen.

In dit scenario wordt in het geheel afgeweken van bestaande modellen en organisatiestructuren binnen de rijksoverheid. In plaats daarvan wordt een geheel nieuw stelsel vormgegeven, waarin de privacy governance wordt vastgelegd en waaraan departementen vervolgens gebonden zijn.

We gaan er in dit scenario vanuit dat men zich bij de ontwikkeling van dit stelsel enkel en alleen richt op het vormgeven van een privacy governance en hiermee dus geen rekening gehouden hoeft te worden met andere stelsels.

Wat betekent dit voor de departementen?

We voorzien bij de uitwerking van dit scenario de volgende elementen:

Departementen worden verplicht om een CPO aan te stellen en deze taken, verantwoordelijkheden en bevoegdheden toe te kennen zoals we deze hebben beschreven in de profielschets.

De positionering van de CPO binnen de departementen wordt vrijgelaten aan de ministeries. Het CPO-stelsel wordt, evenals het CIO-stelsel, zo ingericht dat ministeries ook een departementaal CPO-stelsel kunnen inrichten voor bepaalde dienstonderdelen.

De CPO's hebben dan ook een eigen verantwoordingslijn. Hierin voorzien we twee varianten. Ofwel departementen krijgen de vrijheid om zelf te bepalen aan wie de CPO rapporteert. Of men besluit om in het CPO-stelsel op te nemen dat de CPO rechtstreeks aan de secretaris-generaal rapporteert (of in uitzonderlijke situaties zelfs de minister).

Wat verandert er rijksbreed?

Ook in dit scenario stellen we voor dat er een CPO Rijk wordt aangesteld die verantwoordelijk is voor de coördinatie van maatregelen en beleid inzake de bescherming van persoonsgegevens/privacy.

In dit scenario zal de CPO Rijk voorzitter zijn van een in te richten CPO-beraad, waarin de departementale CPO's als lid deelnemen en waarin besluiten kunnen worden genomen rondom het definiëren van rijksbrede beleidskaders, richtlijnen en adviezen (in lijn met de I-strategie).

Hoe verhoudt dit scenario zich tegenover de uitgangspunten in het toetsingskader?

Uitgangspunt	Toets	Toelichting
Zet privacy hoger op de agenda		Door het inrichten van een afzonderlijk en onafhankelijk stelsel, komt privacy in de toekomst absoluut hoger op de agenda te staan. Echter, realistisch gezien denken we dat het vormgeven van een afzonderlijk (los van het CIO-stelsel) opererend CPO-stelsel een veel langere aanlooptijd zal kennen dan verschillende andere scenario's. We voorzien dan ook dat bij een keuze voor dit scenario, privacy weliswaar actiever op de agenda komt te staan, maar dat de doorlooptijd dusdanig lang is dat dit op korte/middellange termijn geen effectieve oplossing zal zijn.
Bouw voort op bestaande structuren		In dit scenario zal een volledig nieuw stelsel ingericht moeten worden. Hierbij dient niet alleen een volledig nieuwe structuur rondom privacy governance gebouwd te worden, maar zal ook moeten worden nagedacht over de wijze waarop deze zich verhoudt ten aanzien van bestaande structuren, zoals het CIO-stelsel en CISO-stelsel.
Houd voldoende rekening met de diversiteit van de verschillende departementen en organisaties		Evenals de keuze om de privacy governance in te bedden binnen het huidige CIO-stelsel, zal ook de inrichting van een afzonderlijk stelsel bepaalde beperkingen met zich meebrengen ten aanzien van de autonomie van departementen en uitvoeringsorganisaties om een eigen structuur in te richten. Desalniettemin denken we dat dit geen beperking hoeft te zien in de praktijk mits men de juiste maatregelen neemt, door lering te trekken uit eerdere trajecten, zoals bijvoorbeeld de inrichting van het CISO-stelsel.
Richt je bij het inrichten van privacy governance binnen de rijksoverheid op de tweede lijn volgens het 3-LoD model		Bij de inrichting van een afzonderlijk CPO-stelsel is voldoende ruimte om rekening te houden met het 3-LoD model. We voorzien dan ook geen problemen op dit vlak bij een keuze voor dit scenario.

