Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport Informatiebeveiliging Donorregister

Definitief

Colofon

Titel	Informatie beveiliging Donorregister
Uitgebracht aan	mevr. A.I. Norville MSc, plaatsvervangend SG van het ministerie van Volksgezondheid, Welzijn en Sport
Datum	02 september 2021
Kenmerk	2021-0000180981

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

CIBG onderkent de benodigde verbeteringen voor informatiebeveiliging en AVG en geeft hieraan prioriteit middels een programma

In dit rapport staan de onderzoeksresultaten aangaande de Informatiebeveiliging en de bescherming van Persoonsgegevens van het Donorregister, dat per 1 juli 2020 is geïmplementeerd.
Tijdens het onderzoek hebben wij ervaren dat CIBG zich bewust is van de urgentie om de informatiebeveiliging en bescherming van persoonsgegevens bij het Donorregister te verbeteren. CIBG heeft daartoe het afgelopen jaar diverse initiatieven ontplooid. Vanaf juni 2020 zijn Quickscan, Data Protection Impact Assessment (DPIA) (de risicoanalyse naar de bescherming van de persoonsgegevens van de betrokkene) en het zeer verouderde Informatiebeveiligingsplan Donorregister grondig bijgewerkt. Ook heeft het CIBG zelf in februari 2021 een 'Eerste Vervolgonderzoek Informatieveiligheid Donorregister' uitgevoerd. De bevindingen daarvan zijn vertaald en opgenomen in het 'Programma Doorontwikkeling Informatieveiligheid[1]'. Dit programma verkeert ten tijde van ons onderzoek (juli 2021) nog in conceptstadium.

Op basis haar onderzoek beveelt ADR CIBG aan om:
- het IB-beleid te actualiseren en het Privacybeleid daarin te integreren,
- de uitvoering, vastlegging en uitwerking van de risicoanalyses te verbeteren,
- *alle* relevante bedrijfsmiddelen van belang voor het Donorregister te inventariseren en vervolgens een passend autorisatiebeheer in te richten,
- het IB-plan te verbeteren door *alle* maatregelen die van belang zijn voor het Donorregister daarin op te nemen,
- de huidige beschrijvingen, procedures en werkinstructies in kaart te brengen, te actualiseren en daarbij aandacht te schenken aan de onderlinge consistentie van documenten,
- toezicht in te regelen op de uitvoering van de maatregelen.

Op de volgende onderwerpen heeft ADR punten ter verbetering geconstateerd:
- Uitvoering en vastlegging risicoanalyses
  De risicoanalyses voor het Donorregister uit 2020 missen samenhang vanuit beleid en het totstandkomingsproces is niet inzichtelijk gemaakt. Risico's zijn mogelijk niet onderkend of onderbelicht gebleven.
  Vervolgens zien we dat de risicoanalyse nog in het IB-plan wordt doorgevoerd.

- Beheersing van de maatregelen voor informatiebeveiliging en de bescherming van persoonsgegevens
  In IB-plan is aangegeven dat op basis van de QuickScan BBN2[2] van toepassing is. In het IB-plan zijn niet alle BBN2 maatregelen opgenomen. Risico's en maatregelen zijn gezamenlijk in de DPIA verwoord en betreffende maatregelen zijn vervolgens niet geborgd in een Privacy Plan Donorregister.
  De ontvangen documenten ten aanzien van (de organisatie van) beheers-maatregelen zoals handreikingen, procedures en werkinstructies sluiten niet altijd goed op elkaar aan en kennen in enkele gevallen ook overlappingen. Tevens is de verantwoordelijke van de documenten niet altijd bekend en is het versiebeheer ten aanzien van de actualiteit niet altijd op orde. Inventarisatie

[1] Met dit programma wil CIBG – meerjarig – 'toewerken naar een organisatie die volledig in lijn is met de koers van het CIBG en de organisatie op de schaal van het Capability Maturity Model (CMM) naar een hoger volwassenheidsniveau (tenminste niveau 3) tillen. Indien dit niveau bereikt wordt, is er sprake van beheersmaatregelen die zijn gedocumenteerd en die op gestructureerde en geformaliseerde wijze worden uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst'.

[2] De Baseline Informatiebeveiliging Overheid (BIO) onderscheidt een drietal Basisbeveiligingsniveaus (BBN) zijnde BBN1, BBN2 en BBN3. In de BIO staat per BBN beschreven aan welke controls uit de ISO 27002 (Code voor Informatiebeveiliging) moet worden voldaan.

van alle relevante bedrijfsmiddelen is niet volledig waardoor passende maatregelen voor autorisatiebeheer voor deze bedrijfsmiddelen niet inzichtelijk zijn. Voorts heeft CIBG de volledigheid van de (af te sluiten) verwerkersovereenkomsten voor het Donorregister niet vastgesteld. CIBG heeft niet de voorgeschreven jaarlijkse verklaringen opgevraagd op grond van b.v. art. 11 van de verwerkersafspraken-/overeenkomsten met uitzondering van die van KPN.

- ADR ziet ruimte voor verbetering op toezicht op informatiebeveiliging.
  De inhoud van de afgegeven In Control Verklaring (ICV) is gerelateerd aan het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) en is daarmee minder gedetailleerd dan in de maatregelen vanuit de BIO wordt voorgeschreven. De ICV van CIBG bevat op dit moment geen informatie over de maatregelen in het kader van de Privacy, die zijn zelfs expliciet uitgesloten. Volgens de Privacy Governance VWS uit 2018 is het juist wel de bedoeling dat Privacy wordt geïntegreerd in de ICV.
  Naast de bevindingen van de ADR geeft CIBG ook uit eigen onderzoek aan dat CIBG voor de interne beheersing nog geen Auditplan heeft, bezig is met een Information Security Management System (ISMS) project en met het toewijzen van verantwoordelijkheden voor de controle op de naleving.
  Ook onderkent CIBG zelf dat CIBG voor de beheersing van de aan haar leveranciers/ verwerkers uitbestede werkzaamheden (b.v. verwerking (persoons-)gegevens van CIBG) contract-/leveranciersmanagement beter moet gaan oppakken en de PDCA rond leveranciers verder moet gaan inrichten.

1 Aanleiding opdracht

Eind november 2020 heeft de ADR haar onderzoeksrapport aan CIBG opgeleverd: *'Inventarisatie maatregelen t.a.v. beheer externe gegevensdragers Donorregister'*.
De aanleiding voor dat onderzoek was het zoekraken van twee externe harde schijven in maart 2020. De Minister voor Medische Zorg heeft op 4 maart 2021 het onderzoeksrapport van de ADR aangeboden aan de Voorzitter van de Tweede Kamer met een begeleidende brief: 32761/nr. 178.
Gedurende het onderzoek van 2020 heeft Kamerlid Dijkstra c.s. 2 juli 2020 een motie ingediend met het verzoek aan de regering om de hele informatiebeveiliging van het Donorregister te onderzoeken. Later, op 11 februari 2021 dient Kamerlid Van den Berg/Dijkstra een motie in met het verzoek aan de regering om een onafhankelijk onderzoek naar de wijze waarop de informatiebeveiliging bij de huidige donorregistratie is georganiseerd, en de Kamer hierover voor de zomer van 2021 te informeren.
In de brief van 4 maart 2021 schrijft de Minister tevens, dat de ADR - in navolging van de moties van de leden Dijkstra en Van den Berg c.s. - aanvullend onderzoek zal doen naar het nieuwe Donorregister. Voor dit onderzoek zal de ADR de gehele informatiebeveiliging van het nieuwe Donorregister beoordelen. "Zoals ik al eerder heb aangegeven, hoop ik de Kamer voor de zomer te kunnen informeren over de uitkomst van dit aanvullende onderzoek".
Voorliggend rapport is het resultaat van het hierboven toegezegde onderzoek.

