Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Inventarisatie maatregelen t.a.v. beheer externe gegevensdragers Donorregister

Definitief V1.1

Colofon

Titel	Inventarisatie maatregelen t.a.v. beheer externe gegevensdragers
Uitgebracht aan	mw. A.I. Norville pSG VWS
Datum	11 december 2020
Kenmerk	2020-0000228231

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Bij het vernietigen van het papieren archief van het Donorregister bleek dat twee externe harde schijven met daarop een back-up van 6,9 miljoen donorformulieren uit de periode 1998-2010, zich niet meer in de kluis bevonden, waar zij normaliter werden bewaard. Dit datalek is op 4 maart 2020 door CIBG ontdekt en op 6 maart gemeld bij de Autoriteit Persoonsgegevens. Het CIBG heeft de ADR gevraagd om een onafhankelijk onderzoek. Dit onderzoek richt zich op de door het CIBG gehanteerde werkwijze en procedures voor de omgang met externe gegevensdragers teneinde het CIBG via handelingsperspectief in staat te stellen om mogelijke verbeteringen door te voeren en daarmee het risico van herhaling te mitigeren. CIBG heeft dit onderzoek tevens aangekondigd aan de Minister voor Medische Zorg en de Minister van Volksgezondheid, Welzijn en Sport.

Actualiseer informatiebeveiligingsplan en maatregelen voor het Donorregister en zie toe op naleving

Dit onderzoek is uitgevoerd naar aanleiding van het zoekraken van twee externe harde schijven. Deze twee externe schijven bevatten 6,9 miljoen ingescande donorformulieren uit de periode 1998 tot 2010. Omdat de gegevens, die op de schijven stonden succesvol waren ingevoerd in het Donorregister, waren de schijven overbodig en konden zij, conform het vervangingsbesluit, vernietigd worden. Op het moment dat men de schijven wilde vernietigen, bleken ze niet meer in de gebruikelijke kluis te liggen. Hoewel er tot nu toe geen signalen zijn dat de gegevens in 'verkeerde handen' zijn gekomen, is deze vermissing op 6 maart 2020 door het CIBG direct als datalek gemeld. Tevens was dit voor VWS en CIBG ook aanleiding om dit onderzoek direct na de melding te laten uitvoeren.

Teneinde tot een handelingsperspectief te komen om herhaling te voorkomen zijn de volgende vragen in dit onderzoek beantwoord:
1. Zijn de door het CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevensdragers in overeenstemming met richtlijnen vanuit de toenmalige Baseline Informatiebeveiliging Rijksdienst (BIR) en zijn deze nageleefd in de periode vanaf de totstandkoming van de externe gegevensdragers tot nu?
2. Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?
3 Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?
4 Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?

Hierna worden per onderzoeksvraag de verworven inzichten en bevindingen toegelicht. Afsluitend is het handelingsperspectief beknopt beschreven. Voor nadere toelichting en onderbouwing wordt verwezen naar de verdere rapportage.

<u>1. Zijn de door het CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevensdragers in overeenstemming met richtlijnen vanuit de toenmalige BIR en zijn deze nageleefd in de periode vanaf de totstandkoming van de externe gegevensdragers tot nu?</u>

Voor de inventarisatie van bestaande relevante maatregelen voor de omgang met externe gegevensdragers is gebruik gemaakt van het beleid en bijbehorende informatiebeveiligingsplan. Tijdens het onderzoek bleek dat het geldende informatiebeveiligingsplan van het donorregister sinds 2011 niet meer is geactualiseerd (Tactisch Normenkader (TNK) 5.1.2). Hierdoor sloot het informatiebeveiligingsplan niet meer aan op de veranderingen die sinds 2011 hebben plaatsgevonden ten aanzien van (de omgeving van) het donorregister en het vernieuwde informatiebeveiligingsbeleid.

CIBG heeft tijdens het onderzoek aangegeven ook "geconstateerd te hebben dat het Informatie Beveiligingsplan voor het Donorregister niet is geactualiseerd op het moment dat de BIR 2012 van kracht werd. Dit was wel wenselijk geweest [1]"

Bedrijfsmiddelen
In het geldende informatiebeveiligingsplan was een inventarisatie gemaakt van bedrijfsmiddelen (TNK 7.1.1). Echter de bedrijfsmiddelen zoals externe gegevensdragers, zoals DVD's, USB-sticks en harde schijven, waren hierin niet opgenomen. In het plan zijn daardoor geen (verwijzingen naar) maatregelen, procedures en werkwijze aangetroffen voor externe gegevensdragers.

Procedures voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik waren niet volledig uitgewerkt (Procedures voor de behandeling van informatie (10.7.3)). Ten aanzien van het gebruik van kluizen is geen sleutelprotocol aangetroffen en is geen werkinstructie aangetroffen waardoor een actueel inzicht ontbrak aangaande wie in de kluis was geweest en wat er in de kluis behoorde te liggen.

Wij hebben in de praktijk voorbeelden gezien dat bedrijfsmiddelen, zoals DVD's en papieren archief veilig worden afgevoerd (TNK 9.2.6), maar deze maatregelen zijn niet beschreven en zijn niet verankerd in het informatiebeveiligingsplan. Daardoor is het niet geborgd dat dit altijd op deze wijze plaatsvindt.

Personeel
In de praktijk zijn maatregelen ten aanzien van beveiliging personeel wel aangetroffen, deze waren ook beschreven, maar deze waren niet verankerd in het geldende informatiebeveiligingsplan hierdoor zijn er minder waarborgen dat deze maatregelen structureel worden toegepast en actueel blijven. Dit betreft:

- maatregelen ten aanzien van personeel, zoals het afleggen van eed of belofte ondertekenen geheimhoudingsverklaring en beveiligingsbewustzijn (beveiliging Personeel TNK 8.1).

Externe partijen
In ons onderzoek hebben wij ook de aanwezigheid van maatregelen onderzocht in contracten en afspraken met externe partijen (TNK 6.2). In contracten en afspraken met externe partijen zijn vaak geen expliciete afspraken gemaakt over

- het melden van incidenten met betrekking tot vertrouwelijkheid,
- het verplicht stellen van een VOG voor het personeel van betreffende externe partij,
- de minimale beveiligingseisen voor vertrouwelijkheid, beschikbaarheid en integriteit,
- de wijze van eventueel gebruik van externe gegevensdragers,
- de wijze van uitwisseling van informatie,
- de wijze waarop informatie moet worden vernietigd.

Teneinde maatregelen voor de vertrouwelijkheid voor specifiek persoonsgegevens te inventariseren hebben we gebruik gemaakt van de eisen die hieraan gesteld worden vanuit de wet die toeziet op bescherming van persoonsgegevens (nu Algemene Verordening Gegevensbescherming (AVG) en tot 2018 Wet Bescherming Persoonsgegevens (WBP)). Bewerkersovereenkomsten, die verplicht waren voordat de AVG in 2018 in werking trad, zijn niet aangetroffen. Vanaf 2018 zijn verwerkersovereenkomsten aangetroffen. Tot 1 juli 2020 hebben we geconstateerd dat verwerkersovereenkomsten niet helemaal op orde waren, doordat een verouderd model was gebruikt of de datum van ondertekening ontbrak. Toezicht op de naleving van de afspraken met de verwerkers van persoonsgegevens gedurende en bij beëindiging van de overeenkomst hebben we niet aangetroffen.

[1] "Het huidige donorregister bestaat sinds 1998 en maakt nog steeds gebruik van dezelfde persoonsgegevens (zonder bijzondere kenmerken) en het proces van gegevensverwerking is ongewijzigd. Omdat de risico-classificatie1 (die is vastgesteld op II) door de jaren heen niet is veranderd, is de redenatie geweest dat er ook geen veranderingen nodig waren in het IB-plan voor het Donorregister."

Tot 1 juli 2020 was sprake van het 'oude' donorregister, het nieuwe donorregister is 1 juli 2020 gestart.
Onderzoeksvragen 2 tot en met 4 gaan over het nieuwe donorregister.
Tijdens ons onderzoek was het nieuwe donorregister nog niet in werking. Wij hebben daardoor alleen de aanwezigheid van de *opzet* (beschrijving) van de maatregelen voor vertrouwelijkheid van het nieuwe donorregister in beschouwing genomen.

2. Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?

Tijdens het onderzoek is geen actuele risico- analyse en geen actueel informatiebeveiligingsplan voor het nieuwe Donorregister aangetroffen (TNK 5.1.2 / Baseline Informatiebeveiliging Overheid (BIO) 5.1.1). Ook de inventarisatie van bedrijfsmiddelen is niet aangetroffen (TNK 7.1.1 / BIO 8.1.3).

In reactie op het concept rapport laat CIBG zien dat er op 2 juli 2020 een nieuwe quickscan is vastgesteld. De vertrouwelijkheidseis is daarin op 'hoog' aangegeven (op een schaal van laag. midden, hoog en zeer hoog). Tevens is in deze quickscan bepaald dat voor vertrouwelijkheid het standaard niveau van beveiliging, zoals dat binnen de overheid geldt, afdoende is.

3) Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?

De inventarisatie van bedrijfsmiddelen is van belang omdat het dan inzichtelijk is welke bedrijfsmiddelen aanwezig zijn om deze vervolgens de juiste bescherming te bieden. De inventarisatie van bedrijfsmiddelen hebben wij niet aangetroffen. Op basis van beschikbare documentatie hebben we een groot aantal bedrijfsmiddelen kunnen inventariseren, deze staan opgesomd in paragraaf 3.3.

4.) Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?

Een informatiebeveiligingsplan voor het nieuwe donorregister is niet aangetroffen. We hebben niet voor alle door ons geïnventariseerde bedrijfsmiddelen specifieke maatregelen aangetroffen. Voor het nieuwe donorsysteem zelf zijn wel maatregelen, die bijdragen aan de vertrouwelijkheid aangetroffen. Voorbeelden zijn de maatregelen in de Project Start Architectuur met daarin verwijzing naar het toepassen dan database encryptie, de Secure Software Development documentatie, het uitvoeren van toetsen en de opzet van de inrichting van de autorisaties van het nieuwe systeem. Maatregelen in contracten en afspraken met externe partijen zijn niet altijd aangetroffen, zie hiervoor ook de beantwoording bij vraag 1.

Handelingsperspectief

ADR adviseert op basis van de bevindingen om een geactualiseerd informatiebeveiligingsplan voor het donorregister op te stellen; houd daarbij rekening met *alle* (nog) aanwezige bedrijfsmiddelen i.c. zowel het oude systeem als het nieuwe systeem. De actualiteit van de inventarisatie van bedrijfsmiddelen is daarbij van groot belang zodat voorkomen wordt dat er bedrijfsmiddelen c.q. gegevensdragers 'vergeten' worden. Het informatiebeveiligingsplan is van belang omdat hierin alle (verwijzingen naar) (te treffen) maatregelen bijeen worden gebracht om op het juiste niveau bescherming te kunnen blijven waarborgen. Belangrijk is om dit plan bij veranderingen, maar zeker minimaal jaarlijks, te reviewen en te actualiseren.
Daarnaast zal ook controle moeten plaatsvinden op de werkelijke uitvoering van de maatregelen in de praktijk ten einde vast te stellen of deze dusdanige bescherming bieden zoals in het informatiebeveiligingsplan bedoeld is. Houd bij het opstellen van het informatiebeveiligingsplan rekening met de bevindingen, die in dit onderzoek naar voren zijn gekomen, zoals is aangegeven in paragraaf 4.1.

