Auditdienst Rijk
Ministerie van Financiën

Deelrapport tegenlichtrol compliance aspecten applicatie 2022

Definitief

Colofon

Titel	Tegenlichtrol compliance aspecten applicatie
Uitgebracht aan	
Datum	8 februari 2023
Kenmerk	2023-0000027127

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

1 Samenvatting

Algemeen
In dit deelrapport rapporteren wij over de belangrijkste uitkomsten van onze tweede tegenlichtrol uitgevoerd in 2022. Daarbij wordt aangetekend dat onze tegenlichtrollen (drie stuks) zich in wisselende stadia van het vervangingstraject -applicatie[1] naar applicatie plaatsvinden. Onze definitieve bevindingen, die in 2023 of 2024 worden gerapporteerd in het samenvattende eindrapport, kunnen daarom afwijken van onze tussentijdse uitkomsten in 2020 en 2022. In dit deelrapport willen wij met name bevindingen en risico's signaleren die de aandacht behoeven, zodat in 2023 nog maatregelen ter verbetering kunnen worden getroffen.

Aanleiding tweede tegenlichtrol
Bij het invoeren van de nieuwe -applicatie is het van belang om maatregelen te treffen die de compliance aspecten borgen aangaande privacy, informatiebeveiliging en archivering & schoning. De afdeling Compliance en de adviseurs compliance konden behulpzaam zijn bij het goed inrichten van de -applicatie voor wat betreft de compliance aspecten. Vanwege capaciteitsproblemen was dat bij aanvang begin 2020 tot begin 2022 nagenoeg niet gelukt. Aangegeven werd dat hierdoor nog onvoldoende aandacht was besteed aan borging van compliance aspecten. Er was daarom behoefte aan "checklists" waarmee in kaart kan worden gebracht welke maatregelen moesten worden getroffen en welke maatregelen al waren getroffen.

Doelstelling onderzoek
Het doel van de tegenlichtrol is om op een kritische wijze mee te kijken in de ontwikkelingsfase van het vervangingstraject van de applicatie naar
De focus van de opdracht ligt op de manier waarop DUO medewerkers met specialistische kennis, kaders en hulpmiddelen biedt om invulling te kunnen geven aan compliance aspecten en hoe dit bij het inrichten van de -applicatie wordt ervaren en wordt toegepast.

Centrale onderzoeksvraag
Op welke wijze geeft DUO invulling aan de compliance aspecten: privacy, informatiebeveiliging en archivering binnen DUO, toegespitst op de -applicatie?

Deelvragen

- Welke ondersteuning biedt DUO gericht op de invulling van de compliance-aspecten: privacy, informatiebeveiliging en archivering?
- Hoe ervaart het -team dit?
- Op welke wijze wordt invulling gegeven aan de compliance-aspecten (by Design) opgenomen in de AVG, BIO, de AW.

Aanvullend kunnen eventuele suggesties ter verbetering worden gedaan

Hoofdboodschap
Met behulp van 1e en 2e lijns compliance medewerkers, wordt er door het -team in toenemende mate invulling gegeven aan wet- en regelgeving omtrent privacy, informatiebeveiliging en archivering in het vervangingstraject . Er zijn verbetermogelijkheden, maar er is een enorm bewustzijn om zaken goed te doen en enthousiasme om de -applicatie compliant te maken en houden.

Binnen DUO is de afdeling Compliance ingericht (2e lijn). Zij stellen kaders, adviseren, monitoren en toetsen met betrekking tot de compliance aspecten Privacy,

1

Informatiebeveiliging en Archief- en informatiemanagement. Daarnaast zijn er per directie Adviseurs Compliance (AC) (1e lijn) aangesteld, welke het eerste aanspreekpunt zijn voor de business met betrekking tot compliance-zaken. Wanneer de kennis van de AC's ontoereikend is, wordt de 2e lijn ingeschakeld door de AC's. Er wordt momenteel een functieprofiel opgesteld voor de 1e lijn, om meer helderheid te krijgen ten aanzien van hun takenpakket. Er bestaat nu onvoldoende helderheid, waardoor elke directie het takenpakket van de AC verschillend interpreteert en positioneert. Bij de business bestaat soms enige verwarring ten aanzien van welke taken en verantwoordelijkheden bij wie liggen.

Op de wiki's (kennisbank) van Compliance en op Mavim (proceshuis DUO) staat een uitgebreide set aan DUO-brede (wettelijke) kaders, regels, richtlijnen, sjablonen, procesbeschrijvingen en tooling op het gebied van compliance. Deze set moet de business in staat te stellen om invulling te geven aan compliance bij hun werkzaamheden. Door het -team is aangegeven dat zij soms door de spreiding en de hoeveelheid aan informatie door de bomen het bos niet meer kunnen zien. Het gebruik van beschikbare documentatie wordt als complex en lastig ervaren, omdat deze omvangrijk en moeilijk te interpreteren zijn. Het -team wenst daarom een vertaling van de belangrijkste gestelde eisen vanuit de wet- en regelgeving naar toepasbare handvatten voor de situatie in de praktijk. De compliance medewerkers onderzoeken de mogelijkheid om tot integrale normenkaders te komen. Het -team krijgt in toenemende mate ondersteuning vanuit de 1e lijn, maar ook vanuit de 2e lijn.

Het -team heeft de wens om gebruik te maken van DUO-brede generieke componenten zoals archiveringsoplossingen, maar deze bleken volgens geïnterviewden ontoereikend. Er worden wel projecten opgezet om dit te verbeteren, maar dat krijgt geen prioriteit. Hierdoor is het -team genoodzaakt om de verouderde systemen van weer te gebruiken voor waarbij het DevOps-team zelf een nieuwe documenten- en brievenbibliotheek heeft ingericht. Dit verschijnsel van maatwerk bij gebrek aan geschikte generieke componenten vindt naar horen zeggen ook plaats bij DevOps-teams van andere directies. Dit kost (onnodig) veel tijd en is daardoor niet wenselijk.