2 Risicoanalyses voor het Donorregister zijn uitgevoerd door toepassing QuickScan en DPIA

Onderzoeksvraag 1.:
Welke aanpak heeft CIBG toegepast voor de risicoanalyse die ten grondslag ligt aan de maatregelen verwoord in het informatiebeveiligingsplan (IB–plan)? (Proces-Betrokkenen-Uitvoering).

2.1 QuickScan en DPIA kunnen verbeterd worden

Voor het Nieuwe Donorregister is in de periode mei - 2 juli 2020 een gestandaardiseerde QuickScan-informatiebeveiliging uitgevoerd. Het doel van dergelijke QuickScan is om inzicht te krijgen of

- het Donorregister een Te Beschermen Belang is,
- de AVG voldoende is geïmplementeerd en een gegevensbescherming Effecten Beoordeling (GEB) wenselijk is,
- de maatregelen uit de Baseline Informatiebeveiliging voldoende zijn geïmplementeerd om de informatiebeveiligingsrisico's af te dekken.

In de QuickScan voor het nieuwe Donorregister is voor de AVG geen analyse uitgevoerd, omdat er reeds een actuele Gegevensbeschermingseffectbeoordeling GEB (ook wel: Data Protection Impact Assessment: hierna DPIA) beschikbaar was. Deze DPIA is per 10 juni 2020 vastgesteld. Hierin staan de risico's, die de voorgenomen gegevensverwerkingen hebben voor de rechten en vrijheden van de betrokkenen, beschreven. CIBG heeft deze risico's beoordeeld en in de DPIA voorzien van maatregelen.

Bij het analyseren van de QuickScan en DPIA merken we het volgende op:

2.1.1 *Format voor risicoanalyses uit Informatiebeveiligingsbeleid is niet gevolgd*

Het IB-beleid CIBG (2018) (hierna: IB-Beleid) is een bovenliggend document boven de risicoanalyses en het Informatiebeveiligingsplan Donorregister (hierna: IB Plan). In het actuele IB-beleid is in bijlage 9 een format voor risicoanalyses opgenomen. Dit format is niet gevolgd. Onderdelen van dit format komen wel terug in de QuickScan andere onderdelen komen terug in het IB-plan. Ook wordt als onderdeel van de risicoanalyse de AVG genoemd met daarbij te vullen tabellen, deze aanpak is niet gevolgd.

2.1.2 *CIBG heeft kaders voor risicoanalyse voor AVG niet nader uitgewerkt*

Het IB-beleid maakt nauwelijks melding van de AVG. In het format risicoanalyse wordt AVG wel genoemd, maar het vermeldt bijvoorbeeld niet de voorwaarden voor uitvoering van een DPIA. 'Privacy Governance VWS' (november 2018) richt zich op het VWS kerndepartement en haar concernonderdelen (waaronder CIBG). In bijlage 1 en 2 (het Beleidskader en Privacyprogramma) van Privacy Governance VWS staat wanneer een DPIA moet worden uitgevoerd, welke aspecten daarbij een rol spelen en wie welke verantwoordelijkheid draagt in het proces van DPIA. CIBG is voornemens dit beleid te vertalen naar CIBG.

2.1.3 *Uitvoering van risicoanalyses kan beter*

Het aantal deelnemers aan QuickScan workshop was beperkt tot twee deelnemers. De resultaten van de workshop zijn volgens CIBG schriftelijk afgestemd met overige stakeholders. Ten aanzien van DPIA is er door gebrek aan vastleggingen geen zekerheid over wie daadwerkelijk betrokken waren in het proces en hoe het proces van de risicoanalyse van de DPIA is uitgevoerd. Zo is niet duidelijk welke stappen in het proces van risico-inventarisatie, -duiding, -analyse, -acceptatie of afdoening zijn gezet.

2.1.4 *QuickScan kent inhoudelijke verbeterpunten*

Ten aanzien van de QuickScan onderdeel BIO zien wij de volgende verbeterpunten:

- Niet alle systemen zijn onderkend, maar slechts één (informatie-)systeem is onderkend. In de QuickScan is alleen het DORA informatiesysteem onderkend. Echter kijkend naar definitie van het proces zijn meerdere systemen van belang voor de uitvoering van het proces.
- Classificatie van de rol van het systeem (DORA) voor het Donorregister is te laag. In de QuickScan is DORA geclassificeerd als 'ondersteunend'. Echter kijkend naar de definitie van het proces, zoals eerder aangegeven, dan kan het proces niet worden uitgevoerd zonder dit systeem. 'Vitaal' zou daarom een passendere classificatie zijn voor het systeem.
- De procesbeschrijving van het Donorregister is in de QuickScan niet consistent gedefinieerd. Het loopt uiteen van "het beheren van register…" tot het "beheren van beleid over etc. (donorschap)".
- Conclusie van de QuickScan onderdeel BIO niet aangetroffen.
  Binnen BIO zijn er meerdere basis beveiligingsniveaus (BBN1 tot en met BBN3) onderscheiden. BBN2 en BBN3 kennen verbijzonderde maatregelen t.a.v. een lager niveau. Het toe te passen BBN is een resultante van de risicoanalyse i.c. QuickScan. In de QuickScan is niet aangegeven welk BBN passend is voor het Donorregister.

2.1.5 *DPIA bevat zowel risico's als maatregelen*

In de DPIA zijn naast de risico's ook maatregelen opgenomen. Voor de beheersing van de maatregelen is deze aanpak niet overzichtelijk.

3 Het IB-plan is gebaseerd op BBN2 en de maatregelen zijn niet volledig, voor AVG-maatregelen ontbreekt een dergelijk plan

Onderzoeksvraag 2:

Zijn onderkende risico's geagendeerd en is zowel het van toepassing zijnde niveau van de BIO en als de van toepassing zijnde AVG regelgeving vastgesteld?

Zijn de daartoe behorende maatregelen opgenomen in het IB-plan of elders belegd en/of is eventueel aangegeven de onderkende risico's te aanvaarden door daartoe bevoegde functionarissen?

3.1 IB-plan gaat uit van het Basisbeveiligingsniveau 2 (BBN2)

Het ontvangen IB-plan is 10 maart 2021 vastgesteld en goedgekeurd door Afdelingshoofd RK3 en Directeur CIBG. Aangegeven is dat: *Dit plan is gebaseerd op de QuickScan informatiebeveiliging (risicoanalyse) die op 30 juni 2020 door de externe opdrachtgever GMT is vastgesteld, alsmede op de eisen die in het kader van de BIO aan producten met een risicowaardering BBN 2 worden gesteld.* Dit laatste hebben wij in de QuickScan niet aangetroffen. Tevens is aangegeven dat voor de hoge eis aan beschikbaarheid, die door Nederlandse Transplantatie Stichting (NTS) wordt gesteld aan het donorregister, extra maatregelen moeten worden getroffen. In het IB-plan is geen expliciete verwijzing naar de uitgevoerde DPIA.

3.1.1 *IB-plan bevat aanvullende onderdelen van de risicoanalyse*

Het IB-plan bevat een verzameling van maatregelen, die ervoor zorgt dat het gewenste beveiligingsniveau in opzet wordt gewaarborgd. In het actuele IB-plan hebben wij een inventarisatie aangetroffen van meerdere processen en proceseisen met bijbehorende informatiesystemen in relatie tot het donorregister. De procesanalyse lijkt voor een deel te overlappen met de QuickScan. Het IB-plan sluit daarom op punten niet aan op het IB-beleid.

3.1.2 *Aanvullende risicoanalyse in IB-plan is niet volledig*

De risicoanalyse Quickscan bevat een aantal processen. Wij constateren dat in het IB-plan een soort aanvulling op de risicoanalyse wordt gegeven waarin een opsomming van diensten en producten en wetgeving wordt gegeven. Het valt op dat niet alle processen en producten zijn opgenomen in deze opsomming. Voorbeelden zijn 'het proces informatie aanleveren aan CBS' en 'het product ingevuld retour formulier'.