Rekening houdend met de vereisten vanuit AVG adviseert ADR om:

- uniformiteit van persoonsgegevens te bewaken in de verschillende afspraken en verwerkersovereenkomsten,
- toegang tot persoonsgegevens blijvend te monitoren,
- (potentiële) verwerkersovereenkomsten te inventariseren en te actualiseren,
- bewaartermijnen voor de papieren registratieformulieren te implementeren,
- Privacy Impact Analyse (PIA)-review onderdeel te maken van het changeproces,
- thema datalekken blijvend onder de aandacht te houden,
- toe te zien op naleving op afspraken van verwerking persoonsgegevens bij gegevensverwerkende partijen zowel gedurende de overeenkomst als bij de beëindiging daarvan.

1 Inleiding en doelstelling onderzoek

Het CIBG heeft de ADR gevraagd om een onafhankelijk onderzoek. Dit richt zich op de door het CIBG gehanteerde werkwijze en procedures voor de omgang met externe gegevensdragers teneinde het CIBG via handelingsperspectief in staat te stellen om mogelijke verbeteringen door te voeren en daarmee het risico van herhaling te mitigeren.
Dit onderzoek richt zich voornamelijk op de *vertrouwelijkheid* van de data die op externe gegevensdragers is opgeslagen. Het richt zich op de maatregelen die moeten voorkomen dat zwakheden in het gebruik van externe gegevensdragers worden uitgenut. Op basis van de casus van de zoekgeraakte externe gegevensdragers van het Donorregister zijn de gehanteerde werkwijze en procedures geïnventariseerd. Aan de hand van Baseline Informatiebeveiliging Rijksdienst (BIR) zoals die gold tijdens de casus van de twee externe harde schijven, is nagegaan of de informatie uit de procedures en werkwijzen, passende maatregelen kennen (opzet) en of deze worden nageleefd (bestaan).
Voorts is geïnventariseerd welke eisen aan vertrouwelijkheid van het nieuwe donorregister zijn gesteld en op welke wijze (in opzet) hieraan invulling is gegeven.

Het onderzoek is verwoord in de Onderzoeksopdracht die op 9 april 2020 door de pSG van VWS is ondertekend. CIBG heeft dit onderzoek tevens aangekondigd aan de Minister voor Medische Zorg en de Minister van Volksgezondheid, Welzijn en Sport.

De volgende vragen zijn in dit rapport beantwoord:

1. Zijn de door het CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevensdragers in overeenstemming met de richtlijnen vanuit de toenmalige BIR en zijn deze nageleefd in de periode vanaf de totstandkoming van de externe gegevensdragers tot nu toe?
2. Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?
3. Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?
4. Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?

De onderzoeksperiode is gedefinieerd van 2012 tot 1 juli 2020. De eerste vraag heeft vooral betrekking op de situatie zoals van het donorregister tot 1 juli 2020 en wordt beantwoord in hoofdstuk 2.
De overige vragen hebben betrekking op het nieuwe donorregister en worden beantwoord worden in hoofdstuk 3. Op de vermiste harde schijven stonden persoonsgegevens daarom hebben wij in dit onderzoek ook de maatregelen die verwacht worden vanuit de Algemene Verordening Gegevensbescherming (AVG) in beschouwing genomen. De resultaten hiervan zijn opgenomen in hoofdstuk 4, in bijlage 1 is de uitgebreide analyse terug te vinden.

2 Procedures en maatregelen voor externe gegevensdragers

2.1 Inleiding

Dit hoofdstuk geeft antwoord op vraag 1: Zijn de door het CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevensdragers in overeenstemming met de richtlijnen vanuit de toenmalige BIR en zijn deze nageleefd in de periode vanaf de totstandkoming van de externe gegevensdragers tot nu toe?

BIR en TNK
Vanuit een informatiebeveiligingsbeleid worden voor de organisatie de lijnen uitgezet voor informatiebeveiliging. Ten aanzien van het operationaliseren van het beleid worden risicoanalyses uitgevoerd om later de benodigde maatregelen te inventariseren. Om tot de maatregelen te komen, hebben wij dit bekeken vanuit de kaders van het beleid om vervolgens naar concrete maatregelen te komen.

Ten einde antwoord te geven op vraag 1 is een aantal maatregelen uit Tactisch Normenkader(TNK) behorend bij de Baseline Informatiebeveiliging Rijksdienst (BIR) geselecteerd.
De volgende maatregelen zijn van toepassing:

Organisatie van beveiliging (TNK 5).
Beheer bedrijfsmiddelen (TNK 7)

- Eigendom van bedrijfsmiddelen (TNK 7.1.2)
- Classificatie van informatie (TNK 7.2) waaronder
  - Informatie wordt door de eigenaar geclassificeerd met betrekking tot waarde, wettelijke eisen, vertrouwelijkheid en onmisbaarheid in het proces (7.2.1).

Beveiliging van Personeel (TNK 8)

- Vaste medewerkers leggen bij het in dienst treden een eed of belofte af en ondertekenen eventueel een geheimhoudingsverklaring (8.1.3.1)
- Externe partijen dragen zorg voor een geheimhoudingsverklaring en verklaring omtrent gedrag (VOG) (8.1.3.2).
- De lijnmanager zorgt er voor dat medewerkers op de hoogte zijn van de beveiligingsmaatregelen en zich er aan houden (8.2.1).
- Beveiligingsbewustzijn wordt bevorderd door regelmatig aandacht aan de beveiliging te schenken (8.2.2).

Fysieke beveiliging en beveiliging van de omgeving (9)

- Apparatuur met opslagmedia die buitengebruik is gesteld of die hergebruikt wordt, is geschoond van informatie en / of software (9.2.6)

Beheer van communicatie en bedieningsprocessen (TNK 10)

- Back-up (10.5)
  - Er zijn adequate back-up en restore procedures, die periodiek getest worden. Naast de WBP stelt de archiefwet en het Archiefbesluit eisen aan de bewaartermijn van informatie (10.5.1)
- Procedures voor het behandelen van informatie (10.7)
  - Informatie wordt in overeenstemming met de archiefwet en archiefbesluit bewaard (10.7.3.2).
  - Beheer van verwijderbare media (10.7.1)
  - Verwijdering van media (10.7.2)

  Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Externe partijen (TNK 6.2)

- In contracten met externe partijen is vastgelegd op welke manier beveiligingsincidenten moeten worden gemeld en op welke manier deze door de externe partij en het CIBG worden behandeld. (6.2.3.2)

Maatregelen personeel

- Externe partijen dragen zorg voor een geheimhoudingsverklaring en een verklaring omtrent gedrag (VOG) (8.1.3.2). (Toelichting: Externe partijen staan contractueel in voor geheimhouding van hun medewerkers en overleggen een VOG van medewerkers die voor het CIBG gaan werken inhuur onder voorwaarden ARVODI en mantelpartij.)

Maatregelen voor beheer van dienstverlening door een externe partij (10.2)

- Voor zover gebruik wordt gemaakt van dienstverlening t.a.v. ICT-voorzieningen door een externe partij, zijn er dienstverlenings- en beveiligingsniveaus contractueel overeengekomen (10.2.1).
- De diensten en beveiliging t.a.v. ICT voorziening worden door een externe partij beoordeeld en gecontroleerd (10.2.2). Door het CIBG kan een TPM verklaring worden gevraagd.

Uitwisseling van informatie (TNK 10.8)

- Er is een beleid, er zijn procedures en er zijn beheersmaatregelen getroffen om uitwisseling van informatie op een veilige manier te ondersteunen (10.8.1)
- In overeenkomsten met externe partijen worden de beveiligingsaspecten m.b.t. uitwisseling van informatie meegenomen (10.8.2).

2.2 Beveiligingsbeleid is kader voor informatiebeveiligingsplan

Tijdens ons onderzoek hebben we twee beleidsdocumenten ontvangen voor de periode 2011 tot heden. Deze gelden voor heel CIBG en bieden een kader voor het informatiebeveiligingsplan voor het donorregister.

2.2.1 *Het beveiligingsbeleid 2011 CIBG gaat uit van een baseline*

Dit betreft het beveiligingsbeleid, dat gedurende tot november 2018 geldig was. Onder de uitgangspunten en voorwaarden in dit document staat het volgende:

7) Voor de borging van de beveiliging volgt het CIBG primair een productgerichte insteek. Dit betekent dat risicoanalyses over clustergrenzen gaan. Productverantwoordelijke lijnmanagers zijn verantwoordelijk voor het opstellen, beheren en naleven van beveiligingsplannen.
8) Het CIBG werkt met een baseline. Deze baseline bevat de beveiligingsmaatregelen die generiek zijn genomen en waarvan productverantwoordelijken mogen uitgaan dat ze zijn geïmplementeerd. Voor elk product wordt vastgesteld of de beveiligingsmaatregelen in de baseline voldoende zijn. Als aanvullende beveiligingsmaatregelen nodig zijn, worden deze vastgelegd in een productspecifiek beveiligingsplan.
9) Bij het opstellen van baseline en beveiligingsplannen worden beveiligingsmaatregelen geïmplementeerd op basis van een risicoanalyse in samenhang met een kostenafweging.
10) Bedrijfsmiddelen worden onderverdeeld in de categorieën 'systemen', 'informatie', 'fysieke middelen' en 'diensten'.
11) Classificatie van bedrijfsmiddelen wordt ingezet als middel om de behoefte aan beveiliging te bepalen. De classificaties die worden gebruikt zijn hoog, gemiddeld en laag. De classificatie wordt bepaald op basis van de ernst van de gevolgen (impact) wanneer een bedrijfsmiddel dat niet beschikbaar is, fouten bevat, of ten onrechte openbaar is gemaakt.

Onder baseline wordt door het CIBG verstaan: "Een concrete set van beveiligingsmaatregelen en richtlijnen die als basisnorm geldt".

Beveiligingsplan
Onder beveiligingsplan wordt door het CIBG verstaan: "Een opsomming van beveiligings-maatregelen en/of vindplaatsen welke voor een verantwoordelijkheidsgebied van kracht zijn". Het CIBG kiest ervoor om ook de risicoanalyses op te nemen in het beveiligingsplan.

2.2.2 *Het Beleidsdocument informatieveiligheid CIBG is in 2018 geactualiseerd*

Tijdens ons onderzoek hebben wij het Beleidsdocument informatieveiligheid CIBG ontvangen (nov 2018). Het document geeft aan dat dit strategisch beleidsdocument de organisatie en het beleid voor het inregelen van informatieveiligheid binnen het CIBG beschrijft. Daarmee wordt ondersteuning, sturing en richting gegeven aan wat interne en externe medewerkers alsmede derden op het gebied van informatiebeveiliging kunnen en mogen verwachten van het CIBG.

Naar aanleiding van dit vernieuwde beleidsdocument heeft geen aanpassing van het informatiebeveiligingsplan Donorregister (2011) plaatsgevonden.

2.2.3 *Het meest recente en geldende informatiebeveiligingsplan Donorregister is uit 2011*

Tijdens het onderzoek hebben wij twee beveiligingsplannen betreffende het donorregister (van voor 1 juli 2020) ontvangen, één uit 2005 en één uit 2011. In de beveiligingsplannen staan normaliter de maatregelen nader uitgewerkt.
We hebben geconstateerd dat in het ontvangen plan uit 2005 relevante maatregel voor de administratie van elektronische media bevatte en dat deze voorheen belegd was bij de I-afdelingen. De maatregel is niet herkenbaar in het plan uit 2011 en de maatregel wordt niet meer uitgevoerd.