Door het -team is aangegeven dat het grotendeels duidelijk is welke compliance requirements er zijn, maar dat er beperkt zicht is op de mate waarin deze zijn geborgd. Een AC, een informatieanalist en beleidsadviseur ondersteunen het -team om een volledig beeld te krijgen, en bij het vinden en toepassen van relevante documenten. Deze ondersteuning lost het probleem van ontbrekende concrete vertalingen voorlopig grotendeels op. Tools zoals een dashboard en projectenagenda zouden bijdragen aan de mate waarin AC's proactief kunnen handelen, maar deze ontbreken. Wel heerst bij de medewerkers afdeling Compliance, AC's en het -team een groot bewustzijn om zaken goed te doen en enthousiasme om DUO en de -processen compliant te maken.

Suggesties ter verbetering

- Draag compliance en borging ervan uit op elk hiërarchisch niveau
- Vertaal beleid naar uitvoeringspraktijk (bijv. concrete normenkaders per compliance aspect)
- Stel functieprofiel op voor de AC om helderheid in takenpakket te verkrijgen
- Ontwikkel generieke tools voor ondersteuning van werkzaamheden
- Stel een projectleider aan voor verandertrajecten
- Internaliseer de gewoonte om (korte) overlegverslagen te maken, daarmee formaliseer je gemaakte afspraken
- Houd de informatie in Mavim actueel
- Compliance check voor live gaan en betrek medewerkers daarbij

Leeswijzer

De centrale vraag is uitgewerkt in drie deelvragen. Deze deelvragen zijn beantwoord en de bevindingen zijn opgenomen in hoofdstuk twee. In hoofdstuk drie zijn suggesties ter verbetering opgenomen. Tot slot bevat hoofdstuk vier de verantwoording over het onderzoek.

2 Bevindingen tegenlichtrol

Het -team heeft behoefte aan goede begeleiding (beschikbaarheid compliance-specialisten en concrete/integrale normenkaders) om essentiële compliance aspecten bij het inrichten van de -applicatie mee te nemen. Begin dit jaar werd aangegeven dat ze deze begeleiding misten. Om uit te zoeken waarom het -team de juiste begeleiding miste hebben we eerst gekeken aan de hand van deelvraag één of en hoe compliance binnen DUO is ingericht en welke ondersteuning wordt geboden. Vervolgens hebben we aan de hand van deelvraag twee onderzocht of de inrichting van de afdeling Compliance en compliance hulpmiddelen toereikend en duidelijk zijn voor het -team. In deelvraag drie wordt aangegeven op welke wijze het -team invulling geeft aan de compliance aspecten (by Design) opgenomen in de Algemene Verordening Gegevensbescherming, Baseline informatiebeveiliging Overheid, de Archiefwet in relevante documentatie en processen.

Hieronder volgen de bevindingen voortkomend uit de tegenlichtrol. Deze worden per deelvraag in aparte paragrafen weergegeven.

2.1 Bevindingen deelvraag 1

Deelvraag 1:

Welke ondersteuning biedt DUO gericht op de invulling van de compliance aspecten: privacy, informatiebeveiliging en archivering?

Hierna wordt aangegeven welke ondersteuning DUO-breed wordt geboden op het gebied van de in de deelvraag genoemde compliance aspecten.

Ondersteuning in de vorm van medewerkers

Afdeling Compliance
DUO heeft een 2e lijns afdeling Compliance ingericht. Daar zijn verschillende medewerkers werkzaam die gespecialiseerd zijn in een compliance aspect. Per compliance aspect is een cluster ingericht. Het gaat om de volgende drie clusters:

- Privacy;
- Informatiebeveiliging (IB);
- Archief- en informatiemanagement (AIM).

Verder zijn een WOO-functionaris, bedrijfsjuristen en een centrale klachtenfunctionaris werkzaam bij Compliance[2]. Zij vallen niet onder bovengenoemde clusters.

Een jaar of drie geleden zijn 1e lijns Adviseurs Compliance (AC) aangesteld en toegewezen aan een directie. Zij zijn het eerste aanspreekpunt voor de business met betrekking tot compliance-zaken. Zij vallen dus niet onder de afdeling Compliance.

Medewerkers afdeling Compliance
De taken van de medewerkers in de 2e lijn zijn: kaders stellen, adviseren bij DUO-brede en complexe zaken, monitoren en toetsen (KAMT). Ieder bij zijn eigen specialisme.

[2] Three lines of defense houdt in dat de business, de 1e lijn, verantwoordelijk is voor haar eigen processen. De 2e lijn ondersteunt, adviseert, coördineert en bewaakt of de business zijn verantwoordelijkheden ook daadwerkelijk neemt. De 3e lijn controleert of het samenspel tussen de 1e en 2e lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. Bron: pwc.nl/nl/dienstverlening/consulting/risk/three-lines-of-defense-model.

Momenteel ligt, in verband met de beschikbare capaciteit en prioriteitsstelling, de focus meer op kaders stellen en adviseren en hebben ze echter niet de mogelijkheid om hier proactief, in de opstartfase, mee bezig te gaan. Ondersteunende tools zoals een dashboard en projectenagenda ontbreken.
De taken monitoren en toetsen moeten nog (verder) worden ontwikkeld. Nu wordt meestal niet gemonitord of zaken op directieniveau daadwerkelijk worden opgepakt.