3.1.3 *Maatregelen zijn niet volledig geïnventariseerd*

In hoofdstuk 5 van het IB-plan wordt verwezen naar "De genomen en nog te nemen maatregelen". Daartoe is een bijlage opgenomen zijnde "20210215 Concretisering IB-plan vs 1.00". Dit overzicht is niet volledig.

- Maatregelen die voortvloeien uit wettelijke kaders zijn niet geïnventariseerd en uitgewerkt. Wettelijke kaders worden genoemd, maar er is niet aangegeven tot welke maatregelen die leiden. Archiefwet wordt bijvoorbeeld vermeld maar er is niet aangegeven welke specifieke regels daarvan van toepassing zijn voor het Donorregister en met welke maatregelen daaraan invulling wordt gegeven.
- Maatregelen die voortvloeien uit de inventarisatie van de producteisen zijn niet aangegeven.
- Niet alle maatregelen van BBN2 zijn opgenomen en uitgewerkt. CIBG geeft aan dat dat komt omdat de verantwoordelijkheden voor de betreffende maatregelen elders zijn belegd. Ondanks dat de maatregelen elders binnen CIBG zijn belegd zal het Donorregister zich ervan moeten vergewissen dat deze maatregelen daadwerkelijk worden uitgevoerd conform verwachtingen.
- Voorts zijn niet alle maatregelen herkenbaar geïnventariseerd voor de onderkende bedrijfsmiddelen van het Donorregister. Zie hiervoor de paragraaf over "Autorisatie".

3.2 Maatregelen uit DPIA zijn niet in IB-plan of elders bijeengebracht

3.2.1 *Maatregelen uit DPIA waren reeds geïmplementeerd in het proces*

CIBG geeft aan dat de meeste maatregelen bij vaststelling (van de DPIA) al waren geïmplementeerd in het proces. CIBG heeft de herleidbaarheid van de maatregelen naar het proces niet inzichtelijk gemaakt. Het afdelingshoofd is vanuit de lijn verantwoordelijk voor het implementeren van maatregelen vanuit de DPIA.

3.2.2 *IB-plan refereert niet aan DPIA en er is ook geen Privacyplan Donorregister*

In het IB-plan wordt niet (inhoudelijk) gerefereerd aan de risicoanalyse die in het kader van de verwerking van de persoonsgegevens in het Donorregister (DPIA) is uitgevoerd. Er wordt slechts aandacht besteed aan Verwerkersovereenkomsten en summier aan enkele elementen in hoofdstuk 5 bij 'genomen maatregelen'.
CIBG kent geen specifiek Privacyplan Donorregister en heeft de maatregelen dus niet in een separaat Privacyplan opgenomen waarmee de basis zou zijn gelegd voor een ordelijke en controleerbare administratie.

4 Vertaling van maatregelen (uit IB Plan/DPIA) naar procedures is weinig tot niet inzichtelijk, procedures vertonen op inhoud en beheersing tekortkomingen

Onderzoeksvraag 3: *Zijn de in het IB-plan vermelde maatregelen vertaald naar handreikingen, procedures, werkwijzen/instructies ten behoeve van de uitvoering en 'in control zijn' (teneinde toezicht en naleving mogelijk te maken)?*

4.1 Maatregelen uit de DPIA zijn niet eenvoudig herleidbaar naar vindplaatsen waarin zij hun weerslag hebben gekregen

De maatregelen in het kader van de uitgevoerde DPIA zijn rechtstreeks in het proces geïmplementeerd. CIBG heeft een Handleiding DORA voor het primaire werkproces (20 december 2020), een Solution Architecture Document (juni 2021) waarin de zes hoofdprocessen van het proces Actieve Donor Registratie staan vermeld, waaronder het verwijderen van donorregistratie. Andere maatregelen vanuit de DPIA zijn gerelateerd aan het voorlichtingsmateriaal op de website van VWS. Ook heeft CIBG, gebruik gemaakt van teksten die – bij navraag – afkomstig bleken uit de DPIA van NTS, die de ADR niet heeft ingezien.

4.2 Documentatie van maatregelen genoemd in het IB-plan niet geheel op orde

In paragraaf 2.1.3 is reeds aangegeven dat niet alle maatregelen zijn geïnventariseerd. Bij de maatregelen die wel onderkend zijn, zijn de aan te brengen verbeteringen hieronder toegelicht.

4.2.1 *Verwijzingen, aansluitingen en versie beheer niet op orde*

De verwijzingen in documenten zijn niet altijd goed te volgen. In een aantal gevallen hebben de processen of documenten waarnaar verwezen wordt een andere naam. Een voorbeeld hiervan is de verwijzing naar "procedure Security incidenten" terwijl wij een document hebben ontvangen waarop staat "IB-incidenten". Dit kan verwarrend zijn en kan ertoe leiden dat er meerdere versies van documenten zijn opgesteld die hetzelfde beschrijven.
Beleid en werkinstructies sluiten niet altijd op elkaar aan. Voorbeeld hiervan is dat het beleid maandelijkse controle op autorisaties aangeeft, terwijl de werkinstructie deze ieder kwartaal voorschrijft.
In het IB-plan wordt de actor 'eigenaar' gebruikt, maar het is niet duidelijk welke eigenaar bedoeld wordt. Dit zou zowel GMT of de proceseigenaar i.c. Afdelingshoofd kunnen zijn. In het kader van verantwoordelijkheden is het van belang dat duidelijk is welke functionaris daadwerkelijk bedoeld wordt.
Voorts wordt niet altijd naar een bepaald versie nummer van een document verwezen of wordt verwezen naar 'vigerende' versie. Wanneer documenten waarnaar verwezen wordt, veranderen, kan dit ertoe leiden dat de documenten niet meer goed op elkaar aansluiten. Bij nieuwe versies moeten gerelateerde documenten beoordeeld worden of deze ook aangepast moeten worden.

4.2.2 *Onderhoudbaarheid documentatie lastig door overlappingen*

In verschillende documenten is een overlap aangetroffen met andere documenten. Dit is niet wenselijk. Wanneer een wijziging optreedt, zal deze in meerdere documenten moeten worden verwerkt. Voorbeeld hiervan is een paragraaf (uitgangspunten) met algemene uitgangspunten over informatiebeveiliging in het continuïteitsplan. Deze uitgangspunten passen meer in het beleidsstuk informatiebeveiliging.

4.2.3 *Verantwoordelijkheid versiebeheer documentatie niet belegd*

Voor veel documenten is niet duidelijk wanneer deze periodiek geëvalueerd dan wel door omstandigheden aangepast moeten worden. Ook is niet duidelijk wie verantwoordelijk is voor dergelijke evaluaties en aanpassingen en wie erop toeziet dat dit daadwerkelijk gebeurt. We hebben meerdere 'actuele' documenten ontvangen, die meer dan twee jaar oud zijn.

4.2.4 *Relatie met CIBG brede processen niet inzichtelijk*

In een aantal gevallen wordt verwezen naar CIBG brede processen. Hiervan is niet altijd duidelijk wie hiervoor verantwoordelijk is. Ondanks dat dergelijke processen centraal worden uitgevoerd zal het Donorregister zich ervan moeten vergewissen dat deze processen worden uitgevoerd zoals verwacht. Ook zal bij de proceshouders bekend moeten zijn dat het Donorregister 'steunt' op/gebruik maakt van deze dienstverlening. Zodat bij veranderingen de juiste proceshouders en verantwoordelijken worden geïnformeerd.