Uit de aangetroffen colofon in het document kunnen wij afleiden dat tot 2011 bijna jaarlijkse actualisatie plaatsvond.

Versie	Datum	Opmerking
0.1	31-10-2001	Eerste concept
1.0	15-08-2002	Definitieve versie
2.0	02-03-2005	Diverse aanpassingen
3.0	06-12-2006	Diverse aanpassingen
3.1	16-11-2007	Toevoeging crisisplan
3.2	03-03-2008	Diverse aanpassingen
3.3	26-03-2008	Update crisisplan
3.4	20-08-2008	Major update
4.0	20-11-2008	Diverse aanpassingen
4.1	01-09-2009	Major update
4.2	04-01-2010	Update, o.a. nieuwe mantelpartijen opgenomen
4.3	13-12-2011	Nieuwe versie opgesteld op basis van organisatiewijziging, beveiligingsbeleid, baseline en beveiligingsplan van de voormalige unit Donorregister.
5.0	22-12-2011	Aanvullingen verwerkt, definitieve versie

Het plan uit 2011 sluit aan op het beveiligingsbeleid van 2011 en verwijst conform naar de Baseline beveiliging CIBG uit 2011. Maar paragraaf 6.4 waarin maatregelen specifiek uitgewerkt moeten worden voor het donorregister, is niet ingevuld.

Het beveiligingsplan Donorregister 2011 is na 2011 niet meer geactualiseerd en dus het meest actuele, geldende plan voor onze onderzoeksperiode. Wij constateren dat dit afwijkt van de beschrijving zoals dit in het beveiligingsplan zelf is opgenomen. In het plan zelf staat namelijk beschreven dat "het clusterhoofd Registers verantwoordelijk is voor het actualiseren en beheren van dit beveiligingsplan. Dit beveiligingsplan wordt iedere vier maanden getoetst en bij relevante wijzigingen waar nodig geactualiseerd."

2.3 Maatregelen

Lettende op de onderzoeksperiode is BIR 2012 als referentiekader gebruikt. In deze paragraaf zijn de toets resultaten ten aanzien van de aanwezigheid van maatregelen vanuit de BIR:2012 Tactisch Normenkader (TNK) opgenomen.
Per maatregel wordt aangegeven of voor de betreffende maatregel

- een beschrijving is aangetroffen (opzet) en
- een praktijkvoorbeeld is aangetroffen (bestaan).

Voor het vaststellen van de aanwezigheid van de beschrijving (opzet) van de maatregelen zijn het Beveiligingsplan Donorregister 2011 en de Baseline beveiliging CIBG als bronnen gebruikt.

2.3.1 *Beheer van bedrijfsmiddelen (TNK 7) beperkt aangetroffen*

Beheer van bedrijfsmiddelen (alle informatie, systemen en dragers) is relevant omdat door inventarisatie (weten wat je hebt), verantwoordelijkheden kunnen worden belegd en bedrijfsmiddelen dan op de juiste wijze beschermd kunnen worden. Ook externe gegevensdragers zijn bedrijfsmiddelen.
De onderstaande maatregel is opgenomen in de Baseline beveiliging CIBG:

- Classificatie van informatie (TNK 7.2)
    - Informatie wordt door de eigenaar geclassificeerd met betrekking tot waarde, wettelijke eisen, vertrouwelijkheid en onmisbaarheid in het proces (7.2.1).
      Het CIBG gebruikt een classificatiemethode die wordt toegepast in beveiligingsplannen.

Opzet (de norm betreft een beschrijving, bestaan is niet van toepassing voor deze maatregel)
Deze maatregel is opgenomen in de Baseline beveiliging CIBG, waarbij is aangegeven dat de verantwoordelijkheid hiervoor ligt bij het lijnmanagement. In het Beveiligingsplan Donorregister 2011 zijn de bedrijfsprocessen en bijbehorende bedrijfsmiddelen met het bijbehorende classificatie ten aanzien van betrouwbaarheidseisen (beschikbaarheid, exclusiviteit en integriteit) opgenomen. Als fysieke middelen/hardware worden o.a. aangegeven pc's, scanner, printer, briefpapier. Externe gegevensdragers (zoals DVD's, USB-sticks en harde schijven) hierbij niet zijn genoemd.

Specifieke maatregelen ten aanzien van beheer van bedrijfsmiddelen, die wij van belang achten voor het terugdringen van de risico's t.a.v. externe gegevensdragers hebben wij niet aangetroffen in de baseline. Dit betreffen de volgende normen vanuit de TNK:

- Eigendom van bedrijfsmiddelen (TNK 7.1.2)
  Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie.
  Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.

Opzet
Deze maatregel is niet teruggevonden in de Baseline 2011. Ook in het geldende Beveiligingsplan Donorregister is dit niet expliciet aangegeven.
Wel is aangegeven dat de eigenaarsrol ligt bij de Secretaris-Generaal (SG). De SG c.q. plaatsvervangend SG voert aldus het beheer over de registers en is daarmee verantwoordelijk voor het Donorregister. Echter dit is een ander niveau en betreft geen lijnmanager zoals bedoeld in de norm.

Bestaan
Uit interview komt naar voren dat er gewerkt wordt met strategische (management) en tactische (medewerkers) driehoeken waar business en ICT samen komen. Het is niet bekend op welke wijze de verantwoordelijkheden en eigenaarschap van onderliggende ICT bedrijfsmiddelen zijn belegd en welke functionaris

verantwoordelijk is voor het treffen van passende maatregelen die voor betreffende bedrijfsmiddelen nodig zijn.
CIBG geeft in reactie aan dat er tijdens ons onderzoek een taskforce is opgestart waarin een heldere rolverdeling wordt uitgewerkt. Wij hebben hier geen nader onderzoek naar gedaan.
Directie Geneesmiddelen en Medische Technologie (GMT) van VWS is de opdrachtgever van het Donorregister van CIBG. Dit komt naar voren bij Privacy Impact Analyse (PIA). Hoe de governance relatie met GMT is vormgegeven, hebben wij niet aangetroffen.

Beheer van bedrijfsmiddelen met externe leverancier
In het verlengde van TNK 7.1.2 hebben we hiernaar gekeken. De beheerwerkzaamheden ten aanzien van hosting zijn per 2018 aan een andere leverancier uitbesteed. Het is ons onduidelijk op welke wijze CIBG de rol van beheer van bedrijfsmiddelen invult. In de meeste recente overeenkomst is aangegeven dat CIBG primair verantwoordelijk is voor de classificatie en rubricering van bedrijfsmiddelen en dat CIBG daartoe een CMDB bijhoudt. De bedoelde CMDB hebben wij niet aangetroffen. De beschrijving sluit niet aan op de aangetroffen situatie.

Beheer van Bedrijfsmiddelen

Beheer van bedrijfsmiddelen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	KPN Internedservices	CIBG
Alle gebruikte diensten en middelen dienen te worden geclassificeerd (AVG) en gerubriceerd (VIRBI) overeenkomstig de processen waar zij ingezet worden of de gegevens die verwerkt worden.		P
De classificatie/rubricering wordt in de CMDB bijgehouden.		P

In de oude overeenkomst tot 2018 was dit als volgt aangegeven:

3.4. Beheer van Bedrijfsmiddelen

Beheer van bedrijfsmiddelen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LVR]	VWS
Alle gebruikte diensten en middelen dienen te worden geclassificeerd (WBP) en gerubriceerd (VIRBI) overeenkomstig de processen waar zij ingezet worden of de gegevens die verwerkt worden.	nvt	nvt
De classificatie/rubricering wordt in de CMDB bijgehouden.	nvt	nvt

Beheer van bedrijfsmiddelen - criteria	
Rapportage ontbrekende classificaties en rubriceringen.	nvt
Inzage in CMDB	nvt

- Labeling en verwerking van informatie (TNK 7.2.2)
  Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en de verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

Opzet (de norm betreft een beschrijving, bestaan is niet van toepassing voor deze maatregel)
Deze maatregel is niet teruggevonden in de geldende Baseline 2011. Ook in het geldende Beveiligingsplan Donorregister is dit niet expliciet aangegeven.

2.3.2 *Beveiliging van Personeel deels aangetroffen (TNK 8)*

Het is van belang dat personeel bewust is van informatiebeveiliging en daarbij ook bewust is hoe zij zelf daaraan bijdraagt. De maatregelen hiertoe zijn opgenomen in de Baseline beveiliging CIBG 2011 maar niet uitgewerkt of nader gespecificeerd in het Beveiligingsplan Donorregister 2011.
Ondanks dat deze niet zijn gespecificeerd in het beveiligingsplan hebben we tijdens het onderzoek diverse documenten aangetroffen, die invulling geven aan de onderstaande maatregelen.

Maatregelen die van belang zijn voor dit onderzoek:

- Vaste medewerkers leggen bij het in dienst treden een eed of belofte af en ondertekenen eventueel een geheimhoudingsverklaring (8.1.3.1).
- Externe partijen dragen zorg voor een geheimhoudingsverklaring en verklaring omtrent gedrag (VOG) (8.1.3.2) (zie paragraaf 2.4).
- De lijnmanager zorgt er voor dat medewerkers op de hoogte zijn van de beveiligingsmaatregelen en zich er aan houden (8.2.1).
- Beveiligingsbewustzijn wordt bevorderd door regelmatig aandacht aan de beveiliging te schenken (8.2.2).

Opzet en bestaan

Tijdens het onderzoek hebben wij de volgende documenten ontvangen:

- Gedragscode Integriteit Rijk (2017/ 2018) ontvangen. Dit is een uitgebreid document met achtergrond informatie voor alle ambtenaren.
- Gedragsregeling voor de digitale werkomgeving (2016, BZK). Deze Gedragsregeling beschrijft concreet het van je gewenste gedrag bij het gebruik van de digitale werkomgeving, geeft een algemene toelichting daarop en geeft je nadere informatie over het beheer van en de controle op de digitale werkomgeving. Daarin staat expliciet genoemd: Laat mobiele apparaten en gegevensdragers (laptop, smartphone, usb-stick) nooit ergens liggen, zonder dat je vastgesteld hebt dat het voor onbevoegden onmogelijk is om toegang tot de informatie te krijgen.

Deze stukken zijn zeer informatief. Als gevolg van de invoering van de AVG is veel aandacht besteed aan de bewustwording bij medewerkers voor de beveiliging van persoonsgegevens. Er zijn meerdere awareness sessies gehouden. Destijds golden dezelfde regels, maar was minder blijvende aandacht voor dit onderwerp bij medewerkers.

Om aandacht te blijven houden voor beveiliging hebben wij vastgesteld dat CIBG de medewerkers informeert via berichten op intranet en de CIBG Academie (TNK 8.2.2).

Nieuwe medewerkers zijn verplicht om binnen 14 dagen na ontvangst van inloggegevens voor de CIBG Academie in ieder geval de modules (8.2.1) "Introductiemodule CIBG", "Gezond Werken" en de "AVG" module te volgen en af te ronden. De CIBG Introductie wordt afgerond met een test over integriteit en vertrouwelijke informatie.

Voor externe medewerkers direct werkend voor CIBG hebben wij de volgende stukken aangetroffen:

- Model Integriteitsverklaring Rijk voor externen. Daarin staat een verwijzing naar de Gedragscode Integriteit Rijk en de Gedragsregeling digitale werkomgeving opgenomen en de mededeling dat deze beschikbaar zijn gesteld. Tevens is aangegeven: "Ik ben mij bewust van mijn verantwoordelijkheid voor de beveiliging van informatie en informatie dragers." Deze verklaring dient te worden ondertekend alvorens de werkzaamheden starten.
- Tijdens het onderzoek hebben wij voorbeelden van ondertekende formulieren ontvangen.