Adviseur compliance
De AC's adviseren en ondersteunen de business op het gebied van Privacy, IB en AIM. De taken van een AC zijn:
- advisering op operationeel en tactisch niveau;
- verwijzen naar de vindplaats van informatie op de Compliance wiki, waardoor de medewerkers de informatie in de toekomst zelf kunnen vinden;
- bieden van begeleiding bij het opstellen van bijv. een compliance formulier, melden van een datalek of de implementatie van compliance aspecten in processen;
- geven van awareness sessies en het bijwonen van overleggen om de business compliant bewust te maken.

Uitgangspunt is dat de business zelf verantwoordelijk is voor het hanteren en implementeren van de compliance aspecten. Daarbij wordt de business ondersteund door de AC's.

Bij de directie Registers en Examens (RNE), waar het -vervangingstraject onder valt, zijn medio 2022 drie AC's werkzaam, waarvan twee in 2022 zijn aangenomen.

Taakverdeling
De 1e lijn heeft meer inhoudelijke kennis van de directie en de 2e lijn verdiepende kennis van rijksbrede kaders. Wanneer de kennis van de AC ontoereikend is, wordt de 2e lijn ingeschakeld. Samenwerking en actieve kennisdeling is daarom wenselijk. De lijntjes tussen de 1e en 2e lijn zijn kort. Ze weten elkaar te vinden en spreken elkaar ook tijdens overleggen, bijvoorbeeld bij het PIBA-RNE-overleg (privacy, informatiebeveiliging en archiefmanagement).[3]

Er wordt momenteel een functieprofiel opgesteld voor de 1e lijn, om meer helderheid te krijgen ten aanzien van hun takenpakket. Door verschillende geïnterviewden is aangegeven dat die nu onvoldoende bestaan, waardoor elke directie het takenpakket van de AC verschillend interpreteert en positioneert.

Ondersteuning in de vorm van middelen

Op de wiki van Compliance staat een set aan DUO-brede (wettelijke) kaders, regels, richtlijnen, sjablonen en tooling op het gebied van privacy, informatiebeveiliging en archivering & schonen. Het doel van deze set is om de business in staat te stellen om hier invulling aan te geven bij hun werkzaamheden. Voorbeelden hiervan zijn:
- Compliance formulier;
- Data Protection Impact Assessment (DPIA) met invulhulp (Rijksmodel);
- Sjabloon vernietigings/schoningsprotocol;
- Generieke selectielijst OCW;
- Basis selectielijst DUO;
- AVG-register.

Verder zijn in Mavim, het proceshuis DUO, DUO-brede procesbeschrijvingen opgenomen zoals het proces "Afhandelen meldingen datalekken".

Concrete normenkaders
Er is op dit moment niet één integraal concreet normenkader beschikbaar waarmee de business zelf een check kan doen op het gebied van alle compliance aspecten privacy, IB én AIM. Wel zijn er al een aantal losse hulpmiddelen bijv. de DPIA, een compliance

[3] Ten tijde van de definitieve versie van het rapport is de naam van dit overleg gewijzigd in Multi Functioneel Overleg (MFO)

formulier (intakeformulier) waarin alle compliance aspecten zijn meegenomen en een sjabloon vernietigings/schoningsprotocol. Aan een integraal normenkader binnen AIM wordt gewerkt en bij IB wordt gekeken of dit ontwikkeld kan worden. Bij AIM wordt aangegeven dat in bepaalde gevallen op basis van alleen wetgeving niet een goed advies kan worden verstrekt. Ervaring en kennis van processen spelen een grote rol, omdat wetgeving vaak een kwestie van interpretatie is. Voorwaarde is ook dat procesbeschrijvingen actueel en toereikend moeten zijn om de juiste vragen te kunnen stellen.

Tooling
Bij DUO wordt gebruik gemaakt van het Rijksbrede AVG-register, een centrale database. Dit register is echter momenteel nog onvoldoende gevuld met bijvoorbeeld opgestelde DPIA's. DPIA's worden op verschillende locaties bewaard. Het is nu voor de 1e en 2e lijn niet inzichtelijk voor welke processen wel of niet een DPIA is opgesteld. Alleen de functionaris gegevensbescherming beschikt over een overzicht van de uitgevoerde DPIA's.

Proactieve betrokkenheid 1e en 2e lijn
De business schakelt de AC's en/of medewerkers van de afdeling Compliance bij aanvang van een project vaak niet (direct) in. De wens vanuit de AC's en medewerkers van de afdeling Compliance is om in de opstartfase van een project betrokken te worden, zodat tijdig en proactief mee kan worden gedacht. Dit maakt het ook makkelijker om maatwerk adviezen te geven. Momenteel is er geen complete (DUO-brede) projectenagenda waarmee de AC's en de medewerkers van de afdeling Compliance zelf het initiatief kunnen nemen om proactief een bijdrage te leveren.

2.2 Bevindingen deelvraag 2

Deelvraag 2: Hoe ervaart het -team dit (DUO-brede ondersteuning)?

Hieronder volgen de ervaringen die het -team heeft met compliance gerelateerde medewerkers, documentatie en tooling. Aan de hand van interviews met diverse medewerkers uit het -team en diverse compliance medewerkers (1e en 2e lijn) hebben we input verzameld om de tweede deelvraag te kunnen beantwoorden.