Uitgangspunt	Toets	Toelichting
Voorkom dat de inrichting van een (rijksbrede) privacy governance in de tweede lijn leidt tot het buitenspel zetten van de derde lijn (FG's)		Ook bij dit scenario is het van belang om expliciet rekening te houden met de interdepartementale besluitvormingsprocessen enerzijds en de departementale scope van FG's anderzijds.
Zorg voor voldoende checks and balances tussen de verschillende functionarissen		In dit scenario zien we verschillende (potentiële) risico's in het kader van het waarborgen van de juiste 'checks and balances'. Om deze op de juiste manier te borgen is het van belang dat goed wordt nagedacht over de verhouding tussen alle verschillende taken, verantwoordelijkheden en bevoegdheden van rollen en functies rondom de informatievoorziening. Een keuze voor dit scenario is een keuze om bewust af te wijken van hetgeen momenteel is vastgelegd in het CIO-besluit en de structuren die daarin worden gevolgd. Hierbij loopt men het risico om juist ten opzichte van functies en rollen als de CISO en de CDO een ongelijk speelveld te creëren. NB Overigens hebben we tijdens de interviews ook geen concrete ideeën of opvattingen gehoord die een meer concrete invulling aan deze visie geven.
Zoek aansluiting bij functies die momenteel binnen de meeste organisaties zijn/worden ingericht, zoals chief privacy officer (CPO)		Dit scenario biedt voldoende mogelijkheden om aan te sluiten bij functies en rollen die al binnen veel departementen en uitvoeringsorganisaties worden ingericht. Doordat men niet verbonden is aan bestaande stelsels, heeft men hier in theorie zelfs volledige vrijheid in.
Zorg bij de inrichting van een rijksbrede privacy governance voor voldoende mandaat vanuit de ministeries		Dit scenario biedt veel vrijheid om een breed mandaat in te richten vanuit de verschillende departementen en uitvoeringsorganisaties. Doordat men bovendien niet gebonden is aan het mandaat beschreven in het CIO-stelsel, kan men er zelfs voor kiezen om dit mandaat nog uitgebreider vorm te geven. NB We vragen ons wel af of er vanuit de departementen wel behoefte is aan een (nog) omvangrijker mandaat dan waar momenteel al voor gekozen wordt binnen het huidige CIO-besluit.
Zorg voor een integrale aanpak		Door privacy governance geheel los te koppelen van aangrenzende rollen en functie, zoals bijvoorbeeld CIO, CISO en CDO, wordt verkokering versterkt ten koste van een integrale aanpak.

HOOFDSTUK 5

Conclusies en aanbevelingen

In dit hoofdstuk leggen we uit welk scenario wij het meest passend vinden voor de inrichting van de rijksbrede privacy governance en onderbouwen we deze keuze. In de aanbevelingen geven we enkele adviezen voor de verdere uitwerking van dit scenario, inclusief een stappenplan op hoofdlijnen.

5.1 Conclusie

We zien een brede behoefte vanuit maatschappij, politiek en de departementen om meer focus te leggen op het krijgen van meer grip op risico's gerelateerd aan de bescherming van persoonsgegevens. De exponentiële groei aan informatiesystemen, -processen en -voorzieningen hebben geleid tot een (zeer) complex landschap. Bovendien zien we ook dat wet- en regelgeving op dit vlak steeds complexer wordt en gespecialiseerde kennis vereist van privacyfunctionarissen. Dit beeld wordt ook bevestigd in de interviews. Zo zien we dat een meerderheid van de departementen bezig is met een herziening van het privacybeleid en de formalisering van de rol van CPO. Bovendien zien we vanuit de departementen een behoefte om samenwerking op specifieke departement overstijgende vraagstukken te intensiveren (zoals bij stelselvraagstukken).