Voor samenwerkende partijen verwijzen wij naar paragraaf 2.4 van dit document.

2.3.3 *Bestaan Fysieke beveiliging en beveiliging van de omgeving (TNK 9) aangetroffen*

Maatregelen die wij relevant achten in relatie tot dit onderzoek.

- Apparatuur met opslagmedia die buitengebruik is gesteld of die hergebruikt wordt, is geschoond van informatie en / of software (TNK 9.2.6)

Opzet
Deze maatregel is opgenomen in de Baseline beveiliging CIBG en daarin belegd bij het lijnmanagement, maar deze maatregel is niet nader uitgewerkt in het geldende Beveiligingsplan Donorregister. De DVD's en externe schijven zijn niet geïnventariseerd als bedrijfsmiddel (zie ook paragraaf 2.3.1).

Bestaan
Tijdens interview en in het feitenrelaas heeft CIBG aangegeven dat voor vernietiging van DVD's in 2020 gebruik gemaakt is van het contract van de Belastingdienst (bewoner van hetzelfde pand) met Reiswolff. In het interview is aangegeven dat Reiswolff gecertificeerd en gecontracteerd is voor de vernietiging van vertrouwelijke materialen. De formele vastlegging ten aanzien van het gebruik van het contract door CIBG is niet aangetroffen. Ook is aangegeven dat de gegevens op de tijdelijke standalone PC veilig zijn afgevoerd.
Voor externe leveranciers verwijzen wij naar paragraaf 3.3.4 van dit document.

2.3.4 *Beheer van communicatie en bedieningsprocessen (TNK 10) beperkt aangetroffen*

- Back-up (10.5)
  - Er zijn adequate back-up en restore procedures, die periodiek getest worden. Naast de WBP stelt de archiefwet en het Archiefbesluit eisen aan de bewaartermijn van informatie (TNK 10.5.1)

- Procedures voor het behandelen van informatie (TNK 10.7)
  - Informatie wordt in overeenstemming met de archiefwet en archiefbesluit bewaard (TNK 10.7.3.2).

Opzet
Deze zijn opgenomen in de Baseline beveiliging CIBG, maar niet nader uitgewerkt in het geldende Beveiligingsplan Donorregister.

Casus specifiek
Het scanningsproject door de belastingdienst was reeds in 2013 afgerond. De DVD's zijn toen overgedragen. Mede vanuit de archiefwet is het onduidelijk waarom de belastingdienst tot 2015 nog een back-up had van de gegevens. In het projectplan van het scanningsproject wordt het gebruik van de externe harde schijven niet beschreven. CIBG geeft tijdens ons onderzoek aan, dat zij destijds op de hoogte was van de aanwezigheid van de back-up. Het is voor ons onduidelijk waarom deze externe schijven niet eerder zijn overgedragen aan CIBG, bijvoorbeeld aan het eind van het project in 2013.

- Beheer van verwijderbare media (TNK 10.7.1)
  Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

Opzet
De bovenstaande maatregel is niet opgenomen in de Baseline beveiliging CIBG. In het geldende Beveiligingsplan Donorregister zijn hiervoor geen maatregelen aangeduid.

Bestaan deels aangetroffen
Tijdens het interview heeft CIBG aangegeven dat de omgang met verwijderbare media in de Rijksbrede gedragsregels is opgenomen. Deze gedragsregels hebben we aangetroffen. Een vertaling naar de CIBG specifieke omgeving met protocollen, werkwijze ten aanzien van verwijderbare media zijn niet aangetroffen.

We hebben geconstateerd dat in het verleden in het IB-plan 2005 wel in een dergelijke maatregel was voorzien, maar tijdens interview heeft CIBG aangegeven dat dit nu niet meer van toepassing is en dat dit vroeger mogelijk gedaan werd door I-divisie. Het betreft de volgende maatregel uit 2005:

> Elektronische media zijn bij ontvangst/creatie in een administratief proces geboekt. Als een medium moet worden gewist of afgevoerd (vernietigd) dan wordt als eerste de media boekhouding geraadpleegd om te kunnen constateren dat het juiste medium is aangewezen voor deze destructieve handelingen. Is dat het geval dan wordt vóór vernietiging de boekhouding bijgewerkt en het medium gekenmerkt als "te wissen" c.q. "te vernietigen". Voor het vernietigen is er een voorschrift bij Technisch Beheer.

Casus specifiek
In het feitenrelaas staat dat de externe gegevensdragers in de kluis werden bewaard. Echter in het feitenrelaas staat dat een geïnterviewde zegt dat hij deze schijven ook in Heerlen heeft gebruikt, dus na 19 februari 2016. Na gebruik zijn de schijven teruggegeven aan iemand binnen de projectgroep. Het is onbekend aan wie. Dit is de laatste keer dat met zekerheid kan worden vastgesteld dat de schijven nog aanwezig waren. Hieruit blijkt niet dat na gebruik van de gegevensdragers deze altijd weer in de kluis werden opgeslagen.

De Gedragsregeling voor de digitale werkomgeving (2016, BZK) golden toen al. Daar staat in: 'Laat mobiele apparaten en gegevensdragers (laptop, smartphone, usb-stick) nooit ergens liggen, zonder dat je vastgesteld hebt dat het voor onbevoegden onmogelijk is om toegang tot de informatie te krijgen' (zie ook paragraaf 2.2.2).

- Verwijdering van media (TNK 10.7.2)

Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Opzet
De bovenstaande maatregel is niet opgenomen in de geldende Baseline beveiliging CIBG. Ook in het geldende Beveiligingsplan Donorregister zijn hiervoor geen maatregelen aangeduid. De werkwijze ten aanzien van het verwijderen van externe gegevens zoals met Reiswolff is niet in procedures terug te vinden.
Bestaan
Tijdens het onderzoek heeft CIBG in interview aangegeven dat er voor vernietiging van DVD's gebruik gemaakt wordt van het contract van de Belastingdienst (bewoner van hetzelfde pand) met Reiswolff. Reiswolff is gecertificeerd en gecontracteerd voor de vernietiging van media met vertrouwelijke gegevens. CIBG sluit niet uit dat de twee externe schijven al eerder zijn vernietigd, maar een vernietigingsbewijs van de twee zoekgeraakte schijven is niet terug gevonden. Of deze procedure *altijd* is nageleefd kunnen wij niet vaststellen.

- Procedures voor de behandeling van informatie (TNK 10.7.3)

Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

Opzet (beschrijving)
De bovenstaande maatregel is niet opgenomen in de geldende Baseline beveiliging CIBG. In het geldende Beveiligingsplan Donorregister zijn hiervoor geen maatregelen aangeduid.
In het verleden was hierin wel voorzien. In het ontvangen IB-plan 2005 is wel een dergelijke maatregel aangetroffen maar tijdens interview heeft CIBG aangegeven dat dit nu niet meer van toepassing is en dat dit vroeger mogelijk gedaan werd door I-divisie. Het betreft de volgende maatregel uit 2005:

> De informatie op elektronische media is beveiligd door ze op te bergen in een kluiskast, danwel in een ruimte waarvoor beperkte toegang geldt. Bulkaanlevering van media (ong. 180.000 personen/adressen) komt op 1 plaats terecht (bij Technisch Beheer) en blijft daardoor overzichtelijk.

Bestaan
Er zijn diverse maatregelen die hiermee verband houden aanwezig:

- Het gebruik van wachtwoorden en toekennen van autorisaties.
- Tijdens interview heeft CIBG aangegeven dat er ten aanzien van opslag van formulieren een afsluitbare kast wordt gebruikt.

Dit zijn weliswaar maatregelen maar door afwezigheid van een volledige inventarisatie (bijvoorbeeld op welke plekken is er opslag van informatie?), is het onduidelijk of deze maatregelen afdoende zijn. Tevens is het hebben van afsluitbare kasten niet voldoende er dient hierbij ook een werkwijze te worden aangegeven ten aanzien van bijvoorbeeld toegangsbeheer / Sleutelbeheer.

In reactie op het concept rapport heeft CIBG aangegeven de werkwijze beschikbaar te hebben en dat teamleden van het Donorregister vanaf 1 juli 2020 in een ruimte werken waarvoor alleen toegang is met specifieke autorisatie op de Rijkspas.

Casus specifiek
In het feitenrelaas staat het gebruik van twee kluizen aangegeven:

De kluis in Kerkrade (aug 2015- feb 2016) stond in een afgesloten ruimte, waarvan de sleutel in een sleutelkastje werd bewaard op de kamer van Functioneel Beheer. Van het sleutelkastje hadden de Functioneel Beheerders de sleutel, maar er bestond geen sleutelprotocol. Wel waren er ongeschreven afspraken, zoals: degene die als laatste naar huis gaat zorgt dat de sleutelkast en de deuren naar het magazijn – waar de kluis staat – gesloten zijn.

In Heerlen maakt CIBG (feb 2016-heden) gebruik van een kluis van de Belastingdienst. Deze bevindt zich in de kelder van het gebouw. In Heerlen is geen sleutelprotocol of een logboek in gebruik. Er zijn twee sleutels voor de kluis in gebruik: één voor de managementondersteuner die de sleutel bewaart in haar locker en één voor een collega, die een reservesleutel heeft in zijn locker.
Elke medewerker mag gebruik maken van de kluis en krijgt de sleutel op verzoek om spullen erin te leggen of eruit te halen. Medewerkers kunnen individueel de kluis in. In de praktijk zijn dit maar 3 verschillende medewerkers geweest volgens CIBG.

Voor beide kluizen zijn verbeteringen mogelijk door:
- een kluis inventaris beschikbaar te hebben,
- een sleutelprotocol te voeren,
- een logboek op te stellen en te gebruiken,
- een periodieke controle van de inhoud van de kluis en
- een vierogen principe in te voeren: altijd met minimaal twee personen de kluis openen. Hierdoor neemt de betrouwbaarheid van het logboek toe.

In reactie op het concept rapport heeft CIBG laten zien dat inmiddels een procedure, inventarisatie van de inhoud en een logboek voor het gebruik van de kluis is opgesteld.

Verhuisprocedures kluisinhoud
Casus specifiek
In 2016 is CIBG van Kerkrade verhuisd naar Heerlen.
In interview is aangegeven dat er geen specifieke verhuisprocedures voor de verhuizing van de kluisinhoud waren opgesteld. Aangegeven werd dat de coördinatoren van de verhuizing dit hebben georganiseerd, zij hadden toegang tot de kluis. Bij een verhuizing kan een apart protocol opgesteld worden voor de kluisinhoud te inventariseren, begeleid vervoeren (wordt er onderweg niets verloren, worden er geen gegevens gedupliceerd) en begeleid in de kluis te laten plaatsen. Daarbij is het van belang dat alleen geautoriseerde personen toegang hebben tot de kluis en de protocollen zoals hierboven geschetst naleven.

2.4 Afspraken met samenwerkende partijen van CIBG

Tijdens ons onderzoek werd duidelijk dat CIBG voor het Donorregister veel werkzaamheden heeft uitbesteed. De externe gegevensdragers zijn ontstaan in 2013 tijdens een uitbesteding van een digitaliseringstraject aan de Belastingdienst. Om de vertrouwelijkheid van data te waarborgen en daarmee ook te voorkomen dat data (onbedoeld) op (onbeheerde) externe gegevensdragers belanden, is het van belang afspraken te maken met de externe partijen ten aanzien van informatiebeveiliging, waardoor het CIBG zich ervan kan verzekeren dat de uitvoerende partij de informatiebeveiliging (Vertrouwelijkheid in het bijzonder) goed heeft geborgd.