4.2.5 *Rollen en verantwoordelijkheden niet geheel inzichtelijk*

Binnen het donorregister zijn diverse rollen onderkend. Volgens het IB-Beleid is het afdelingshoofd van RK 3 lijnverantwoordelijk ("accountable") voor het borgen van informatieveiligheid. Voor het product Donorregister is de productmanager eerste aanspreekpunt ("responsible"). Het is niet duidelijk wie verantwoordelijk is voor het actueel houden van de risicoanalyses en het uitvoeren daarvan en bijvoorbeeld het afsluiten van de Dossier Afspraken en Procedures (DAP) en het vaststellen van documenten zoals procedures en werkinstructies.

Voorbeelden zijn de DAP met de Belastingdienst voor print en mail, die is ondertekend door 'het afdelingshoofd RK3'. De verwerkersovereenkomsten met Belastingdienst Heerlen en Apeldoorn zijn ondertekend door 'afdelingshoofd R&K3'. De verwerkersovereenkomsten met zowel KPN als T&T en de raamovereenkomst met KPN en de nadere overeenkomst zijn ondertekend door de algemeen directeur Agentschap CIBG. De SLA met KPN is in maart ondertekend door Directeur Informatiemanagement/CIO. Ondanks dat functionarissen bevoegd zijn, is niet altijd inzichtelijk waarom juist deze functionarissen en niet andere functionarissen betreffende stukken ondertekenen. Wij adviseren hierover duidelijkheid te scheppen in het IB-Beleid.

4.3 Verwerkersovereenkomsten-/afspraken in het IB-plan aangetroffen

In het IB-plan staan (binnen par. 3.7 'het Afsprakenstelsel') voor vijf verwerkers verwerkersovereenkomsten-/afspraken vermeld. Het gaat om T&T, Belastingdiensten Apeldoorn en Heerlen, KPN en ATOS.

4.3.1 *Volledigheid van (af te sluiten) verwerkersovereenkomsten niet door CIBG vastgesteld.*

CIBG heeft geen document waaruit blijkt dat de volledigheid van de benodigde verwerkersovereenkomsten-/afspraken is vastgesteld. Volgens CIBG zijn alle verwerkers in beeld. CIBG kent nog geen verwerkersovereenkomst met Reisswolf en de Interdepartementale Post- en Koeriersdienst (IPKD). CIBG is in overleg met VWS kerndepartement over de vraag of dit een Rijksbreed contract is of dat elke organisatie individueel een contract moet afsluiten.

4.3.2 *IB-plan kende geen juiste weergave voor de samenwerking met DocDirekt*

Tussen DocDirekt en CIBG bestaat een 'Klantcontract Beheer' uit 2012. In het IB-plan van september 2020 stond nog geen verwerkersovereenkomst voor DocDirekt opgenomen, ondanks dat deze al had moeten bestaan. De verwerkersovereenkomst 'Verwerking van Persoonsgegevens' is in maart 2021 door beide partijen ondertekend. Op 30 juni 2021 informeert DocDirekt CIBG middels een Kennisgeving van vernietiging voor het Donorarchief 2010-2020. CIBG heeft aangegeven dat de samenwerking met DocDirekt inmiddels is beëindigd.

4.3.3 *Samenwerking met ATOS is inmiddels beëindigd maar staat nog in IB-plan.*

In IB-plan wordt ATOS genoemd met een verwerkersovereenkomst, maar inmiddels is de samenwerking beëindigd.

4.4 Interne beheersingsmaatregelen (PDCA) verdienen nog aandacht

De ADR heeft inzicht gezocht in het huidige systeem van toezicht en controle bij CIBG opdat leren en verbeteren cyclisch plaats kan vinden. Toezicht en controle hebben betrekking op de (interne) leveranciers maar ook op de beheersmaatregelen van het Donorregister zelf. CIBG geeft zelf aan dat er nog geen proces bestaat, waarin de rollen en verantwoordelijkheden zijn vastgelegd t.a.v. monitoring van de voorgestelde maatregelen. Als onderdeel van het IB programma wordt een ISMS ingericht waarin dit wordt geregeld.

4.4.1 *Jaarlijkse verklaringen in gevolge van verwerkersafspraken ontbreken m.u.v. KPN*

Art. 11.1/11.2 stelt dat de Verwerker jaarlijks aan de Verwerkingsverantwoordelijk een verklaring van een auditor overlegt waaruit blijkt of zij voldoet aan de (in art. 5) ten uitvoer gelegde maatregelen voor informatieveiligheid, aan de hand waarvan partijen de getroffen maatregelen evalueren die in Bijl. 2 zijn opgenomen en passen deze zo nodig aan.

CIBG heeft aangegeven dat deze verklaringen nog niet jaarlijks worden ontvangen en dat het intern onduidelijk is wie bij CIBG b.v. een Third Party Mededeling (TPM) moet opvragen en hier vervolgens verder actie op moet ondernemen.

Volgens CIBG wordt de dienstverlening door KPN, gemonitord en volgt jaarlijks een audit. Issues uit de rapportage worden besproken en gevolgd en afwijkingen worden wederom gemonitord. In de ontvangen documentatie van CIBG is niet aangetroffen op welke wijze en door wie de opvolging op eventuele bevindingen is vormgegeven. Idealiter is er voorzien in een proces waarin een inschatting wordt gemaakt van de risico's die samenhangen met eventuele bevindingen in de audit van KPN. Dit geldt natuurlijk ook voor opvolging van overige onderzoeken bij andere leveranciers.

CIBG heeft gemotiveerd waarom KPN wel wordt gevraagd naar de jaarlijkse verklaring: KPN is een private organisatie en is niet zoals publieke diensten, verplicht aan de BIO gecommitteerd. Dit argument zou dan ook voor T&T gelden, maar van T&T wordt geen verklaring gevraagd. Ook beide entiteiten van de Belastingdienst Heerlen en Apeldoorn hebben geen verklaring geleverd.

4.4.2 *Proef ICV van september 2020 volgt niet Privacy Governance van VWS*

CIBG ressorteert voor AVG onder de Privacy Governance van VWS. Hierin staat dat jaarlijks een uitvraag wordt gedaan - gebaseerd op een self-assessment met daarin KPI's privacy m.b.t. het Privacy Beleid VWS - naar de stand van zaken op het gebied van privacy. Self-assessments zijn onderdeel van de Informatiebeveiliging en worden gebundeld en onderdeel van de jaarlijkse rapportage die de CIO naar de concernleiding stuurt. In de Proef ICV (3 september 2020) van CISO CIBG aan CISO VWS staat dat de ICV zich richt op informatieveiligheid: "het stelsel van beveiligingsmaatregelen inzake onder meer: bescherming van persoonsgegevens conform de AVG, valt niet onder de proef ICV".

4.4.3 *De inhoud van de ICV (gerelateerd aan de VIR) is minder vergaand BIO-richtlijn*

De proef ICV is gebaseerd op het VIR. Het VIR schrijft een beperkt aantal basisregels voor. Het VIR is een kaderstellend voorschrift, dat veel overlaat aan de verantwoordelijke beheerders zelf. Het voorschrift stelt minimumeisen aan het te ontwikkelen beveiligingsbeleid binnen een ministerie. CIBG heeft aangegeven dat de hele Governance inclusief Audits nog verder vorm moeten krijgen. Dan zal ook opnieuw worden gekeken naar de inhoud van documenten die de stand van zaken weergeven.

4.4.4 *Doorgroei van In Control Verklaring (ICV) naar Informatiebeveiligingsbeeld (IBB) biedt CIBG de uitdaging tot een meer integrale aanpak van BIO en AVG*

Op 21 juli 2020 is door de ICBR vastgesteld om het IBB-beeld **vanaf 2022** te gebruiken in plaats van de ICV-IB. In 2021 bestaat nog de keuze tussen beiden.

Het IBB-beeld beoogt een breder en realistischer beeld van de status van informatiebeveiliging en betere integratie met bestaande P&C-processen. Het IBB-beeld is een instrument en werkwijze voor (2e lijns) advisering van de CISO aan verantwoordelijk management ten behoeve van sturing op IB. Het is nadrukkelijk geen instrument voor (3e lijns) toezicht.