Momenteel vindt interdepartementale samenwerking op het vlak van privacy nog onvoldoende plaats. Het CIO-stelsel heeft de afgelopen jaren een belangrijke rol gespeeld in het coördineren en waarborgen van een integrale aanpak gericht op de digitale transformatie binnen de rijksoverheid. In deze integrale aanpak spelen de departementale CIO's en CISO's, respectievelijk CIO Rijk en CISO Rijk, een belangrijke rol. Sterker nog, uit de toelichting bij het CIO-besluit blijkt dat men ook de mitigatie van privacyrisico's als onderdeel ziet van deze integrale aanpak. Toch zien we dat taken en verantwoordelijkheden rondom het waarborgen van een goede bescherming van persoonsgegevens momenteel niet expliciet zijn beschreven in het CIO-besluit. Het gevolg is dat er geen (eenduidig/gecentraliseerd) mandaat bestaat voor de huidige (C)PO's binnen de verschillende departementen en dienstonderdelen voor het bepalen van rijksbrede kaders, adviezen en plannen op het gebied van privacy.

Op basis van het voorgaande komen we tot drie belangrijke conclusies. Allereerst zien we dat een tweedelijnsprivacyfunctie inmiddels is uitgegroeid tot een volwaardige functie binnen de departementen. Daarnaast zien we verschillende interdepartementale vraagstukken op het gebied van privacy, waarvoor een rijksbrede aanpak noodzakelijk dan wel wenselijk is. Tot slot zien we dat het huidige CIO-besluit in de Nota van Toelichting al ruimte biedt om ook op het gebied van privacy taken en verantwoordelijkheden te beleggen. Dit past logischerwijs ook binnen het beoogde doel van het CIO-besluit, namelijk een integrale aanpak rondom verdere digitalisering.

Op basis van bovenstaande conclusies adviseren we dan ook om bij de verdere rijksbrede inrichting van privacy governance te kiezen voor het inrichten van een CPO-stelsel binnen het CIO-stelsel (scenario 1). Door voor deze oplossing te kiezen, bouwt men voort op de eerder gekozen strategie voor een integrale aanpak rondom verdere digitalisering binnen de rijksoverheid. De ontwikkeling van een CPO-stelsel binnen het CIO-stelsel zorgt ervoor dat samenwerking met andere functies binnen het CIO-office wordt geïntensiveerd en dat er bovendien een helder mandaat gecreëerd wordt om rijksbrede kaders te stellen, beleid op te stellen en adviezen te geven. Bovendien kan men op deze wijze effectiever en efficiënter een risicobeeld vormen en bepalen welke maatregelen noodzakelijk zijn.

We raden het af om privacy in te bedden in een andere bestaande functie, zoals de CISO (scenario 2), of de in te richten functie CDO (scenario 3). Zoals in het voorgaande punt al beschreven, beschouwen we de taken en verantwoordelijkheden op het gebied van privacy als een volwaardige functie, die specifieke kennis en vaardigheden vereisen. Recente incidenten en problemen laten ook zien dat de rijksoverheid voor diverse uitdagingen staat op dit vlak en dat veel departementen nog ver staan van een volwassen inrichting van de organisatie. Het onderbrengen van de privacyfunctie onder CISO of CDO leidt in onze ogen tot onvoldoende (specifieke) aandacht voor het onderwerp privacy. Daarnaast denken we dat de uitoefening van taken en verantwoordelijkheden in het kader van privacy in de praktijk niet altijd verenigbaar zijn met de taken en verantwoordelijkheden van een CISO, respectievelijk een CDO. Wanneer men niets verandert aan de huidige privacy governance (scenario 4), dan vermoeden we dat de privacyvraagstukken onvoldoende sterk aan bod komen. Tot slot vinden we dat het CIO-office het hart vormt van de Nederlandse informatievoorziening. Om risico's en vraagstukken integraal te kunnen benaderen, is het wat ons betreft een logische stap om de CPO dan ook in het CIO-office te plaatsen. Bovendien kan in dit geval de kennis en ervaring die is opgedaan tijdens de positionering van de CISO dan ook worden toegepast bij de positionering. Hierdoor achten we scenario 5 dan ook niet het meest voor de hand liggende scenario.

Bij het uitwerken en inrichtingen van het scenario hebben we nog een aantal aanbevelingen geformuleerd. Deze aanbevelingen werken we uit in de volgende paragraaf.