De onderstaande maatregelen zijn daarvoor relevant en dienen voornamelijk in contracten, servicelevel agreements (SLA's) en Dossier Afspraken en Procedures (DAPs) met leveranciers te zijn uitgewerkt / opgenomen.

Maatregelen met externe partijen t.a.v. beveiligingsincidenten (TNK 6)

- In contracten met externe partijen is vastgelegd op welke manier beveiligingsincidenten moeten worden gemeld en op welke manier deze door de externe partij en het CIBG worden behandeld. (6.2.3.2)

Maatregelen met externe partijen t.a.v. Personeel (TNK 8)

- Externe partijen dragen zorg voor een geheimhoudingsverklaring en een verklaring omtrent gedrag (VOG) (8.1.3.2). (Toelichting: Externe partijen staan contractueel in voor geheimhouding van hun medewerkers en overleggen een VOG van medewerkers die voor het CIBG gaan werken inhuur onder voorwaarden ARVODI en mantelpartij.)

Maatregelen voor beheer van dienstverlening door een externe partij (TNK 10.2)

- Voor zover gebruik wordt gemaakt van dienstverlening t.a.v. ICT-voorzieningen door een externe partij, zijn er dienstverlenings- en beveiligingsniveaus contractueel overeengekomen (10.2.1).
- De diensten en beveiliging t.a.v. ICT voorziening worden door een externe partij beoordeeld en gecontroleerd (10.2.2). Door het CIBG kan een TPM verklaring worden gevraagd.

Uitwisseling van informatie (TNK 10.8)

- Er is een beleid, er zijn procedures en er zijn beheersmaatregelen getroffen om uitwisseling van informatie op een veilige manier te ondersteunen (10.8.1)
- In overeenkomsten met externe partijen worden de beveiligingsaspecten m.b.t. uitwisseling van informatie meegenomen (10.8.2).

2.4.1 *Maatregelen voor uitbesteding niet altijd herkenbaar aangetroffen*

Leveranciers worden ingezet voor specifieke projecten, maar er zijn leveranciers die structureel een onderdeel van het beheer van het Donorregister uitvoeren. Voorbeelden hiervan zijn het technisch beheer voor het Donorregister, het ontvangen en inscannen van Donorformulieren, het verzenden van gepersonaliseerde poststukken.

Wij hebben diverse contracten, SLA's, DAPs in beschouwing genomen. In diverse documenten ontbrak de formele ondertekening, desondanks hebben wij deze documenten wel als leidend beschouwd in het onderzoek.

De onderstaande maatregelen zijn niet altijd herkenbaar opgenomen.

- *Melden van beveiligingsincidenten is niet in alle contracten benoemd*. Bij prioritering van incidenten valt op dat deze vaak wordt bepaald aan de hand van de kwaliteitseis van beschikbaarheid van het systeem en niet op basis van schaden van vertrouwelijkheid (6.2).
  CIBG geeft in reactie op het conceptrapport aan dat dit is aangepast en nu is

opgenomen in de verwerkersovereenkomst. Deze is nog in concept, wij hebben hier geen nader onderzoek naar gedaan.

- *Afspraken omtrent geheimhouding en Verklaring Omtrent Gedrag (VOG) zijn niet altijd beschreven in de DAP of SLA (8.1.3.2).* CIBG geeft aan dat zij dit bij overeenkomsten met de Belastingdienst niet nodig acht omdat dit algemeen overheidsbeleid is. Tegelijkertijd zien wij dat dit wel in een nieuwe overeenkomst met de Belastingdienst is opgenomen.
  In een andere situatie is dit vastgelegd in raamovereenkomst. Het is niet nader benoemd in de SLA of DAP. Hierdoor kan het gebeuren dat bij uitvoer van het contract dit niet bewust onderkend wordt als maatregel.
  In security eisen (Beveiligingsovereenkomst [Capgemini], Beveiligingsafspraken en criteria – versie 1.0) is aangegeven dat de medewerkers een geheimhoudingsverklaring hebben getekend maar het VOG is doorgehaald. Het is niet duidelijk wat hieraan ten grondslag ligt.

- *De vereiste beveiligingsniveaus (beschikbaarheid, exclusiviteit en integriteit) zijn niet altijd herkenbaar in afspraken.*
  In een contract met een leverancier (Capgemini) is aangegeven dat de security eisen van CIBG gelden (10.2.1). Deze eisen hebben wij opgevraagd en ontvangen. BEVEILIGINGSOVEREENKOMST [CAPGEMINI], Beveiligingsafspraken en criteria – versie 1.0 (volgens colofon eerste versie 2014 laatste versie 2018). Maar de echte security eisen zoals 7 * 24 uur beschikbaarheid van het Donorregister, hebben wij hierin niet aangetroffen. Opvallend is dat aangegeven is "Dit document beschrijft enkel de afspraken en criteria rondom het beheer van diensten, de volgende onderwerpen zijn daarmee expliciet buiten scope: Beveiligingseisen voor software ontwikkeling (Secure Software Development Lifecycle), Beveiligingseisen voor voorzieningen en diensten, Het veilig gebruik van voorzieningen en diensten."

- *Over de naleving en service level rapportages zijn in de overeenkomsten afspraken vastgelegd (opzet).*
  Een belangrijke leverancier heeft ondanks dat hierover afspraken waren vastgelegd, geen TPM verklaring over 2018 verstrekt (10.2.2.). Ook over andere jaren hebben wij tijdens ons onderzoek geen verklaringen ontvangen. ADR heeft tijdens het onderzoek wel een bewijs van certificering van de leverancier middels een link op internet ontvangen, maar dergelijke certificering is niet specifiek voor het Donorregister afgegeven en is niet vergelijkbaar met de toegezegde TPM verklaring.

- *De wijze waarop Uitwisseling van informatie (10.8) plaatsvindt, is in de afspraken met leveranciers niet altijd aangegeven.*
  Voorbeeld hiervan is dat bij beëindiging "op verzoek van VWS alle gegevens waarvoor VWS verantwoordelijk is en/of waarvan VWS eigenaar is tijdig en in bruikbaar formaat overgedragen aan VWS". Er is niet vermeld hoe deze wordt overgedragen en niet bekend of de informatie daarna wordt vernietigd.
  In de recent aangepaste concept bewerkingsovereenkomst is opgenomen dat de verwerker een verklaring moet afgeven. We hebben hier geen nader onderzoek naar gedaan.

- *Afspraken t.a.v. autorisaties niet eenduidig vastgelegd.* Lettende op de aangetroffen Operational Level Agreement tussen CIBG en NTS t.b.v. donorregister (van 15 februari 2016) is een werkwijze voor de periodieke controle beschreven.
  > "NTS verplicht zich tot het direct doorgeven van gegevens (naam + account) voor het opheffen van een Odisys-account indien er sprake is van uitdiensttreding, functiewisseling waarbij uit hoofde van die functie geen toegang nodig is of anderszins door een mail te sturen naar de afdeling functioneel beheer van het CIBG. Eén keer per maand controleert de NTS de actieve Odisys-accounts op actualiteit. En dat opgeheven Odisys-accounts worden door CIBG-IV binnen één werkdag verwijderd uit het Donorsysteem."

In de kantlijn is een opmerking gemaakt dat CIBG liever actieve meldplicht ziet waarin NTS iedere maand de benodigde gebruikers aanlevert ondertekend door de directeur. Welke werkwijze uiteindelijk gevolgd is, is niet bekend.

Ondanks dat in de OLA vermeld staat dat dit document jaarlijks gereviewd wordt, is het document uit 2016, bijvoorbeeld lettende op de genoemde functionarissen, niet actueel.

2.4.2 *Overig: Waarde van afspraken in de DAP onduidelijk*

De Diensten en afspraken procedures (DAP) is een uitwerking van de Service Level Agreement. Voorbeeld hiervan zijn nadere specificaties van maandelijkse en TPM rapportages. Maar in de DAP staan ook aanvullende onderwerpen vermeld, die niet in de SLA voorkomen, zoals beveiliging. Tegelijkertijd staat er het volgende: "Dit DAP vormt een operationele uitwerking van de SLA welke door beide partijen gezamenlijk wordt vastgesteld. Het DAP vormt geen contract document. Het service level agreement (SLA) dat van toepassing is op de diensten die aan het CIBG worden geleverd is te allen tijde leidend. Indien er binnen dit DAP afwijkende afspraken worden gemaakt, maken deze geen deel uit van de contractuele overeenkomsten, maar zijn dat operationele afspraken en/of werkinstructies. " Het is voor ADR onduidelijk hoe bindend de afspraken in DAP zijn.

2.5 Samenvatting bevindingen vraag één

Hieronder wordt het antwoord op de vraag één "*Zijn de door het CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevensdragers in overeenstemming met de richtlijnen vanuit de toenmalige BIR en zijn deze nageleefd in de periode vanaf de totstandkoming van de externe gegevensdragers tot nu toe?*" in tabelvorm samengevat.
In de onderstaande tabel staan in de linkerkolom maatregelen die vanuit de BIR gezien relevant zijn voor de omgang met externe gegevensdragers. In de kolom opzet is weergegeven of een beschrijving bij betreffende norm een bijpassende maatregel is aangetroffen in de documentatie. In de kolom 'bestaan' is weergegeven of er maatregelen zijn uitgevoerd horende bij de norm. In sommige gevallen is bestaan niet van toepassing omdat de norm slechts betrekking heeft op de aanwezigheid van een beschrijving.

Veel maatregelen betrekking hebbend op procedures ten aanzien van bedrijfsmiddelen zijn niet aangetroffen.
Maatregelen betrekking hebbend op personeel zijn zowel in opzet als in bestaan aangetroffen. Echter borging van de maatregelen in een breder plan is niet aangetroffen.
Maatregelen met betrekking tot externe dienstverleners zijn deels aangetroffen. Er zijn (grote) verschillen in afspraken met dienstverleners aangetroffen..