Vanuit een evaluatie is onder meer naar voren gekomen dat IBB meer ruimte schept voor onderwerpen buiten het kader van de BIO, zoals Privacybescherming, Capaciteitsvraagstukken, Kennisbehoefte en Betrouwbaarheidscriteria. Door een breder perspectief (belangen, risico's en maatregelen) is de IBB meer risicogericht i.p.v. compliance gericht. Op het niveau van dienstonderdelen (directies, uitvoeringsorganisaties) kan ook een IBB-beeld worden gemaakt. Het departementale IBB-beeld kan dan worden opgesteld o.b.v. deze deelbeelden.

Deze ontwikkeling biedt CIBG meer perspectief en ruimte op verbetering bij een meer integrale aanpak op het gebied van de BIO en AVG gezien de onderlinge interdependenties en de eisen en wensen die per 2022 zijn opgenomen voor het Informatiebeveiligingsbeeld.

4.5 CIBG onderzoekt zelf Informatieveiligheid Donorregister

In Februari 2021 heeft CIBG intern het onderzoeksrapport "Eerste Vervolgonderzoek Informatieveiligheid Donorregister" opgesteld, nadat de algemeen directeur december 2020 aan het afdelingshoofd RK3 had gevraagd om een actueel beeld van de beheersing van informatieveiligheid van het nieuwe donorregister. De onderzoeksbevindingen leveren ook informatie voor het Programma Door-ontwikkeling Informatie CIBG, dat juni 2021 in concept stadium verkeert. In de laatste fase van ons onderzoek is dit onderzoeksrapport aan ons ter beschikking gesteld.

Het onderzoek is voor CIBG zeer bruikbaar en geeft duidelijk aan op welke punten CIBG zelf tekortkomingen ziet. Wij hebben het rapport niet op alle punten kunnen verifiëren en gedurende ons onderzoek is CIBG reeds met verbeteringen bezig waardoor eerdere bevindingen uit dit interne onderzoek mogelijk al zijn opgelost. Voorts heeft CIBG aangegeven dat zij door het voorliggende onderzoek nog meer zicht krijgt op te nemen verbeteracties.

4.5.1 *CIBG constateert zelf aandachtspunten voor de interne beheersing*

Ten aanzien van informatiebeveiligingsbeoordelingen vermeldt het onderzoeksrapport van CIBG ten aanzien van controle op naleving van de maatregelen de volgende bevindingen:

- Het CIBG heeft geen Auditplan;
- Voor Donor vindt jaarlijks een verplichte DigiD assessment plaats maar er is geen sprake van een breed extern onderzoek voor Donor (scope DigiD audit is beperkt);
- Tenminste jaarlijks vindt een pentest (technische security test) op het Donorregister plaats.
- Er is gestart met een ISMS-project om de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze aantoonbaar af te dekken;
- Verantwoordelijkheden m.b.t. de naleving zijn niet toegewezen.

4.5.2 *CIBG constateert zelf aandachtspunten voor de beheersing van uitbestede werkzaamheden aan leveranciers*

CIBG heeft zelf geconcludeerd dat binnen de organisatie contract-/leveranciersmanagement nog verder vorm moet krijgen. Aandacht moet komen op de inkoopvoorbereiding, de risicoanalyse, de business case, de KPI's en de afhankelijkheid van leverancier (risico's/maatregelen). Daarbij dienen de verantwoordelijkheden m.b.t. leveranciersmanagement duidelijk worden belegd, initieel en bij wijzigingen. Een RACI-tabel is daarbij zinvol.

De PDCA-cyclus van leveranciers moet volgens CIBG verder worden ingericht. Jaarlijks evaluatie van de risicoanalyse, afspraken (uit de verwerkersovereenkomsten) moeten worden gecontroleerd.

4.6 Verbeteringen Autorisatie Donorregister

Voor informatiebeveiliging speelt toegang een belangrijke rol. Daarom hebben wij hier een aantal bevindingen die te maken hebben met autorisatie in deze paragraaf samengevoegd.

4.6.1 *Inventarisatie bedrijfsmiddelen onvolledig*

Uit het IB-plan blijkt dat niet alle bedrijfsmiddelen in kaart zijn gebracht. Voorbeelden van deze bedrijfsmiddelen zijn: de bedrijfsmiddelen die worden gebruikt voordat het databestand op het uitwisselportaal van CBS wordt geplaatst, acceptatie omgeving (die in nood als uitwijkvoorziening gebruikt kan worden), Bestandsportaal, DORA-Vita webservice en het uitwijkportaal.

4.6.2 *De opzet voor de controle op autorisaties is deels aangetroffen*

Naast het inventariseren van deze bedrijfsmiddelen is het passend dat, afhankelijk van de rol in het proces, controle op autorisaties plaatsvindt. Wij hebben de opzet voor de controle op autorisaties aangetroffen voor de volgende 'Donor applicaties': DORA, Reporting Services, Bestandsportaal en BRP bevraging GBA-V.
Uit de feitelijke controle hebben wij kunnen afleiden dat voor het scanportaal (beheerder_ scanportaal en behandelaar_scanportaal) en het printportaal autorisaties zijn uitgereikt aan medewerkers van de Belastingdienst. In het autorisatieformulier staat "Bestandsportaal" vermeld. CIBG geeft aan dat hiermee hetzelfde wordt bedoeld.

De inrichting van de controle op autorisaties op bijvoorbeeld het bestandsportaal (CBS), op het CBS-bestand na het draaien van het script, op het uitwijkportaal en op de acceptatie-omgeving, hebben wij niet aangetroffen.

4.6.3 *Wijze waarop autorisaties worden toegekend is niet inzichtelijk*

Voor toegang tot DORA wordt gebruik gemaakt van Identity Management (IDM). Het ontvangen autorisatie model IDM geeft een aantal applicaties weer, maar DORA is daarin niet genoemd. Hierdoor ontbreekt inzicht in hoe de rollen en autorisaties voor DORA daadwerkelijk worden verleend en welke waarborgen dit proces kent. Het is ons evenmin duidelijk hoe de toegang tot het bestandsportaal met de Belastingdienst is georganiseerd. Toepassing van IDM lijkt niet mogelijk omdat het gaat om medewerkers Belastingdienst. Het is ook niet duidelijk wie autorisaties hiervoor uitreikt en hoe controle op het uitgifte proces is ingeregeld.

4.6.4 *Diverse onduidelijkheden over de logging van DORA*

In de documentatie staat dat de toegang tot logging van het verstrekken van autorisatie tot DORA is in te zien door de technische beheerders. Wij hebben geen procedures of werkinstructies aangetroffen op welke wijze aan technisch beheerders toegang wordt gegeven. Er is geen duiding hoeveel technische beheerders er zijn en wie dit zijn (is dat de externe partij of zijn dat technische beheerders van CIBG?). Tevens is niet duidelijk op welke wijze deze logging is beschermd tegen muteren.

4.6.5 *Beveiligingsmaatregelen voor het CBS-bestand zijn onbekend*

Voor de levering van data uit het Donorregister aan het CBS wordt maandelijks automatisch een script uitgevoerd dat een databestand klaarzet. Vervolgens wordt het bestand, na handmatige aanpassing van de titel, via een beveiligde portal van het CBS overgedragen. CIBG geeft aan dat het bestand niet geëncrypt is. Het is ons niet duidelijk welke waarborgen voor de beveiliging van het databestand zijn getroffen voordat het wordt overgedragen aan het CBS, hoe bijvoorbeeld de toegang tot het databestand is georganiseerd.