5.2 Aanbevelingen

5.2.1 Wijze van implementatie

De inrichting van het huidige CIO-stelsel en daarbinnen het CISO-stelsel is niet van de een op de andere dag gerealiseerd. Dit zal ook zo zijn voor de inrichting van een CPO-stelsel. We raden dan ook aan om gebruik te maken van de lessen die geleerd zijn bij deze eerdere ontwikkelingen.

Op hoofdlijnen adviseren wij een stapsgewijze aanpak naar een volgroeid CPO-stelsel. Hierbij moet er eerst een CPO binnen elk departement zijn. Het is van belang dat, op hoofdlijnen, duidelijk is welk profiel nodig is voor de taken, verantwoordelijkheden en bevoegdheden die naar alle waarschijnlijkheid belegd gaan worden binnen deze functie. Hiermee kunnen departementen de doorgroei naar de gewenste CPO-functie in gang zetten. In elk geval moet expliciet worden aangesloten op het three lines of defense model en dient gericht te worden op de tweedelijnsfunctie voor privacy. Naast het in kaart brengen van de CPO-functie dient tevens geduid te worden hoe de relatie met andere IV-gerelateerde functies, alsook de FG, is.

Vervolgens kan gestart worden met het voorbereiden op een aanpassing van het Besluit CIO-stelsel Rijksdienst 2021. We adviseren hier om de functie CPO (Rijk) naar analogie van de CISO in te richten, omdat we zien dat de tweedelijnsfunctie voor informatiebeveiliging en privacy in elkaars verlengde liggen en zich op dezelfde wijze tot de CIO verhouden. De herkenbaarheid van de beschrijving helpt bij het creëren van het benodigde draagvlak. Ditzelfde geldt voor de wijze waarop de CPO-raad geformaliseerd wordt.

In deze periode van voorbereiding van de formalisatie, adviseren we het huidige privacy officersoverleg in stand te houden. Nieuw aangestelde CPO's (indien afwijkend van huidige CPO's) worden toegevoegd aan het overleg. Naarmate meer zekerheid wordt verkregen over de vaststelling van de CPO-functie, waarin ook de CPO-raad als voorportaal van het CIO-beraad gaat functioneren, raden we aan om de CPO-raad vast in stelling te brengen voor advisering van het CIO-beraad.

Vervolgens dient een CPO Rijk aangesteld te worden. Deze wordt de voorzitter van de CPO-raad. De CPO Rijk zal de huidige privacyadviseurs, gepositioneerd in team IB&P, onder zijn of haar aansturing krijgen. Mogelijkerwijs is een versterking nodig om de tweedelijnsfunctie volwaardig in te vullen.

We adviseren tevens het CPO-stelsel circa twee à drie jaar na formele instelling te evalueren.

5.2.2 Zorg voor een sterke positie van de FG

De FG is, en blijft, een departementale derdelijnsfunctie. Een versterking van de tweedelijnsfunctie rijksbreed mag niet leiden tot een beperking van de toezichthoudende (wettelijk bepaalde) functie van de FG. De scheiding tussen de tweedelijns en derdelijns zien we als zeer belangrijk.

Er is op dit moment een rijksbreed overleg van FG's. Dit is informeel geregeld en daar zouden we op korte termijn geen wijziging in aanbrengen. Wel vinden we dat de bevoegdheid van de FG's om in te grijpen bij rijksbrede kaderstelling van de tweedelijns CPO's geborgd dient te zijn. Derhalve lijkt het ons verstandig om de adviserende rol van de FG's in de toekomst richting CPO-raad in elk geval te borgen binnen het Besluit CIO-stelsel Rijksdienst. Hiermee wordt tevens de positie van de FG versterkt met de inrichting van het CPO-stelsel. We adviseren om bij het inrichten van deze rijksbrede derdelijnsadviesrol van de FG's, hen actief te betrekken om zowel op proces als inhoud afspraken te maken. Hiermee versterk je het draagvlak onder de FG's en voorkom je dat rijksbrede besluitvorming wordt vertraagd door inefficiëntie in de communicatie tussen CPO's en FG's. Trek daarbij lessen uit de ervaringen die zijn opgedaan door de PAR.