	Opzet	*Bestaan*
Organisatie van beveiliging (TNK 5)		
Informatiebeveiligingsplan	Verouderd	Verouderd
Beheer bedrijfsmiddelen (TNK 7)		
Eigendom van bedrijfsmiddelen (TNK 7.1.2)	Niet aangetroffen	n.v.t.
Classificatie van informatie (TNK 7.2) waaronder ○ Informatie wordt door de eigenaar geclassificeerd met betrekking tot waarde, wettelijke eisen, vertrouwelijkheid en onmisbaarheid in het proces (7.2.1).	Deels aangetroffen,	n.v.t.
Labeling en verwerking van informatie (7.2.2)	niet aangetroffen	niet aangetroffen
Beveiliging van Personeel (TNK 8)		
○ Vaste medewerkers leggen bij het in dienst treden een eed of belofte af en ondertekenen eventueel een geheimhoudingsverklaring (8.1.3.1)	Aangetroffen, maar geen borging middels IB-plan	Aangetroffen
○ De lijnmanager zorgt er voor dat medewerkers op de hoogte zijn van de beveiligingsmaatregelen en zich er aan houden (8.2.1).	Aangetroffen, maar geen borging middels IB-plan	Aangetroffen, maar blijft menselijk handelen.
○ Beveiligingsbewustzijn wordt bevorderd door regelmatig aandacht aan de beveiliging te schenken (8.2.2).	Aangetroffen, maar geen borging middels IB-plan	Aangetroffen
Fysieke beveiliging en beveiliging van de omgeving (9)		
• Apparatuur met opslagmedia die buitengebruik is gesteld of die hergebruikt wordt, is geschoond van informatie en / of software (9.2.6)	Niet aangetroffen	Aangetroffen
Beheer van communicatie en bedieningsprocessen (TNK 10)		
• Er zijn adequate back-up en restore procedures, die periodiek getest worden. Naast de WBP stelt de archiefwet en het Archiefbesluit eisen aan de **bewaartermijn** van informatie (10.5.1) ○ Procedures voor het behandelen van informatie (10.7)	Niet aangetroffen	Niet aangetroffen

○ Informatie wordt in overeenstemming met de archiefwet en archiefbesluit bewaard (10.7.3.2).		
○ Beheer van verwijderbare media (10.7.1)	Niet aangetroffen	Deels aangetroffen
○ Verwijdering van media (10.7.2) Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Niet aangetroffen	Deels aangetroffen, volledigheid niet vastgesteld.
Externe partijen (TNK 6.2)		
○ In contracten met externe partijen is vastgelegd op welke manier beveiligingsincidenten moeten worden gemeld en op welke manier deze door de externe partij en het CIBG worden behandeld. (6.2.3.2)	Deels aangetroffen	n.v.t.
Maatregelen personeel i.r.t. externe partijen (TNK 8)		
○ Externe partijen dragen zorg voor een geheimhoudingsverklaring en een verklaring omtrent gedrag (VOG) (8.1.3.2). (Toelichting: Externe partijen staan contractueel in voor geheimhouding van hun medewerkers en overleggen een VOG van medewerkers die voor het CIBG gaan werken inhuur onder voorwaarden ARVODI en mantelpartij.)	Deels aangetroffen	n.v.t.
Maatregelen voor beheer van dienstverlening door een externe partij (TNK 10.2)		
• Voor zover gebruik wordt gemaakt van dienstverlening t.a.v. ICT-voorzieningen door een externe partij, zijn er dienstverlenings- en beveiligingsniveaus contractueel overeengekomen (10.2.1).	Deels aangetroffen	n.v.t.
• De diensten en beveiliging t.a.v. ICT voorziening worden door een externe partij beoordeeld en gecontroleerd (10.2.2). Door het CIBG kan een TPM verklaring worden gevraagd.	Aangetroffen	Niet aangetroffen
Uitwisseling van informatie (TNK 10.8)		
• Er is een beleid, er zijn procedures en er zijn beheersmaatregelen getroffen om uitwisseling van informatie op een veilige manier te ondersteunen (10.8.1) · In overeenkomsten met externe partijen worden de beveiligingsaspecten m.b.t. uitwisseling van informatie meegenomen (10.8.2).	Niet aangetroffen	Niet aangetroffen

3 Opzet Nieuwe Donorregister

Ten tijde van het onderzoek was het nieuwe Donorregister nog niet geïmplementeerd. Zoals in de onderzoeksvragen is aangegeven hebben wij analyse uitgevoerd op de aanwezige documentatie en niet naar het daadwerkelijk inrichting. In dit hoofdstuk worden antwoorden gegeven op de volgende vragen:
Vraag twee: Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?
Vraag drie: Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?
Vraag vier: Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?

3.1 Beleid CIBG schrijft een risicoanalyse voor om beveiligingseisen vast te stellen

In deze paragraaf wordt antwoord gegeven op vraag twee: Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?

We hebben documentatie aangetroffen die de reden tot het vaststellen van beveiligingseisen (binnen CIBG) weergeven. Ten aanzien van het vaststellen van de eisen van vertrouwelijkheid wordt een risicoanalyse vereist vanuit het Beleidsdocument informatieveiligheid CIBG (november 2018). Daarin is het volgende aangegeven:

> "Elke afdelingshoofd, als eigenaar van zijn primaire processen en ondersteunende informatiesystemen (waaronder de registers), zorgt voor een risicoanalyse, een risicowaardering, de invoering van de daaruit voortvloeide maatregelen en het bepalen van restrisico's (zie verder hoofdstuk 2). " (….)
> "De BIR bevat de - bewezen – maatregelen ("controls") om informatieveiligheid, als bedoeld in het VIR, concreet in te richten, tenzij ingevolge bovenliggende wet- en regelgeving een ander framework dan de BIR, voor informatieveiligheid van toepassing is verklaard. Dit is ten minste van toepassing op het UZI-register (en ZOVAR) dat is gehouden aan het ETSI framework voor ICT en informatieveiligheid."

In hoofdstuk 2 staat onder andere aangegeven:

> "Op grond van het vereiste betrouwbaarheidsniveau wordt de vertaalslag gemaakt naar de maatregelen uit de BIR die van toepassing zijn (tenzij ingevolge bovenliggende wet- en regelgeving een ander framework dan de BIR van toepassing is verklaard)."

en

> "Het lijnmanagement stelt voor de aan de orde zijnde processen en informatiesystemen vervolgens een informatieveiligheidsplan (IB-plan) op. Een IB-plan is een opsomming van alle beveiligingsmaatregelen, onderliggende beleidsdocumenten en/of de vindplaatsen daarvan die van kracht zijn. Dit IB-plan wordt vastgesteld door het lijnmanagement en de algemeen directeur CIBG, na te zijn geadviseerd door CISO van het CIBG."

In het Beleidsdocument informatieveiligheid CIBG (november 2018) is bij sturing en beheersing aangegeven dat informatieveiligheid wordt geborgd door:

a. Jaarlijks afgegeven in control verklaringen van de afdelingshoofden over de toepassing en naleving van de BIR (zie verder hoofdstuk 3).

Ook vanuit de Baseline Informatiebeveiliging Overheid (BIO) spelen de vastgestelde beveiligingseisen een belangrijke rol. De Baseline Informatiebeveiliging Overheid (BIO) is sinds 2019 verplicht gesteld.
In de BIO zijn op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Vervolgens definieert de BIO maatregelen per BBN (1,2 of 3) die getroffen zouden moeten worden.

3.1.1 *Op diverse momenten is de eis voor vertrouwelijkheid van het nieuwe donorregister vastgesteld maar middels Quickscans*

Tijdens het onderzoek hebben we geen actuele risicoanalyse en geen informatiebeveiligingsplan voor Dora ontvangen. Dit wijkt af van het beleid dat CIBG definieert in het Beleidsdocument informatieveiligheid CIBG (november 2018).
Wel is een memo van CIBG ontvangen: "Toelichting op informatie t.b.v. onderzoek ADR" d.d.8 mei 2020 aan ons gericht. Hierin staat het volgende vermeld: "In 2018 zijn we gestart met het project Actieve Donor Registratie (ADR) om een nieuw Donorregister te ontwikkelen. Voorafgaand aan de start van dit project is een Quick Scan Informatie Beveiliging Donorregister uitgevoerd. Een van de belangrijkste conclusies was dat alleen de 'Beschikbaarheidseisen' boven BIR-niveau waren."

We hebben een uitgevoerde QuickScan Informatiebeveiliging Donorregister (QS), december 2017, ontvangen. Daarin is aangegeven dat het vereiste niveau ten aanzien van Vertrouwelijkheid "hoog" is. Als argument wordt gegeven: Het betreft Wbp risicoklasse II persoonsgegevens die in het systeem staan opgeslagen. Het schenden van de vertrouwelijkheid van wilsbeschikkingen kan schade toebrengen aan het ministerie.

Gegevensbeschermingseffectbeoordeling (PIA) is aangetroffen
Voorts hebben wij ook een gegevensbeschermingseffectbeoordeling (PIA), mei 2020, ontvangen dit betreft het nieuwe Donor register. Een Privacy Impact Assessment (PIA) is een instrument waarmee organisaties privacyrisico's in een vroegtijdig stadium op een gestructureerde en heldere manier in kaart wordt gebracht.
Het uitvoeren van een PIA is sinds 2014 verplicht bij de ontwikkeling van een nieuw systeem. Bij risicoafweging in het kader van informatiebeveiliging is gericht op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), bij een PIA is de risicoafweging gebaseerd op de risico's voor de betrokkenen.

3.1.2 *Meest recente vertrouwelijkheidseis is vastgesteld op hoog*

In reactie op het concept rapport laat CIBG zien dat er op 2 juli 2020 een nieuwe quickscan is vastgesteld. De vertrouwelijkheidseis is daarin op 'hoog' aangegeven (op een schaal van laag. midden, hoog en zeer hoog). Tevens is bepaald dat het Donorproces 'strategisch' is en het informatiesysteem 'ondersteunend' is. Deze combinatie leidt ertoe dat de eis voor vertrouwelijkheid het standaard niveau van beveiliging, zoals dat binnen de overheid geldt, afdoende is.

3.2 Samenvatting bevindingen voor vraag twee

Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?

In de meest recent uitgevoerde quickscan is de vertrouwelijkheidseis 'hoog' aangegeven (op een schaal van laag. midden, hoog en zeer hoog). Tevens is bepaald dat het Donorproces 'strategisch' is en het informatiesysteem 'ondersteunend' is. Aangegeven is dat deze combinatie ertoe leidt dat voor de eis aan vertrouwelijkheid het standaard niveau van beveiliging, zoals dat binnen de overheid geldt, afdoende is.

3.3 Inventarisatie bedrijfsmiddelen voor het nieuwe donorsysteem niet aangetroffen

Deze paragraaf geeft antwoord op Vraag 3 *Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?*
In het oude beveiligingsplan van het Donorregister (2005) hebben wij deze, inmiddels wel verouderde, inventarisatie aangetroffen. Voor het nieuwe systeem hebben wij een dergelijke inventarisatie niet aangetroffen.

Op basis van beschikbare documentatie, met name de PIA, hebben we een groot aantal bedrijfsmiddelen kunnen inventariseren:

Fysieke / digitale documenten

- Binnengekomen papieren registratie / formulier
- Te verzenden voor ingevulde registratie formulieren
- Herinneringsbrief
- Records van maximaal 5 mb
- Steekproef (De steekproef bestaat uit printproeven in de vorm van PDF's.)
- Mailpacks
- Gescande juiste formulieren
- Gescande onjuiste formulieren
- Registratiebevestiging: naam en adresgegevens. gemaakte keuze en geldigheidsdatum van de registratie van belang (Het BSN niet)
- Brief (BD Apeldoorn verstuurt een brief, die betrekking heeft op het foutief ingevulde registratieformulier, en een nieuw gepersonaliseerd registratieformulier).

Qua informatiesystemen en middelen

- Dora (Registratie in Donorregister Dora.),
- Dora (data vanuit het koppelvlak direct naar Dora),
- Rappelbestand,
- correspondentietool (adres en vervolgactie in een correspondentietool),
- beleidsrapportages: Het generen van registratiegegevens voor beleidsdoeleinden (zoals bijvoorbeeld hoeveel mensen zich actief hebben geregistreerd met welke keuze en hoe is het verdeeld over een aantal leeftijdsgroepen en/of gemeentecode gebied in Nederland),
- e-mail toepassing gebruikmakend van Haagse Ring,
- koppelvlak (Het koppelvlak regelt het digitale verkeer (beveiligd via IP-filtering)),
- Haagse Ring,
- servers etc. bij leverancier (KPN),
- printer (voor het gepersonaliseerde registratieformulier),
- apparaat samenvoegen (mailpack samen (brief, registratieformulier, invulinstructie en retourenvelop),
- machines voor Uitpakken, controleren en sorteren registratieformulier
- machines voor printen en gereedmaken registratiebevestiging in BD Apeldoorn.