4.6.6 *Policy autorisatie niet aantoonbaar nageleefd*

In de BIO Policy autorisatie uit 2020 staan de minimale verwachtingen ten aanzien van autorisatie beheer en beheersmaatregelen. Tevens wordt vermeld dat er explains opgesteld moeten worden wanneer een toepasselijke beheersmaatregel niet of onvoldoende wordt gerealiseerd. Wij hebben geen explains aangetroffen, tegelijkertijd zijn er voorbeelden dat niet aan alle maatregelen voldaan wordt.

Op een aantal punten hebben wij geconstateerd dat de policy niet wordt nageleefd. Voorbeelden zijn: Afwezigheid van een mandaatregister, het niet toepassen van need-to-know principe voor DORA voor functioneel beheerders vanwege inwerkperiodes, het gebruik van unnamed account voor BPR en de vastlegging, bescherming van logbestanden van gebruikers activiteiten.

4.6.7 *Meerdere documenten voor autorisatiebeheer in omloop*

Wij hebben een CIBG Procedure Autorisatiebeheer (dec 2013) ontvangen waarin staat dat de functioneel beheerder opdracht geeft aan applicatiebeheerders om autorisaties te verlenen. In het autorisatiebeheer document (2019) staat omschreven dat applicatie gemachtigden verantwoordelijk zijn voor de accounts, dit zijn de product owners. Uitzondering is afdeling FAD, coördinator Functioneel beheer is gemachtigd autorisaties aan te vragen voor de functioneel beheerders. Op de formulieren die nu gebruikt worden, zien wij dat de product owner deze ondertekent voorzover het niet gaat om autorisaties voor functioneel beheerders, dit is conform het document uit 2019.
Wij adviseren te evalueren hoe wenselijk het is dat functioneel beheerders hun eigen autorisaties beheren en of daar eventueel een controle op de logging voor het uitgeven voor autorisatie wenselijk is.

4.7 Applicatie DORA

4.7.1 *Onduidelijkheid over doel werkinstructie en handleiding voor DORA*

Er is zowel een werkinstructie als handleiding beschikbaar. Deze documenten lijken veel op elkaar en het is niet duidelijk wat de verschillen zijn. Het is niet aangegeven waarvoor de handleiding of de werkinstructie is geschreven. Dit kan verwarrend zijn. De handleiding is niet ondertekend en is opgesteld door Netcompany en in december 2020 voor het laatst bijgewerkt. De werkinstructie is door afdelingshoofd op 30-6-2020 ondertekend en de revisiehistorie laat zien dat het document in november 2020 voor het laatst is aangepast. Het is niet duidelijk of bij wijzigingen de documenten tegelijkertijd actueel worden gehouden.

4.7.2 *Kwaliteit van scan middels 'Nieuw werkvoorraad item aanmaken' onbekend*

In de handleiding staat "De werkvoorraad is de basis van waaruit inkomende donorformulieren en correspondentie kunnen worden afgehandeld. Deze inkomende documenten worden automatisch aan de werkvoorraad toegevoegd wanneer ze via de scanstraat (belastingdient) zijn ontvangen en verwerkt." Het bevreemdt ons dat volgens de werkinstructie van DORA een werkvoorraad aangemaakt kan worden in DORA op basis van documenten op een lokale schijf. Is de kwaliteit van scans geborgd nu ook volgens de werkinstructie werkvoorraad items in DORA aangemaakt kunnen worden?

4.7.3 *Gedefinieerde 4-ogen principe in DORA is niet gebruikelijk*

Er is een 4-ogen principe in DORA. De invulling van dit principe wijkt af van de verwachting bij een 4-ogen principe. In de inrichting van DORA is het mogelijk dat de laatste 2-ogen ongezien door anderen wijzigingen doorvoert. Volgens de reactie van CIBG wordt het vier-ogenprincipe alleen uitgezet na het doorlopen van 'de procedure'. Echter in de werkinstructie van DORA is bij de functionaliteit van het uitzetten van 4-ogenrpincipe niet aangegeven dat hiervoor een speciale aanvullende procedure geldt.

4.7.4 *Informatie is tegenstrijdig over bewaartermijnen binnen DORA*

In de handleiding is niet aangetroffen hoe de vernietiging van gegevens plaatsvindt. Het is wel opgenomen in het Solution Architecture Document (SAD). Hierin staat *Het donorregister haalt de persoonsgegevens op bij Basisregistratie Personen (BRP) en verwerkt deze in het systeem. Indien een ingezetene is overleden of de ingezetene is geëmigreerd, dan blijft deze ingezetene in het systeem volgens de gestelde wettelijke (bewaar)termijn van drie jaar en wordt daarna verwijderd (inclusief de registratie) uit het systeem. Bewaartermijn is niet configureerbaar*.
Uit een reactie van CIBG is vernomen dat dit pas gebeurt 10 jaar na overlijden c.q. emigratie. Mede gelet op de tekst dat de bewaartermijn drie jaar is en deze niet configureerbaar is, is het niet duidelijk welke waarborgen in dit proces, van automatisch verwijderen na tien jaar is ingericht. Het is ook niet bekend of deze registraties zijn meegekomen en herkenbaar zijn vanuit het vorige register. In reactie laat CIBG weten dat dit verouderde documentatie is, maar het een en ander nog zal verifiëren.

4.7.5 *Noodzaak van sommige invoervelden beperkt door automatische correctie*

De documenten worden verwerkt volgens een aantal verwerkingsregels. In enkele gevallen corrigeert het systeem bepaalde veldwaarden. Hierdoor is toch een geldige registratie mogelijk. Specificaties van de verwerkingsregels en de automatische correcties zijn beschreven in bijlage: “Handleiding DORA - v1.3 - Bijlage 1 - Automatische verwerking documenten”. Uit de bijlage blijkt dat de datum van ondertekening wel in beschouwing wordt genomen, maar altijd leidt tot een geldige registratie. Bij een afwijkende datumdagtekening wordt deze gevuld met datum ontvangst scanstraat.

4.8 Encryptie

In de documentatie staat dat de database van DORA is encrypt. Echter ondanks de policy van encryptie, zien wij geen waarborgen dat deze ook altijd op de data buiten de database wordt toegepast. Voorbeelden zijn het intern gebruik van USB-sticks (zonder vingerafdruk) bij de Belastingdienst en de tijdelijke opslag van het databestand voordat dit wordt uitgewisseld met CBS.

5 Aanbevelingen

5.1 Verbeteringen op meerdere aspecten nodig

In bovenstaande hoofdstukken staan de bevindingen gerapporteerd. In deze paragraaf geven we aanbevelingen om informatiebeveiliging en bescherming van persoonsgegevens te verbeteren.

5.1.1 *Actualiseer IB-beleid en integreer Privacy daarin*

Het vigerende IB-Beleid (2018) is op onderdelen verouderd en slechts heel beperkt informatief op AVG-thema's. Het vigerende Privacy Beleid (2018) is van VWS. CIBG heeft dit als concernonderdeel omarmt en wil een vertaling naar de eigen organisatie maken.
Informatiebeveiliging en Privacy zijn als thema's erg met elkaar verweven. Informatiebeveiliging gaat immers over de bescherming van alle soorten gegevens, en dus ook over persoonsgegevens. In de Privacy Governance van VWS staan verschillende samenwerkingsgremia vermeld tussen IB- en AVG-functionarissen op verschillende niveaus. In het kader van de In Control Verklaring (ICV) wordt gesproken over het integreren van beide rapportages waarmee de samenhang wordt benadrukt, er aandacht is voor onderlinge afhankelijkheden en meer efficiency in de uitvraag wordt bereikt (selfassessments). Deze onderlinge verbondenheid heeft een groeiende tendens; dit is mede te herleiden uit het Informatie Beveiligings Beeld dat ingaande jaar 2022 in werking treedt en de ICV opvolgt.