Ervaring -team tot 2e kwartaal 2022
Bij aanvang van het vervangingstraject 2019/2020 keek het -team met name naar de technische aspecten en functionaliteiten. Compliance aspecten hadden niet de hoogste prioriteit, omdat er onvoldoende kennis binnen het -team aanwezig was en zij niet of zeer beperkt op hulp kon rekenen van de afdeling Compliance. Compliance vragen zijn wel gesteld aan de medewerkers afdeling Compliance, maar deze antwoorden werden soms te vaag ervaren om er wat aan te hebben. De AC's waren net aangenomen en speelden op dat moment nog niet direct een rol in het vervangingstraject. In een latere fase waren ze wegens ziekte en/of onderbezetting weinig beschikbaar. Het -team is daarom zelf aan de slag gegaan op basis van "best effort" ("*De trein liep en moest blijven lopen*"). Daarom werden compliance aspecten pas in een later stadium meegenomen dan de bedoeling en wenselijk was.

Ervaring -team vanaf 2e kwartaal 2022
Vanaf het 2e kwartaal 2022 ontvangt het -team ondersteuning van een AC ten aanzien van de compliance aspecten. Het team ervaart de samenwerking met de AC als prettig, de lijntjes zijn kort. De adviezen van de AC geven richting, ze hebben toegevoegde waarde. Desondanks blijven er ook vraagstukken liggen. De AC haakt steeds meer aan bij overleggen en geeft advies over vervolgstappen, wat wel of niet te doen en draagt oplossingen aan. Dat wordt door het -team al als enorme meerwaarde ervaren, omdat tot voor kort helemaal niemand van compliance betrokken was, afgezien van een hele korte periode aan het begin van het vervangingstraject. Een analist (penvoerder) is ten

tijde van het onderzoek (juni en juli 2022) met spoed bezig om de DPIA verder op te stellen en wordt daarbij geholpen door een AC en een beleidsadviseur.

Toegankelijkheid, interpreteerbaarheid en bruikbaarheid documentatie
Op het gebied van compliance is veel informatie te vinden verspreid over diverse informatiekanalen zoals DUO wiki en Mavim. Dit komt de toegankelijkheid niet ten goede en het -team ziet soms "door de bomen het bos niet meer". Het gebruiken van documentatie zoals wet- en regelgeving wordt als lastig ervaren, omdat deze vaak zeer omvangrijk en moeilijk te interpreteren zijn. De ervaring is dat medewerkers van de afdeling Compliance uitgezette vragen soms vaag beantwoorden waardoor het -team niet is geholpen.
De wens van het -team is te werken met een concrete vertaling gemaakt vanuit de wet- en regelgeving naar de situatie in de praktijk. Een vertaling met de belangrijkste (minimale) gestelde eisen (kaders, checklijsten, stroomschema's of draaiboeken), zodat de compliance aspecten voor het -team inzichtelijker worden en gemakkelijker zijn mee te nemen.

Ondersteuning analist en AC
Het -team krijgt nu ondersteuning van een analist en AC. Zij hebben nu (meer) tijd om aan te haken, te helpen. Dit geeft meer helderheid en zekerheid ten aanzien van de toe te passen compliance aspecten. Bij het vinden en toepassen van relevante documenten wordt hulp geboden op het gebied van algemene en specifieke zaken. Aangegeven wordt dat dit grotendeels het probleem van ontbrekende concrete vertalingen oplost. Desondanks zijn compacte normenkaders voor de business wenselijk om onafhankelijker te kunnen werken.

Samenwerking en taakverdeling 1e en 2e lijn
De AC's en medewerkers van de afdeling Compliance ervaren de samenwerking overwegend positief. Aangegeven is echter dat er verwarring bestaat bij de AC's en medewerkers van de afdeling Compliance door het ontbreken van een duidelijk functieprofiel van de AC, maar ook bij de business ten aanzien van welke taken en verantwoordelijkheden bij wie liggen. Het gebrek aan functieafbakeningen heeft geleid tot een aantal escalaties tussen de 1e en 2e lijn.

Generieke componenten
Het -team is wat compliance betreft afhankelijk van DUO-brede ontwikkelingen op het gebied van generieke componenten, waarbij het -team op een gegeven moment moet aanhaken. Het team heeft gekeken naar beschikbare en/of geschikte generieke componenten, maar deze bleken volgens meerdere geïnterviewden afwezig of ontoereikend te zijn. Een voorbeeld van afwezig is het Digitaal archief 2.0 en ontoereikend is het Digitaal archief 1.0. Tijdens een interview werd aangegeven dat de ervaarde ongeschiktheid van generieke componenten DUO-breed gedeeld wordt. Er worden wel projecten opgezet om deze te verbeteren, maar deze krijgen geen prioriteit. Door de ongeschiktheid van de huidige DUO-brede archiveringoplossingen, worden de verouderde systemen van weer gebruikt voor Om het werkbaar te maken heeft het team aangegeven dat het te veel tijd heeft gekost om zelf zaken op orde te brengen, zoals een documentenbibliotheek en brievenbibliotheek. DevOps-teams van verschillende directies richten zelf applicaties en/of processen in, wat (onnodig) veel tijd kost.

AVG versus klantvriendelijkheid
Medewerkers binnen het -team ervaren dat compliance op dit moment in de weg kan staan van DUO's kerndoelstelling om klantvriendelijk te handelen. Een voorbeeld dat wordt aangedragen is dat een beschikking per post moet worden verstuurd. Wanneer iemand in het buitenland woont komt het voor dat de post pas na maanden aankomt, waardoor de bezwaartermijn dan al verlopen kan zijn. Klanten willen beschikkingen graag per mail willen ontvangen, maar dat mag vanuit privacy oogpunt momenteel niet omdat de veiligheid van het mailverkeer niet gegarandeerd is. Medewerkers geven aan dat het veilig versturen van bijlagen per mail bij externen wel al mogelijk is.