Vanuit de documentatie leiden wij af dat meerdere partijen betrokken zijn bij het nieuwe Donorregister. Dit zijn

- Belastingdienst Apeldoorn,
- Belastingdienst Heerlen,
- Reiswolff,
- PostNL,
- NTS (afnemer),
- KPN

3.4 Samenvatting bevindingen voor vraag drie

Vraag 3: *Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?*
ADR heeft tijdens het onderzoek geen inventarisatie van onderkende bedrijfsmiddelen voor Dora aangetroffen. Op basis van diverse documentatie zien wij de volgende bedrijfsmiddelen:

Fysieke / digitale documenten

- Binnengekomen papieren registratie / formulier
- Te verzenden voor ingevulde registratie formulieren
- Herinneringsbrief
- Records van maximaal 5 mb
- Steekproef (De steekproef bestaat uit printproeven in de vorm van PDF's.)
- Mailpacks
- Gescande juiste formulieren
- Gescande onjuiste formulieren
- Registratiebevestiging: naam en adresgegevens. gemaakte keuze en geldigheidsdatum van de registratie van belang (Het BSN niet)
- Brief (BD Apeldoorn verstuurt een brief, die betrekking heeft op het foutief ingevulde registratieformulier, en een nieuw gepersonaliseerd registratieformulier).

Qua informatiesystemen en middelen

- Dora (Registratie in Donorregister Dora.),
- Dora (data vanuit het koppelvlak direct naar Dora),
- Rappelbestand,
- correspondentietool (adres en vervolgactie in een correspondentietool),
- beleidsrapportages: Het generen van registratiegegevens voor beleidsdoeleinden (zoals bijvoorbeeld hoeveel mensen zich actief hebben geregistreerd met welke keuze en hoe is het verdeeld over een aantal leeftijdsgroepen en/of gemeentecode gebied in Nederland),
- e-mail toepassing gebruikmakend van Haagse Ring,
- koppelvlak (Het koppelvlak regelt het digitale verkeer (beveiligd via IP-filtering)),
- Haagse Ring,
- servers etc. bij leverancier (KPN),
- printer (voor het gepersonaliseerde registratieformulier),
- apparaat samenvoegen (mailpack samen (brief, registratieformulier, invulinstructie en retourenvelop),
- machines voor Uitpakken, controleren en sorteren registratieformulier
- machines voor printen en gereedmaken registratiebevestiging in BD Apeldoorn.

Vanuit de documentatie leiden wij af dat meerdere partijen betrokken zijn bij het nieuwe Donorregister. Dit zijn

- Belastingdienst Apeldoorn,
- Belastingdienst Heerlen,
- Reiswolff,
- PostNL,
- NTS (afnemer),
- KPN

3.5 Invulling van maatregelen voor het nieuwe donorregister

In onderstaande paragrafen tot en met paragraaf 3.11 wordt antwoord gegeven op vraag 4:*Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?*
De maatregelen die van belang zijn voor vertrouwelijkheid van Dora zijn in beschouwing genomen. Dit zijn maatregelen met betrekking tot

- het ontwerp en ontwikkeltraject van Dora (paragraaf 3.5.1),
- het beheer van verwijderbare (externe) gegevensdragers (paragraaf 3.5.2)
- de toegangsbeveiliging voor Dora (paragraaf 3.5.3 tot en met 3..5.7),
- personeel (paragraaf 3.5.8)
- overeenkomsten met externe partijen (paragrafen 3.6 tot en met 3.7)

3.5.1 *De maatregelen die de beveiliging van het nieuwe donorregister bekrachtigen, zijn benoemd in de Project Start Architectuur*

Tijdens ons onderzoek hebben we een memo van CIBG ontvangen: "Toelichting op informatie t.b.v. onderzoek ADR". Hierin staat aangegeven dat

> "de conclusie uit de Quickscan in 2018 meegenomen is in de ontwikkeling van het nieuwe Donorregister, waarbij in de Project Start Architectuur (PSA) in hoofdstuk 5 de eisen rondom de beveiliging van het nieuwe systeem staan beschreven. Zo mogen er in de testomgeving geen persoonsgegevens gebruikt worden, wordt autorisatie gecontroleerd en gedefinieerd, voldoet het systeem aan de eisen van de BIR en moet worden voldaan aan de richtlijnen van de CIBG_secure_software_development V2_5.pdf."

In de PSA is het toepassen van de Always Encrypted functie voor dataencryptie in de database aangegeven.
In opzet komen we goede principes tegen voor de ontwikkeling van Dora.
Voor een overzicht zie bijlage 2.

Tevens hebben wij Security Requirements binnen Secure Software Development tijdens ons onderzoek ontvangen. Hierin staat "Overheidsorganisaties zijn zelf verantwoordelijk voor het borgen van het beveiligingsniveau in de eigen organisatie, informatiesystemen en het implementeren en uitvoeren van beveiligings-maatregelen. Ter ondersteuning van dit proces en ter waarborging van een verhoogd beveiligingsniveau bevat dit document de *richtlijnen* voor informatiebeveiliging van webapplicaties."
Dit document geeft aan hoe deze kwetsbaarheden kunnen worden voorkomen of de schade door misbruik van de kwetsbaarheden kan worden beperkt. Een ontwikkelaar dient deze richtlijnen toe te passen in zijn of haar ontwikkelproject(en)".
We hebben geen uitwerking van (selectie van) deze richtlijnen aangetroffen die zijn beschreven voor de Dora specifieke organisatie. Dit document geeft niet aan welke maatregelen daadwerkelijk zijn getroffen, of getroffen moeten worden in het nieuwe donorregister.

Ons onderzoek vond plaats voor 1 juli, het nieuwe systeem was nog niet operationeel. Wij hebben in ons onderzoek niet getoetst of al deze principes zijn toegepast voor Dora.

Acceptatiecriteria van het project en ontwikkelteam hebben wij ontvangen. Deze criteria zijn veelomvattend en in enkele gevallen wordt aangegeven dat er externe toets moet plaatsvinden. Wij hebben geen stukken aangetroffen dat deze acceptatiecriteria (in- en of extern) zijn getoetst. Wij hebben daarom ook geen inzicht of aan de acceptatiecriteria wordt voldaan. In reactie geeft CIBG aan dat "*een penetratietest uitgevoerd om te checken of aan alle beveiligingseisen is voldaan. Hier zijn een paar kleine bevindingen uit gekomen die inmiddels zijn opgelost. Direct na oplevering van het systeem in productie wordt een hertest gedaan. Deze is inmiddels uitgevoerd en er zijn geen bevindingen meer.*

- *De Software Improvement Group (SIG) heeft de software getoetst o.a. op de toepassing van beveiligingseisen.* " Wij hebben dit niet nader onderzocht.

3.5.2 *Maatregelen ten aanzien van verwijderbare (externe) gegevensdragers bij CIBG beperkt aangetroffen*

In de BIO staat onder paragraaf 8.3.1 de volgende beheersdoelstelling:
Beheer van verwijderbare (externe) media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.

Wij hebben ten aanzien van de door ons geïnventariseerde bedrijfsmiddelen geen specifieke procedures aangetroffen. Mogelijk zijn die er wel maar voor ons niet heel duidelijk herkenbaar. Wij verwachten dat gelet het ontvangen memo van CIBG dat CIBG dit overzicht met haar eigen review werkzaamheden zal verkrijgen. Er staat "Met het oog op het live gaan van het nieuwe systeem op 1 juli 2020 voert het CIBG een interne review uit, bestaande uit:
- interviews
- een toets op de aantoonbaarheid van het voldoen aan de nu geldende baseline."

In reactie geeft CIBG aan dat de interne review tot het volgende heeft geleid:"
1. Geen gebruik van externe gegevensdragers;
2. Beveiligingsplannen aangepast
3. Verwerkersovereenkomsten scherper formuleren
4. Heldere governance intern
5. Awareness en opleiding
6. Verantwoording aan DT

Daarnaast is er een BIO GAP-analyse gemaakt, waarvan we de openstaande punten meenemen in het nieuwe Donorregister."

ADR heeft deze uitkomsten van de review en de exacte duiding niet nader onderzocht.

3.5.3 *Maatregelen toegangsbeveiliging CIBG*

In de BIO staan in hoofdstuk 9 maatregelen beschreven voor toegangsbeveiliging.

3.5.4 *Opzet autorisaties voor het nieuwe register (Dora) aangetroffen*

We hebben een document ontvangen "Rollen en bevoegdheden in Dora" daarin is de opzet van de autorisaties aangegeven. Autorisaties zijn gekoppeld aan de volgende rollen: Frontoffice medewerker (Raadpleger_Donor), Backoffice medewerker behandelaar (Behandelaar_Donor), Backoffice medewerker toetser (SeniorBehandelaar_Donor), Functioneel beheerder (Beheerder_Donor).

Per rol staan toegestane functionaliteiten aangegeven. Het valt op dat
- raadplegen van logging niet als activiteit is aangegeven.
- de Functioneel beheerder rechten heeft om
  - vier-ogen principe uit te zetten terwijl niet uit de functionaliteiten blijkt dat er vier-ogen principe van toepassing is (bijv. 1e muteerder, 2e muteerder);
  - de rapportage ten aanzien van raadplegen door NTS te bekijken. Echter de rol 'NTS raadpleger oid' is niet aangegeven. In reactie geeft CIBG aan dat functioneel beheerder via deze rapportage kan zien hoe vaak per periode de NTS een raadpleging middels de web koppeling heeft gedaan.

3.5.5 *Geactualiseerde PIA in overeenstemming met het ontvangen document "Rollen en bevoegdheden in Dora".*

In de uitgevoerde PIA van het nieuwe Donorregister staat:
In totaal hebben 122 medewerkers (rollen) van het CIBG en NTS, namelijk Functioneel Beheerders, Medewerkers Klant Contactcenter, Registratiemedewerkers (Scan en NTS), toegang tot de persoonsgegevens.
In de PIA staat aangegeven dat deze personen een geheimhoudingsverklaring hebben ondertekend. In reactie heeft CIBG aangegeven dat de PIA van 10 juni 2020

is aangepast en dat in de nieuwe versie van de PIA staat aangegeven dat maximaal 40 medewerkers toegang tot Dora hebben en dat NTS het systeem niet meer raadpleegt middels een autorisatie in het systeem. Raadpleging verloopt via koppeling met een webservice. We hebben hier geen nader onderzoek naar gedaan.

3.5.6 *Controle toegangsrechten Dora in opzet aangetroffen*

Tijdens ons onderzoek hebben wij een procedure ontvangen waarin wordt aangegeven op welke wijze autorisaties voor CIBG-systemen worden beheerd. Zoals het uitreiken van autorisaties en periodieke controle op autorisaties.

In de nieuwe samenwerkingsafspraken tussen CIBG en NTS staat beschreven dat NTS bij het nieuwe Donorsysteem op een andere wijze toegang krijgt tot de Donorgegevens. Toegang tot de gegevens wordt verleend middels een Webservice naar het Vita-systeem van NTS. NTS is een eigen verwerkingsverantwoordelijke op het moment waarop zij de gegevens raadplegen.