- *Het lijkt nu een goed momentum om nieuw Beleid 'Informatieveiligheid & Privacy' op te stellen waarbij de Informatiebeveiliging en Privacy thema's in samenhang worden beschouwd.*

In dat nieuwe 'gecombineerde' beleid dient, mede gezien de bevindingen in dit rapport, in elk geval aandacht te zijn voor:

- Taken, Verantwoordelijkheden en een coördinerende rol (voor beide thema's),
- evaluatie en geldigheidsduur van beleid, plan, risicoanalyses en procedures
- eigenaarschap (en back-ups) met betrekking tot systemen, processen, producten, gegevens en documenten (procedures, handleidingen, werkinstructies etc.),
- eigenaarschap van contracten, bijlagen, verwerkersovereenkomsten etc. met dienstenleveranciers en het inregelen van goed beheer (onderhoud/actualiteit) hiervan,
- externe verantwoording van dienstenleveranciers aan de verwerkingsverantwoordelijke,
- interne verantwoording
- kaders en randvoorwaarden bij uitvoering van risicoanalyses (Proces, Vorm, Inhoud)
- de nulmeting die CIBG zelf heeft uitgevoerd: 'Eerste Vervolgonderzoek Informatiebeveiliging Donor' geeft ook handvatten voor aanpassing van beleid.

5.1.2 *Verbeter het uitvoeren en documenteren van Risicoanalyse*

Het is gedurende het onderzoek gebleken dat er slechts deels kadering vanuit Beleid bestaat rond het vormgeven van risicoanalyses en de wijze waarop risicoanalyses uitvoering zouden moeten krijgen is niet door CIBG omschreven. Risicoanalyses werden - zo blijkt - vormgegeven langs de formats voor de QuickScan en voor de DPIA.

- *Wij bevelen aan om kaders en randvoorwaarden te stellen voor de wijze waarop CIBG het uitvoeren van een risicoanalyse voorschrijft.*

Activiteiten die het proces verbeteren zijn:

- Definiëren van de processtappen van de risicoanalyse. Denk hierbij aan risico-inventarisatie, -duiding, -analyse, -weging, -acceptatie of afdoening.
- Definiëren en beleggen van de Taken (b.v. organisator/eigenaar van het risicoproces), Rollen (b.v. facilitator en notulist) en Bevoegdheden (b.v. wie beslist over acceptatie of afdoening van risico's.).

Activiteiten die kunnen leiden tot een verbeterde inhoud van de risicoanalyse:

- beschrijven van de aanpak, denk aan genodigden,
- zorgen voor goede inbreng door een passend gezelschap uit te nodigen gezien het thema (diversiteit van vertegenwoordigers uit operationeel, tactisch en strategisch niveau, extern deskundige, externe leveranciers, ketenpartners 'out-of-the box denkers' etc.),
- zorgen dat de aanwezigen zich gecommitteerd voelen, vanuit verschillende belangen en perspectieven redeneren en elkaar serieus nemen: dus spelregels zijn belangrijk,
- vastleggen van hetgeen besproken in de verschillende fasen is belangrijk, om de uitkomsten te kunnen herleiden naar passende maatregelen en het collectief geheugen te borgen.

- *Analoog aan hetgeen hiervoor is aangereikt met betrekking tot een gecombineerd Beleid 'Informatieveiligheid & Privacy' zien wij gecombineerde risicosessies voor de thema's IB en AVG een natuurlijke consequentie voor verrijking van discussies, synergie-effect etc.*

5.1.3 *Neem alle relevante IB- en privacy maatregelen op in één plan*

Het Informatieveiligheidsplan Donorregister (IB-plan) is van maart 2021. Voor AVG/Privacy staan zowel de risico's als de maatregelen in de DPIA verwerkt. CIBG kent geen Privacy Plan voor het Donorregister.
In het IB-plan trof de ADR zowel risico's als maatregelen aan.

- *Wij bevelen aan om risico's buiten het IB-plan te houden en de maatregelen te duiden in het IB-plan.*

Bij gebrek aan een Privacy Plan voor het Donorregister is nog geen basis aangebracht voor een ordelijke en controleerbare administratie. Tevens ontbreekt inzicht in de samenhang van maatregelen en de onderlinge afhankelijkheden.

- *Wij bevelen aan een Privacy Plan voor het Donorregister op te stellen wat idealiter wordt gecombineerd met het IB-plan Donorregister en dus de resultante weerspiegelt van de maatregelen die zijn getroffen op grond van uitkomsten uit gecombineerde risicosessies (AVG en IB-vraagstukken).*

5.1.4 *Breng Procedures, Handleidingen, Werkinstructies op orde*

De ADR heeft in het onderzoek een veelheid van procedures, handleidingen, werkinstructies aangetroffen waarbij bevindingen waren op het gebied van overlappingen en onduidelijke verwijzingen tussen documenten,

- onduidelijkheid over verantwoordelijkheid voor versiebeheer documenten,
- onduidelijkheid over eigenaarschap van het document,
- onduidelijkheid tussen werkinstructie en CIBG brede processen niet inzichtelijk,
- onduidelijkheid over eigenaarschap van het beschreven proces,
- onduidelijk over waar geïmplementeerde maatregelen in het proces (AVG) zijn beschreven en terug te vinden,
- onduidelijkheid hoe autorisatiebeheer is ingericht voor alle bedrijfsmiddelen die een rol spelen bij het Donorregister,
- onduidelijkheid hoe encryptie is toegepast op de data bij het donorregister buiten de database,
- onduidelijk over ontvangst van een overeenkomst, daar waar samenwerking inmiddels niet meer aan de orde blijkt,
- status van het document wanneer na ondertekening nog aanpassingen hebben plaatsgevonden,
- screenshots van informatie op Intranet die verouderd blijkt.

> ➢ *Wij bevelen aan om meer Governance in de documentatie aan te brengen en een overzicht te hebben van de relaties tussen de documenten.*

Wat hierbij helpt is het in relatie brengen van het Beleid met de Risicoanalyse en met het IB-plan zoals hiervoor is geschetst. Taken die hiervoor van belang zijn, zijn

- het uitlijnen van de maatregelen uit het Plan naar actuele procedures en dit herleidbaar en inzichtelijk maken (Plan – Maatregel – Procedure),
- voortdurende inventarisatie van documenten (onderwerp/leeftijd document/eigenaar),
- coördinatie van de inhoud van de documenten vanuit een geïntegreerd gezichtspunt IB en AVG,
- het bewaken en coördineren van de samenhang tussen verschillende documenten,
- de geldigheidsduur van documenten aan maximale termijnen koppelen,
- bewaking van interne en externe ontwikkelingen die van invloed kunnen zijn op documentatie,
- feedback vragen aan de organisatie over gebruiksvriendelijkheid en effectiviteit/verbeteropties van de procedures,
- minimaal jaarlijkse evaluaties van documentatie inregelen en bewaken op naleving,
- leerpunten uit evaluatie verzamelen en implementeren daar waar van toepassing, verantwoordelijken voor deze taken moeten uiteraard expliciet worden gemaakt.

> ➢ *Aan verbetering en samenhang in deze situatie kan het onderhanden ISMS bijdragen.*

6 Verantwoording onderzoek

6.1 Onderzoeksobject en afbakening

Object van onderzoek zijn zowel de risicoanalyses als de plannen, procedures, handreikingen etc. die daaruit volgen, vanuit het perspectief van de BIO en de AVG, en gericht op het nieuwe Donorregister dat per juli 2020 in gebruik is genomen. Er zijn geen auditwerkzaamheden uitgevoerd bij IT-dienstleveranciers. De gemaakte afspraken tussen CIBG en dienstleveranciers zijn wel onderzocht. Het onderzoek is gestart in april 2021 en de definitief concept rapportage is 6 augustus ter beschikking gesteld aan CIBG. Op 2 september 2021 is de managementreactie van CIBG ontvangen en als bijlage opgenomen in het rapport.