2.3 Bevindingen deelvraag 3

Deelvraag 3:
Op welke wijze wordt invulling gegeven aan de compliance aspecten (by Design) opgenomen in de AVG, BIO, de AW in:

- het functionele ontwerp van de applicatie
- de procedures (inclusief taken, bevoegdheden en verantwoordelijkheden) van de toekomstig gebruikers van de -applicatie.

Op de volgende wijze wordt al dan niet invulling gegeven aan compliance aspecten.

Functioneel ontwerp

Functioneel ontwerp (FO) - Use Cases
Voor de -applicatie is niet één FO opgesteld, maar meerdere use cases (UC) per deelapplicatie die tezamen het FO vormen. Deze UC betreffen procesonderdelen zoals het verwerken van een aanvraag of het omzetten van aanvraaggegevens.
In de UC van zijn geen compliance aspecten opgenomen.

Requirements
Requirements (functioneel en niet-functioneel) worden opgesteld om inzichtelijk te maken aan welke eisen het systeem moet voldoen. Compliancy is een voorbeeld van een niet-functionele requirement.

Op de wiki van DUO is onder Diplomadiensten/ (nieuwbouw) een schema opgenomen met business en functionele requirements die nodig zijn voor -deelapplicaties "VAE" en de "core". Wat betreft compliance aspecten komt in dit schema alleen een requirement aangaande archivering aan bod, privacy en informatiebeveiliging zijn niet opgenomen. Vermeld is dat het schema steeds verder wordt uitgebreid, maar niet of deze betrekking heeft op de twee genoemde deelapplicaties of eventuele andere -deelapplicaties.

Geïnterviewde medewerkers geven aan dat voor het overgrote deel duidelijk is welke compliance requirements er zijn, maar dat er geen volledig overzicht is van welke moeten worden meegenomen en welke zijn meegenomen. Een AC ondersteunt het -team om een volledig beeld te krijgen

Security en Online
In het overzicht"Security - en Online (d.d. 29 juni 2022)" staat een uiteenzetting van applicatieattributen met een toelichting erop. Bij verschillende attributen wordt de noodzaak aangegeven om een DPIA uit te voeren vanwege de aanwezigheid van privacygevoelige informatie. In het bijbehorende document "Privacy en persoonsgegevens" wordt verder uitleg gegeven over soorten persoonsgegevens met voorbeelden. Naast privacy, komt informatiebeveiliging bij één attribuut ter sprake, maar in het overzicht wordt niets aangegeven over archivering.

Procedures en processen

Opstart bouw applicatie
Bij het vormgeven van de -applicatie was het uitgangspunt om alle bestaande elementen van de -applicatie over te nemen, maar dan in een "nieuw en verbeterd jasje". In worden geen nieuwe functionaliteiten toegevoegd, afgezien van de automatisering van een aantal handmatige werkzaamheden. Ook de compliance elementen worden overgenomen uit Echter, wat betreft de -applicatie is weinig tot niets gedocumenteerd. De informatie zit veelal in de hoofden van medewerkers en veel oudgedienden met kennis van zaken hebben de organisatie verlaten.

Voor het vervangingstraject naar is geen projectleider aangesteld, omdat een ander vervangingstraject in het verleden goed was verlopen. Bij aanvang van het

vervangingstraject heeft er een kick-off meeting plaatsgevonden tussen de functioneel beheerder, bouwers, testers, business analist, beleidsadviseur en de product owner. Hierin is onder andere besproken hoe het vervangingstraject eruit moest komen te zien. Van deze kick-off meeting is geen verslag opgemaakt, dus de hierin gedeelde informatie en overwegingen alsmede gemaakte afspraken zijn niet vastgelegd.

Borging compliance in
In de beginfase van het vervangingstraject is beperkt aandacht geschonken aan de borging van compliance-aspecten in Er is wel een begin gemaakt met het invullen van een compliance formulier, waarbij echter veel onderwerpen niet waren ingevuld. Daarnaast had er bij aanvang van het vervangingstraject een DPIA uitgevoerd moeten worden, wat niet is gebeurd. Inmiddels is het opstellen van de DPIA met spoed opgepakt door een analist met hulp van een AC en beleidsadviseur. De verwachting van het team is dat hier niet veel verrassende zaken meer uitkomen, omdat heel veel DPIA-onderwerpen in de afgelopen jaren al zijn besproken.

In veel -producten komen NAW-gegevens van de klant voor. Volgens een medewerker zijn deze gegevens verwerkt conform de gestelde compliance-eisen in de AVG.

Taken, bevoegdheden en verantwoordelijkheden
Vanuit interviews hebben we verschillende geluiden gehoord met betrekking tot taken, bevoegdheden en verantwoordelijkheden. Op hoofdlijnen is binnen het -team duidelijk wie wat moet doen en wie waar verantwoordelijk voor is. Uit interviews kwam echter naar voren dat er verschillende percepties bestaan over wie verantwoordelijk is voor het initiëren (de manager of product owner) en uitvoeren (analist of beleidsmedewerker) van een DPIA.

Protocollen, procesbeschrijvingen en werkinstructies
Er zijn "praatplaten" opgesteld, deze tonen hoe bepaalde processen/procestappen en API's (Application Programming Interface) lopen tussen de verschillende -applicaties. Rollen (inclusief rollen, taken en bevoegdheden) zijn hierin niet weergegeven. Voor gebruikers van de -applicatie zijn nog geen protocollen en werkinstructies opgesteld.

Op RNE-niveau is een aantal werkinstructies beschikbaar, maar de vertaalslag naar applicatieniveau moet nog worden gemaakt. Twee medewerkers zijn daar momenteel mee bezig.