5.2.3 Toekomstige integratie CDO en privacy

De CDO-rol is bij het opstellen van deze rapportage nog volop in ontwikkeling. Dit betekent ook dat de taken, bevoegdheden en verantwoordelijkheden van deze rol nog niet volledig zijn uitgewerkt. Op dit moment zien we bij geen van de CDO's die we gesproken hebben dat de privacy governance geïntegreerd is met de CDO-rol en is hier ook geen draagvlak voor. Duidelijk is wel dat bij het aanjagen van een datagedreven overheid, privacy een grote rol speelt bij het voldoen aan wet- en regelgeving.

In paragraaf 5.2.1 adviseren we het CPO-stelsel twee à drie jaar na instelling te evalueren. De CDO-rol is op dat moment waarschijnlijk verder ontwikkeld. Dat zou daarmee een goed moment zijn om ook te bekijken of er wijzigingen mogelijk zijn die het gehele CIO-stelsel kunnen versterken.

De focus van de CDO op het gebruik van data binnen de rijksoverheid, vereist veel kennis op het gebied van privacy-by-design, dataminimalisatie en andere relevante concepten. Een CDO kan een belangrijke rol spelen in de uitwerking hiervan en het identificeren en mitigeren van risico's op dit vlak. Een nadere integratie op deze onderwerpen biedt in potentie mooie kansen voor een verdere integrale aanpak binnen het CIO-stelsel. Ook kan dan goed bekeken worden welke taken in elk geval niet passen bij het CDO-stelsel, waarbij we in elk geval verwachten dat zaken als het afhandelen van datalekken en het behandelen van verzoeken van betrokkenen ook in de toekomst niet passend zijn bij de CDO-rol.

5.2.4 Geef ruimte voor departementale inrichting

Er zijn veel verschillen tussen de departementen, niet alleen wat taken en verantwoordelijkheden betreft, maar ook qua governance. Een meer centrale of decentrale inrichting heeft invloed, net als het hebben van veel en grote uitvoeringsorganisaties. Ook zit er verschil in de uitdagingen op het vlak van privacy. Dit vraagt om een andere focus qua taken vanwege de aard van de informatiehuishouding en een andere inrichting passend bij de wijze waarop het departement is ingericht. Uit de interviews komt naar voren dat men het belangrijk vindt om ruimte te hebben voor departementale bijzonderheden en is men angstig voor een te grote focus op een eenduidige inrichting.

Het besluit CIO-stelsel stelt een aantal eisen aan de inrichting en positionering van de CIO, zoals een rechtstreekse lijn met de SG, lid zijn van de bestuursraad en het inrichten van een CIO-office. Een CISO dient onder de CIO geplaatst te worden. Uit de nulmeting van het CIO-stelsel van de Auditdienst Rijk komt naar voren dat het CIO-besluit ruimte biedt voor verscheidenheid in implementatie: *'Het 'wat' wordt gedefinieerd. Het 'hoe' (lees: de implementatie) wordt aan de departementen overgelaten.'*

In de uitwerking van het voorkeursscenario moet daarom ruimte worden overgelaten voor een departementale inrichting, zoals ook voor de CIO en CISO geldt. De CPO hoort bijvoorbeeld thuis in het CIO-office onder de CIO, maar er is ruimte voor een nadere invulling om rekening te houden met de eisen van het specifieke departement. Hierbij moet uiteraard wel worden gekeken naar eventuele waarborgen en functiescheiding.

5.2.5 Kennis en capaciteit beter versterken rijksbreed

Bij een aantal interviews komt naar voren dat het gebrek aan kennis en capaciteit binnen de departementen een belangrijke drempel is voor het kwalitatief inrichten van een privacystelsel en in meer algemene zin het groeien in volwassenheid op het gebied van privacy binnen departementen. Daarnaast helpt het ontwikkelen van privacykennis voor alle medewerkers om het thema beter te begrijpen. We adviseren om de functie van privacy officer op te nemen in het functiehuis van de rijksoverheid en daarbij de kwalitatieve eisen vast te stellen.