Wat betreft afbakening ligt de focus - overeenkomstig de opdrachtbevestiging - op de *Opzet* van de maatregelen. Als duiding voor het onderscheid tussen Opzet, Bestaan en Werking het volgende:
Bij de *Opzet* onderzoeken we of documenten betreffende informatiebeveiliging zoals risicoanalyses, (IB-)plannen, procedures, handreikingen consistent zijn en op logische wijze samenhangen en op zichzelf aangeven wat de organisatie van plan is.
Bij *Bestaan* van de maatregelen wordt onderzocht of op een bepaald moment in de tijd de procedures werkinstructies, handreikingen etc. daadwerkelijk door de organisatie worden opgevolgd.
Bij de *Werking* van de maatregelen wordt onderzocht of de procedures, handreikingen etc. over een periode daadwerkelijk worden opgevolgd zoals bedoeld.

De keuze voor de Opzet is - uiteraard - gemaakt in afstemming met het CIBG. De aanleiding om het onderzoek in te richten vanuit de Opzet ligt in de management-reactie (januari 2021) van CIBG op het vorige ADR-onderzoek bij het CIGB. Hierin staat dat CIBG vanaf eind januari 2021 inzet op uitvoering van de maatregelen, het inregelen van controles en toezicht en bezig is met het verduidelijken van taken, rollen en verantwoordelijkheden. Dit zorgt ervoor dat onderzoek door de ADR naar het Bestaan van de maatregelen op het moment van de opdracht nog te vroeg was.

CIBG en de ADR hebben de potentiële scope van de opdracht diverse malen besproken en hebben besloten om het onderzoek vanuit een min of meer ‘iteratief proces’ te gaan vormgeven. Deze werkwijze kreeg als volgt vorm:
ADR heeft in twee memo’s tussentijdse bevindingen verwoord, waarna CIBG in de gelegenheid was om dit met de ADR te bespreken en inhoudelijk op de memo’s te reageren en indien van toepassing de ADR van aanvullende documentatie te voorzien. Dit werkproces vroeg van beide partijen intensieve aandacht, tijd en flexibiliteit. Deze voorwaarden zijn voorafgaand aan het onderzoek tussen partijen besproken.

6.2 Uitgevoerde werkzaamheden

Voor het uitvoeren van het onderzoek is door CIBG veel documentatie verstrekt. De documentatie bestond onder andere uit risicoanalyses, (IB-) plannen, verwerkersovereenkomsten, leveranciersafspraken, procesbeschrijvingen, systeembeschrijvingen en werkinstructies.

Zoals eerder aangegeven was de focus van het onderzoek afgebakend tot de Opzet van de maatregelen. In de onderzoekspraktijk bleek een strak onderscheid tussen opzet en bestaan soms lastig aan te brengen en een grijs gebied. Hierdoor is het gebeurd dat de ADR op sommige momenten ‘doorprikte’ van opzet naar bestaan.

6.3 Referentiekader

Het referentiekader voor deze opdracht betreft de ‘Baseline Informatiebeveiliging Overheid (BIO)’, versie 1.04 en de AVG.

6.4 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek 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.

6.5 Verspreiding rapport

De opdrachtgever, mevr. A.I. Norville MSc, plaatsvervangend SG van het ministerie van Volksgezondheid, Welzijn en Sport, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op www.rijksoverheid.nl.

7 Ondertekening

Den Haag, 2 september 2021

Auditmanager
Auditdienst Rijk

8 Bijlage 1: Managementreactie CIBG

CIBG
Ministerie van Volksgezondheid, Welzijn en Sport

Agentschap CIBG

Bezoekadres

Hoftoren - Rijnstraat 50
2515 XP Den Haag
T 070 340 54 87

Postadres

Postbus 16114
2500 BC Den Haag

www.cibg.nl
info@cibg.nl

Datum

2 september 2021

Managementreactie

Naar aanleiding van de moties van Kamerleden Dijkstra[1] en Van den Berg/Dijkstra[2] is de Audit Dienst Rijk (ADR) in het voorjaar van 2020 een onderzoek gestart naar de informatiebeveiliging van het Donorregister, dat per 1 juli 2020 is geïmplementeerd. Dit onderzoek is een vervolg op een eerder onderzoek naar de vermissing van twee harde schijven van het Donorregister in maart 2020.[3] Dit eerdere onderzoek met onze managementreactie daarop is op 4 maart 2021 door de minister van VWS met de Tweede Kamer gedeeld.

Het vervolgonderzoek van de ADR vond plaats in een periode waarin het CIBG bezig was met het doorvoeren van verbeteringen op gebied van informatiebeveiliging voor het Donorregister en de gehele organisatie. Vanwege de fase waarin het CIBG zich op dat moment bevond, heeft de ADR onderzoek gedaan naar de wijze waarop het CIBG de processen en procedures voor het Donorregister in documenten heeft beschreven.

De ADR heeft in haar vervolgonderzoek geconstateerd dat het CIBG diverse initiatieven heeft ondernomen om de informatiebeveiliging te verbeteren. Vanaf juni 2020 zijn de Quickscan, de Data Protection Impact Assessment (DPIA) en het Informatiebeveiligingsplan Donorregister bijgewerkt. De ADR constateert dat er nog verdere verbeteringen mogelijk zijn op het gebied van uitvoering en vastlegging van risicoanalyses en op het gebied van de beheersing van de maatregelen voor informatiebeveiliging en de bescherming van persoonsgegevens. Tevens ziet de ADR ruimte voor verbetering op het toezicht op informatiebeveiliging.

Het Donorregister is een belangrijk register voor alle burgers. De burger moet op ons kunnen vertrouwen als het gaat om zorgvuldige en goed beveiligde omgang met persoonsgegevens. Wij nemen de constateringen en aanbevelingen van de ADR daarom zeer serieus en hebben dit hoge prioriteit gegeven in ons meerjarenprogramma voor informatiebeveiliging en privacy. Onderdeel van dit programma is ook de implementatie van een Information Security Management System (ISMS) en de verdere inrichting van governance.

Tijdens het onderzoek van de ADR hebben we ook geconstateerd dat de grote hoeveelheid documenten waarin processen en procedures staan beschreven, een gefragmenteerd en complex beeld oplevert. We gaan daarom de komende tijd ook aan de slag om die complexiteit terug te brengen.

---

[1] Motie om onderzoek te doen naar de gehele informatiebeveiliging van het Donorregister bij het CIBG.

[2] Motie om onderzoek te doen naar de wijze waarop de informatiebeveiliging bij de huidige donorregistratie is georganiseerd.

[3] Onderzoekrapport Inventarisatie Maatregelen t.a.v. beheer externe gegevensdragers Donorregister (kenmerk 2020-0000228231)

We zien geen onoverkomelijke problemen om alle maatregelen volledig te implementeren en vooruitgang te maken, maar we hebben tijd nodig om dit op een gestructureerde wijze in de organisatie te borgen. Het integreren van informatiebeveiliging en privacy in onze plan-do-check-act-cyclus is hierbij een belangrijke stap. Zo kunnen we de plannen, procedures en processen regelmatig herijken en zorgen dat de uitvoering hiermee in lijn is. De ervaring met de ADR heeft ons geleerd dat een externe blik hierbij helpt. Daarom willen we jaarlijks een externe audit voor informatiebeveiliging van het Donorregister gaan invoeren. Als op termijn de nieuwe donorwet wordt geëvalueerd, zijn we ook voornemens om de informatiebeveiliging van het Donorregister daarbij mee te nemen.

Tot slot wil het CIBG haar waardering uitspreken voor de kritische en constructieve wijze waarop de ADR dit onderzoek heeft uitgevoerd. Dit heeft geleid tot een rapportage die ons veel handvatten biedt en zeer waardevol is voor de verdere vormgeving van onze informatiebeveiliging.

Namens de directie van het CIBG,

N.A. Laagland
Directeur CIBG

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