Een medewerker gaf aan dat er regelmatig schoningsacties van bijvoorbeeld documenten plaatsvinden, ondanks dat er geen schoningsprotocol is opgesteld. Door het ontbreken van een schoningsprotocol is het onduidelijk of de kennis werkelijk bij alle -teamleden aanwezig is en (alle) stappen bij het opschonen op een juiste wijze plaatsvindt.

Wel is er een document "Schonen in het kader van AVG, bewaartermijnen van documenten" opgesteld. Hierin staan de bewaartermijnen van -producten zoals kopieën identificatiedocumenten en besluiten. Dit document omvat echter maar een deel van wat er volgens het sjabloon schoningsprotocol moet worden opgesteld. Het opstellen van een "verklaring van vernietiging" van (digitale) archiefbescheiden ontbreekt bijvoorbeeld.

Voorwaarden live gaan
De "Go", "No-Go"-momenten in het vervangingstraject vinden plaats via de eindsprints, die elke 3 weken plaats vinden. Wanneer het gebouwde voldoende is of het volstaat dan gaat het opgeleverde in productie (Go). De product owner geeft daarvoor zijn akkoord.

Go-voorwaarden voor het uiteindelijk live gaan van de -applicatie zijn:
- geen cruciale compliance onvolkomenheden (DPIA);
- een Gebruikersacceptatietest (GAT);
- een hacktest;

- een akkoord op technische aspecten.

Deze vier voorwaarden zijn onderling afgesproken, maar nergens formeel beschreven.
In tegenstelling tot privacy (middels de DPIA) en informatiebeveiliging (op beperkte wijze middels uitsluitend een hacktest), komt (de opzet van) archivering maar heel summier (onderdeel in de DPIA) aan bod als zijnde een voorwaarde om live te laten gaan. Dit is opmerkelijk, omdat uit interviews blijkt dat archivering op dit moment een grote zorg is binnen Door het gebrek aan aansluiting met de DUO-brede oplossing Digitaal Archief 2.0, alsmede onvoldoende mankracht om dit te verhelpen, is genoodzaakt terug te vallen op verouderde systemen. Maar ondanks dat archivering en schoning nog onvoldoende is geregeld hoeft dit geen problemen op te leveren voor het live gaan van de werking van Archivering speelt pas op een later moment in het proces een rol. Het sjabloon schoningsprotocol helpt daarbij en kan wel alvast opgesteld worden, zodat de business weet wat te doen zodra archiveren en schonen aan de orde zijn.
Het -team heeft de wens uitgesproken om alvorens live te gaan een meetmoment in te lassen om te bepalen hoe het ervoor staat wat betreft compliance. Dit is echter lastig te realiseren, omdat het -team geen compleet overzicht heeft van de relevante compliance aspecten mede vanwege het ontbreken van concrete normenkaders. Betrokken medewerkers uit zowel de 1e als 2e lijn gaven aan wel te weten dat momenteel niet aan alle compliance aspecten wordt voldaan.

Live gaan
De planning was dat alle -componenten op 1 september 2022 live in productie zouden gaan. Dit is niet gelukt. De vastgestelde deadline is 1 januari 2023. In de planning is rekening gehouden met het feit dat de ontwikkeling van op 1 september 2022 nog niet helemaal gereed zou zijn. Er is namelijk niet voldoende tijd, mensen en geld om alle wensen direct mee te kunnen nemen. Wanneer in gebruik wordt genomen wordt er voldaan aan de minimale functionele eisen, waardoor medewerkers kunnen werken met deze applicatie. blijft voorlopig functioneren en fungeert straks als schaduwadministratie. Mocht er bij het live gaan van iets fout gaan kan er worden teruggegrepen op

Overleg
Het -team spreekt elkaar dagelijks via een stand-up. Informatie wordt mondeling gedeeld en sprints worden gezamenlijk ingepland. In een roadmap in Jira wordt een backlog bijgehouden en maandelijks wordt gerapporteerd over de output. Wekelijks vindt (analyse-)overleg binnen het BAT-team plaats waar ook veel hamerstukken worden besproken. Bij dit overleg zijn aanwezig: product owner, vertegenwoordiger van communicatie, beleidsadviseur, relatiemanager, toekomstige gebruikers en een gast. Zaken over de AVG, IB en Archivering worden hier ook besproken, een AC schuift regelmatig aan voor de nodige adviezen bij voorkomende problematiek.

Rapportage
Het managementteam RNE krijgt tweemaandelijks een rapportage Risk & Compliance, opgesteld door Compliance platform/staf RNE i.o. De opgenomen onderwerpen betreffen: Risico beheersingstabel, Monitoring & Kwaliteit, Compliance en Aanbevelingen. Momenteel staat er nog weinig informatie in over de -applicatie of over de algehele status van het vervangingstraject

Informatiebeveiliging
Vanuit de directie RNE is momenteel veel aandacht voor informatiebeveiliging. Recentelijk zijn alle managers bijeengeroepen voor een informatiesessie over phishing gegeven door een externe organisatie. De bedoeling is dat dergelijke sessies maandelijks georganiseerd gaan worden. Daarnaast vinden er DUO-breed security awareness programma's plaats. Hier wordt ook aandacht aan besteed in de nieuwsbrief van DUO, in de mail en in stand-up's. Het is in de toekomst de bedoeling om bepaalde informatie/onderwerpen aan te bieden via e-learning.

3 Suggesties ter verbetering

In dit hoofdstuk doen wij een achttal verbetersuggesties ten behoeve van het borgen van de compliance aspecten, welke zowel DUO-breed als -specifiek toepasbaar zijn.

Allereerst een top.