Het is momenteel moeilijk om goede privacyprofessionals te werven (zie ook I-strategie hoofdstuk 7 over het *'opbouwen toekomstbestendig I-vakmanschap'*), en daarmee is het belangrijk om de beperkte capaciteit slim in te zetten binnen de gehele rijksoverheid. We adviseren om gelijktijdig met het inrichten van de privacy governance ook in te zetten op versterking van de kennis en capaciteit op het gebied van privacy rijksbreed. Een tweetal suggesties die we hierbij doen om te investeren op samenwerking en efficiënte inzet van aanwezige capaciteit:

- **Inrichting flexibele schil**
  We hoorden in de interviews dat departementen met soortgelijke privacyissues worstelen. Bij vraagstukken die bij of over meerdere departementen heen spelen, kan het zinvol zijn om op basis van een specifiek vraagstuk inzet van een kundig privacy officer op dat vlak bij meerdere departementen te organiseren. Hierbij wordt de gedachte van privacy officers puur voor het eigen departement deels loslaten en wordt een flexibele schil over de departementen heen georganiseerd die efficiëntie oplevert.

- **Inrichting thematische werkgroepen**
  In plaats van bovenstaande of naast bovenstaande kan het helpen om werkgroepen op basis van specifieke thema's in te richten. Denk hierbij aan een specifieke werkgroep voor geautomatiseerde besluitvorming, een werkgroep voor AI-toepassingen, datatransfers, etc. Dit zijn behoorlijk specialistische onderwerpen en door de krachten te bundelen wordt voorkomen dat men het wiel opnieuw dient uit te vinden.

HOOFDSTUK 6

Verantwoording

6.1 Aanpak

Het onderzoek is uitgevoerd tussen juni 2022 en augustus 2022 en bestond uit drie stappen:

1. ***Quickscan huidige privacy governance***, waarin we de huidige situatie in kaart hebben gebracht door middel van interviews en een documentstudie.
2. ***Inventariseren en beschrijven alternatieven***, waarin we voor elk alternatief in kaart hebben gebracht wat de taken, verantwoordelijkheden en bevoegdheden zijn. Daarnaast hebben we ook de samenhang met de CIO, CDO, CPO en CISO beschreven. We hebben het Besluit CIO-stelsel Rijksdienst hiervoor als basis gebruikt.
3. ***Bepalen voorkeursoplossing***, waarin we de voor- en nadelen van de verschillende alternatieven in kaart hebben gebracht.

Deze rapportage is afgestemd met de opdrachtgevers van CIO-Rijk.

6.2 Functionarissen geïnterviewd

We hebben de volgende functionarissen gesproken:

- Beleidsadviseur privacy EZK
- Beleidsmedewerker data
- BVA BZ
- CDO EZK
- CDO JenV
- CIO-Rijk
- CISO/PO AZ
- CISO/PO BZK
- CISO Rijk
- Coördinator data en algoritmen
- CPO AZ
- CPO JenV
- CPO VWS
- FG BZ
- FG BZK
- FG EZK
- FG Financiën
- FG IenW
- FG JenV
- FG OCW
- FG VWS
- Hoofd Privacy Beleidsteam JenV
- PO Belastingdienst (3x)
- PO Financiën
- PO IenW
- PO OCW
- Privacyadviseur Rijk/rijksbrede kaders (2x)
- Privacycoördinator RWS
- PSG en CIO LNV
- Regeringscommissaris Informatiehuishouding

Berenschot

‘WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG’

Nederland is continu in ontwikkeling. Maatschappelijk, economisch en organisatorisch verandert er veel. Al meer dan tachtig jaar volgen wij als adviesbureau deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. De behoefte om iets fundamenteels te betekenen voor mens en maatschappij zit in onze genen. Met onze adviezen en oplossingen hebben we dan ook actief meegebouwd aan het Nederland van vandaag. Altijd op zoek naar duurzame vooruitgang.

Alles wat we doen is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. Zo komen we tot gefundeerde adviezen en slimme oplossingen. Die zijn op het eerste gezicht misschien niet altijd de meest voor de hand liggende. Juist deze eigenzinnigheid maakt ons uniek. Daarbij zijn we niet van symptoombestrijding. En gaan pas naar huis als het is opgelost.

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG Utrecht

Postbus 8039, 3503 RA Utrecht

030 2 916 916

www.berenschot.nl