3.1 Top

Groeiende inrichting en awareness compliance
Er is in toenemende aandacht voor compliance, zowel op directieniveau als bij uitvoerende medewerkers. Binnen DUO is een afdeling Compliance opgetuigd met een eigen uitgebreide wikipagina. Er is en wordt gewerkt aan de creatie, vindbaarheid en bruikbaarheid van compliance-informatie. Zo onderzoeken medewerkers van de afdeling Compliance momenteel de mogelijkheid om tot concrete/integrale normenkaders te komen, zodat compliance-eisen inzichtelijker worden en gemakkelijker door de business zelf zijn mee te nemen in hun processen.

Een jaar of drie geleden is de compliance functie heringericht naar een 1e lijn in de vorm van adviseurs compliance en een 2e lijn in de vorm van medewerkers van de afdeling Compliance met ieder een expertise op het gebied van privacy, informatiebeveiliging of archiefinformatiemanagement. De adviseurs compliance fungeren als een eerste aanspreekpunt voor de business en verzorgen ook awareness presentaties. De medewerkers van de afdeling Compliance gaan over complexe en DUO-brede zaken en fungeren weer als aanspreekpunt voor de adviseurs compliance. Hierdoor beschikt de algehele compliance functie over direct contact met de uitvoering, alsmede over de expertise om compliance gerelateerde vraagstukken af te handelen. Bij de medewerkers van de afdeling Compliance, adviseurs compliance en het -team heerst een groot bewustzijn om zaken goed te doen en enthousiasme om de DUO en de -applicatie compliant te maken en te houden.

3.2 Verbetersuggesties

Draag compliance en borging ervan uit op elk hiërarchisch niveau
Ten eerste is het belangrijk om het belang van compliance en de borging daarvan uit te dragen op elk hiërarchisch niveau. Bij de directie RNE is compliance relatief goed onder de aandacht. Het bewustzijn moet (DUO-breed) komen dat compliance niet een eenmalige check is maar een belangrijk doorlopend thema. Ook is het van belang om compliance aspecten op te nemen in relevante documentatie zoals requirementsoverzichten, zodat er wordt afgedwongen dat compliance wordt meegenomen bij de (her)inrichting van applicaties. Daarbij is het van belang om te realiseren dat compliance breder is dan alleen privacy. Immers, middels een DPIA worden de BIO en Archiefwet nog niet afgedekt.

Vertaal beleid naar uitvoeringspraktijk
Ten tweede dient er een vertaalslag plaats te vinden van beleid naar uitvoering. Er bestaat DUO-breed een aantal voorschriften, waarvan het niet duidelijk is hoe dit in de praktijk uitgevoerd moet worden. Voorbeelden hiervan zijn concrete normenkaders per compliance aspect en het uitvoeren van een risicoanalyse; het uitvoeren daarvan is voorgeschreven, maar het is voor medewerkers niet duidelijk op welke wijze risico's in de praktijk geformuleerd of vastgelegd moeten worden.

Stel functieprofiel AC op om helderheid in takenpakket te verkrijgen
De derde verbetersuggestie is het DUO-breed opstellen van een functieprofiel van de Adviseur Compliance, zodat er binnen de organisatie een eenduidig beeld ontstaat van de

taken, bevoegdheden en verantwoordelijkheden van deze functie. Doordat dit functieprofiel vaag geformuleerd is, geven de directies verschillende invullingen aan de functie van AC. Hierdoor zou capaciteit verloren kunnen gaan door een (onopgemerkte) overlap in werkzaamheden van de 1e en 2e lijn (compliance) medewerker. Ook riskeer je dat bepaalde werkzaamheden onopgemerkt niet worden uitgevoerd, omdat verondersteld wordt dat deze bij iemand anders zijn/haar takenpakket behoren. Ook zou het bijdragen aan het toezien op de naleving van taken, verantwoordelijkheden en bevoegdheden, aangezien deze dan vastgelegd zouden zijn.
Tijdens het onderzoek is aangegeven dat er aan het opstellen van het functieprofiel voor de AC wordt gewerkt.

Ontwikkel generieke tools voor ondersteuning van werkzaamheden
Ten vierde zouden wij aanbevelen tools te ontwikkelen die zowel de 1e als 2e lijn zouden ondersteunen in een efficiënte en effectieve uitvoering van hun werkzaamheden. Voorbeelden hiervan zijn het organiseren van een (centrale) projectenagenda, dashboard met daarop de stand van zaken van bijvoorbeeld DPIA's, normenkaders en/of draaiboeken voor de (opstart van) de (her)inrichting van applicaties. Dergelijke tools dragen bij aan de mogelijkheid voor 1e en 2e lijn compliance medewerkers om proactief te kunnen handelen en niet reactief. Tevens helpt een vertaling met de belangrijkste (minimale) gestelde eisen in concrete normenkaders de business om snel inzicht te krijgen in essentiële compliance aspecten en deze gemakkelijker zelf mee te nemen. Door dergelijke tools centraal te ontwikkelen, creëer je bovendien uitwisselbaarheid tussen verschillende medewerkers in eenzelfde functie zoals een AC.
Tijdens het onderzoek is aangegeven dat er wel aan wordt gewerkt (archiefinformatiemanagement) of gekeken of concrete normenkaders ontwikkeld kunnen worden (informatiebeveiliging).

Stel een projectleider aan voor verandertrajecten
De vijfde verbetersuggestie betreft het aanstellen van een projectleider bij toekomstige verandertrajecten. In het geval van is hier niet voor gekozen in verband met een eerdere succeservaring. Eerdere ervaringen bieden echter geen garanties voor toekomstige projecten. Door het aanstellen van een projectleider kan deze zich bezighouden met de het borgen van de uitvoering van projectstappen, zoals het tijdig op (laten) opstellen van een DPIA. Zo kan de product owner zich bezighouden met de zaken die het product, de -applicatie, zo waardevol mogelijk maakt voor de eindgebruiker.

Internaliseer de gewoonte om (korte) overlegverslagen te maken
De zesde verbetersuggestie betreft het internaliseren van de gewoonte om (korte) overlegverslagen te maken, zeker in het geval van belangrijke overleggen zoals kick-off sessies. Door het vastleggen van hetgeen besproken wordt, formaliseer je onderlinge afspraken. Hierdoor wordt het eenvoudiger om taken, bevoegdheden en verantwoordelijkheden na te leven en elkaar daarop aan te spreken. Bovendien bieden verslagen de mogelijkheid om ergens op terug te kunnen grijpen bij onduidelijkheden. Ook wordt hiermee voorkomen dat kennis die veelal impliciet is, verloren gaat wanneer medewerkers vertrekken.

Houd de informatie in Mavim actueel
De zevende verbetersuggestie heeft te maken met het feit dat op het gebied van compliance veel informatie te is vinden verspreid over diverse informatiekanalen zoals DUO wiki en Mavim. We zouden willen meegeven om Mavim door te nemen om te kijken in welke mate de informatie daarop nog actueel is en of aansluit op de huidige praktijk. Daarbij zou het mooi zijn als er op de DUO wiki wordt verwezen naar de betreffende processen, omdat vraagstukken ontstaan bij medewerkers bij de uitvoering van processen. Dit zou ook bijdragen aan de vindbaarheid van informatie, omdat een zoekopdracht in Mavim dan sneller leidt tot relevante zoekresultaten en duidelijk is dat dit actuele informatie is.

Compliance check voor live gaan en betrek medewerkers daarbij
Tot slot was er gedurende het ontwikkeltraject weinig zicht op welke compliance aspecten meegenomen moeten worden en welke meegenomen zijn. Het -team heeft de wens uitgesproken om alvorens live te gaan een meetmoment in te lassen om te bepalen hoe het ervoor staat voor wat betreft compliance. Betrek hierbij de AC en medewerkers van de afdeling Compliance om een zo compleet mogelijk overzicht te krijgen van de relevante compliance aspecten met daaraan een prioriteit gehangen.

4 Verantwoording tegenlichtrol

4.1 Werkwijze en afbakening

Aan de hand van relevante documentatie en het houden van interviews met betrokken functionarissen hebben wij, in de periode mei, juni en juli 2022, een beeld gevormd over hoe invulling is gegeven aan compliance binnen DUO, de bruikbaarheid ervan voor het -team en of en hoe compliance aspecten zijn meegenomen bij de (processen van de) -applicatie.

4.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Deze tegenlichtrol verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd. De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

4.3 Verspreiding deelrapport

De ADR is de interne auditdienst van het Rijk. Dit deelrapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen.
Er is in 2020 een eerste tegenlichtrol uitgevoerd in de ontwikkelingsfase van het vervangingstraject van de applicatie naar De bevindingen van die tegenlichtrol zijn teruggekoppeld in een brief van bevindingen. De bevindingen uit deze tweede tegenlichtrol zijn weergegeven in een deelrapport. Na uitvoering van de derde en laatste tegenlichtrol zal een eindrapport worden opgesteld. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

5 Ondertekening

Groningen, 8 februari 2023

(projectleider)

6 Managementreactie

CONCEPT/VERTROUWELIJK/DEFINITIEF

Directie
Registers & Examens
Afdeling
M&O
Contactpersoon

Datum
10 03 2023
Bijlagen

memo

Managementreactie op het ADR Deelrapport Tegenlichtrol compliance aspecten applicatie d.d. 8 februari 2023, met als kenmerk 2023-0000027127

Dit rapport belicht de uitkomsten van de tweede tegenlichtrol zoals die door de ADR is uitgevoerd in 2022. Een rapportage over de uitgevoerde eerste tegenlichtrol is in een eerder stadium al besproken en vastgesteld.

In de tweede fase van de tegenlicht rol is op verzoek van de opdrachtgever de focus vooral gelegd op de compliance aspecten van , te weten privacy, informatiebeveiliging en archivering.
De opdrachtgever wilde een extra check op de compliance aspecten van de applicatie juist omdat met de oude applicatie niet werd voldaan aan de gestelde compliance eisen.
Juist deze gebreken van waren de belangrijkste drivers om te ontwikkelen.
De tegenlichtrol is uitgevoerd om het team dat de nieuwe applicatie ontwerpt en bouwt en gaat beheren (Agile: You built it, You run it) te helpen om de juiste en essentiële compliance aspecten bij de ontwikkeling van de applicatie te realiseren.

Het onderzoek kende een langere doorlooptijd dan verwacht, ruim een half jaar.
Deels ook vanwege veranderingen met het oog op rapportage en verantwoording in het kader van de Wet open overheid (Woo). Dit had tot gevolg dat dat aanbevelingen daardoor soms gedeeltelijk en soms volledig zijn achterhaald.

Ondanks de opgetreden vertraging tijdens het uitvoeren van de tegenlichtrol kan worden geconcludeerd dat alle betrokken partijen verheugd zijn met de hoofdboodschap van dit ADR-Rapport:

Met behulp van 1e en 2e lijns compliance medewerkers, wordt er door het RDI-team in toenemende mate invulling gegeven aan wet- en regelgeving omtrent privacy, informatiebeveiliging en archivering in het vervangingstraject
Er zijn verbetermogelijkheden, maar er is een enorm bewustzijn om zaken goed te doen en enthousiasme om de applicatie compliant te maken en houden.

DUO neemt de concrete suggesties ter verbetering ter harte, de verbetersuggesties zijn reeds intern uitgezet.

Ondertekend door:

Directeur Registers & Examens

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00