3.5.7 *Opzet maatregelen toegangsbeveiliging voor overige bedrijfsmiddelen binnen CIBG niet expliciet aangetroffen*

Net als de bevinding zoals beschreven bij paragraaf 3.5.2 verwijzen wij naar de memo waarin staat dat CIBG ten tijde van ons onderzoek een review uitvoert.

3.5.8 *Maatregelen Personeel van CIBG zijn onveranderd van de situatie zoals beschreven in paragraaf 2.3.2*

De maatregelen die wij hebben aangetroffen zijn reeds beschreven in paragraaf 2.3.2. De maatregelen ten aanzien van het personeel van CIBG zullen niet veranderen bij de invoering van het nieuwe systeem. Deze maatregelen zijn reeds beschreven in paragraaf 2.3.2

3.6 Maatregelen in overeenkomsten met externe partijen

In paragraaf 3.7 zijn de maatregelen in de overeenkomst met de Belastingdienst Heerlen beschreven.
In paragraaf 3.8 zijn de maatregelen in de overeenkomst met de Belastingdienst Apeldoorn beschreven.
In paragraaf 3.9 zijn de maatregelen in de overeenkomst met de Hosting partij beschreven.

3.7 Overeenkomst met Belastingdienst Heerlen (BD-H) kent maatregelen voor vertrouwelijkheid maar verbetering is mogelijk

In het 'Implementatieplan Wet op Orgaandonatie van Belastingdienst' zijn maatregelen voor vertrouwelijkheid opgenomen

Met de Belastingdienst -Heerlen is een opdracht overeengekomen (Implementatie plan van WOD (versie 3.0 datum na 8 april 2020 (D.4.6))) aangaande het ontvangen van gestructureerde retourenveloppen met gestructureerde retourdocumenten in het kader van de uitvoering van de Wet op Orgaandonatie en het scannen daarvan en beschikbaar stellen aan CIBG.

Wij treffen geen ondertekening aan in dit implementatieplan. In het implementatieplan van WOD (versie 3.0 datum na 8 april 2020) herkennen wij maatregelen die betrekking hebben op de vertrouwelijkheid van het Donorregister. We hebben ze hieronder kort aangegeven:

3.7.1 *Opzet van maatregelen aangetroffen voor digitale bestanden en uitwisseling daarvan*

- De ingescande bestanden worden als ZIP-bestand middels een beveiligde site geupload naar CIBG. Tevens is voorzien in een checksum (MD5) (uitwisseling informatie) .
- De productiebestanden blijven tot 3 maanden na oplevering aan de opdrachtgever gearchiveerd op de server. Na deze 3 maanden worden deze bestanden op de server geautomatiseerd geschoond. Dit is onherroepelijk.

3.7.2 *Maatregelen voor vernietiging fysiek archief BD-H aangetroffen*

- Er wordt voorzien in een tijdelijke opslag (met aparte nummering) in een apart gedeelte van het archief. Na opdracht van de opdrachtgever worden de fysieke documenten vernietigd. Dit betreft een gecertificeerde vernietiging door de firma Reiswolff. Het verslag van vernietiging wordt opgeleverd aan de opdrachtgever. Vernietiging is onherstelbaar.
- Na afronding van het gehele project stelt de opdrachtnemer een verklaring op dat alle fysieke documenten en digitale bestanden onherstelbaar zijn vernietigd.

  Observatie ADR: Het is onduidelijk of bij afronding van het project ook onderliggende bewijzen worden geleverd ten behoeve van gecertificeerde vernietiging. Tevens is het onduidelijk hoe bepaald wordt, wanneer het project is afgerond.
  In reactie op het concept rapport geeft CIBG aan dat het project in 2021 afgerond zal zijn en dat in het projectcontract staat aangegeven wanneer het project beëindigd kan worden. We hebben hiernaar geen nader onderzoek gedaan.

Tijdens interview gaf CIBG aan dat Belastingdienst scant voor ons en doet de verwerking voor nieuwe systeem. BD maakt een backup. De formulieren staan tijdelijk bij de Belastingdienst. Als CIBG digitaal archief heeft dan wordt papier vernietigd. Deze informatie sluit niet geheel aan op de afspraken die wij hebben aangetroffen. Volgens deze informatie wordt het papier vernietigd *na* opdracht van de opdrachtgever.

3.7.3 *Maatregelen voor externe gegevensdragers aangetroffen, maar deze verdienen verduidelijking*

- De productiebestanden blijven, na oplevering aan de opdrachtgever, ook gedurende 3 maanden gearchiveerd op USB Storage. De bestanden worden na 3 maanden vernietigd. (De storage wordt 2x geformatteerd) Dit is onherroepelijk. Deze storages worden zeker niet fysiek overgedragen aan de opdrachtgever.

  Observatie ADR: Hierbij is niet aangegeven of de USB Storage
  - beveiligd /versleuteld is,
  - op welke wijze de USB bewaard wordt en
  - op welke wijze voorkomen wordt dat deze niet gedupliceerd wordt.

Wij bevelen aan hierover expliciete afspraken te maken.

Voorts is het onduidelijk waarom deze USB storage is aangeduid als "aflevermedium" als elders in het plan staat dat oplevering plaatsvindt via een beveiligde site.

Een toelichting van CIBG leert dat het scannen op een standalone omgeving plaatsvindt. Vervolgens worden de gescande documenten middels een USB Storage overgezet naar een beveiligde site. Tevens is in reactie aangegeven dat de USB storages niet beveiligd zijn en bewaard worden in een kluis en dat deze kluis slechts toegankelijk is voor enkele personen, waarmee voorkomen wordt dat gegevens gedupliceerd worden.
Wij bevelen aan om in overweging te nemen om dit explicieter te beschrijven en te overwegen of deze werkwijze passend is en voldoende waarborgen biedt voor de gegevens.

3.7.4 *Autorisatiemaatregelen beperkt aangetroffen*

Bij autorisaties is aangegeven:
- Extra autorisatie noodzakelijk voor het samenwerkingsgebied voor de aflevering van de digitale bestanden.

Observatie ADR: Onduidelijk dat geen autorisatie wordt aangegeven of benodigd is om bestanden op de server of op de USB te plaatsen.

Elders treffen wij gepaste maatregelen (autorisaties) t.a.v. Archief aan.
Wij herkennen de volgende maatregelen:
- Het archief waar de fysieke documenten tijdelijk worden opgeslagen is extra beveiligd en slechts toegankelijk voor een beperkt aantal medewerkers van de Belastingdienst.
  Hiervoor is een specifieke gradatie ingericht op de Rijkspas. Toegang wordt gelogd. Onder voorwaarden kunnen deze gegevens worden opgevraagd.
- De ruimte waarin de servers staan waarop de digitale documenten tijdelijk worden opgeslagen, is extra beveiligd en slechts toegankelijk voor een beperkt aantal medewerkers van Belastingdienst. Hiervoor is een specifieke gradatie ingericht op de Rijkspas. Toegang wordt gelogd. Onder voorwaarden kunnen deze gegevens worden opgevraagd.

3.7.5 *Maatregelen t.a.v. personeel aangetroffen maar niet heel overzichtelijk*

Een aantal maatregelen ten aanzien van personeel is aangegeven:
- Afhankelijk van het aanbod zal extra personeel (inhuur) worden ingezet. Ingehuurd personeel voldoet aan de binnen de Belastingdienst geldende regels voor inhuur.

  Observatie ADR: Het is niet duidelijk welke regels er gelden voor inhuur binnen de Belastingdienst. In reactie op het concept rapport geeft CIBG aan dat de nieuwe overeenkomsten met de Belastingdienst hierop worden aangepast. Dit is in dit onderzoek niet verder onderzocht.

Beveiliging
Onder beveiliging is onder andere aangegeven dat

- verwerking plaatsvindt uitsluitend door medewerkers met een VOG die een geheimhoudingsverklaring hebben afgelegd.

  Observatie ADR: Onduidelijk waarom dit niet aanvullend onder Personeel is opgenomen. In reactie op het concept rapport geeft CIBG aan dat dit in de nieuwe overeenkomsten met de Belastingdienst wordt aangepast. Dit is niet verder onderzocht.

  Observatie ADR: kopje beveiliging is nog niet geheel uitgewerkt ten aanzien van de jaarlijkse audit.

3.7.6 *Maatregelen zijn onderkend, maar moeten nog uitgewerkt worden.*

Tijdens ons onderzoek kwam naar voren dat maatregelen nog niet geheel zijn uitgewerkt. Voorbeelden hiervan zijn:

- Ingevulde formulieren: "Deze zullen wel tijdelijk (aantal weken) in het archief van de scanlocatie bewaard moeten blijven. Er worden nog afspraken gemaakt over het digitaal archiveren en vervolgens vernietigen van het papieren archief." In de toekomst zal gebruik worden gemaakt van een documentmanagement systeem, dit is op dit moment nog niet aanwezig.
- In interview is aangegeven dat gegevens uit het oude systeem worden gemigreerd naar nieuwe systeem. Odisys stopt te bestaan. Het oude systeem wordt afgebouwd, zodat er geen gegevens meer inzitten. Dit plan is er nog niet. Aangegeven is dat de focus ligt op de start van het nieuwe systeem.

3.8 Service Niveau Afspraken (SNA) met Belastingdienst Apeldoorn

Tijdens het onderzoek hebben wij een concept ontvangen van Service Niveau Afspraken met de Belastingdienst Apeldoorn. Dit betreft werkzaamheden aangaande bouw printprogramma's, printen, couverteren (envelopperen) en verzenden van ontvangen opdrachten.

3.8.1 *Diverse maatregelen zijn niet specifiek gemaakt.*

In het document staat dat "voor de informatiebeveiliging dezelfde richtlijnen gehanteerd zullen worden die ook voor de processen van de Belastingdienst gelden. We doen dit door het treffen van de noodzakelijke organisatorische, procedurele en technische maatregelen die gebaseerd zijn op een (organisatieafhankelijke) risicoanalyse of een wettelijke verplichting."

Specifieke bedrijfsmiddelen die ingezet worden voor deze dienstverlening, worden beperkt genoemd. Maatregelen of waarborgen die van belang zijn voor de vertrouwelijkheid van de gegevens van het Donorregister (zoals adreslijsten) treffen wij nauwelijks aan.
Voorbeelden hiervan zijn:

- maatregelen aangaande digitale bestanden, er zijn geen specifiek maatregelen aangetroffen voor uitwisseling, opslag, autorisatie en (tijdige) verwijdering van de bestanden,
- maatregelen personeel zoals een VOG zijn niet expliciet opgenomen,
- maatregelen voor gebruik van externe gegevensdragers indien deze gebruikt worden.

Deze concept SNA is voorzien in ondertekening door *afdelingshoofd* CIBG. Wij hadden verwacht dat de productmanager Donorregister hiervoor verantwoordelijk is en daarom ook ondertekent.
CIBG geeft in reactie op het conceptrapport aan dat er een taskforce is opgestart waarin een heldere rolverdeling wordt uitgewerkt. Wij hebben hier geen nader onderzoek naar gedaan.

3.9 Overeenkomst met hostingpartij kent maatregelen voor vertrouwelijkheid

In de overeenkomst met hostingpartij staat:
"Producten die wel door CIBG voor een van haar cliënten worden beheerd, maar die niet gebaseerd zijn op de CIBG architectuur dienen ook gehost te kunnen worden. CIBG staat toe dat Internedservices voor deze producten *een derde partij* inzet. Het betreft: RedHat Linux, MySQL, PHP, Hippo, Java applets en Apache, Splunk".

Het is voor de ADR onbekend of dit producten zijn die voor Dora worden ingezet. Indien dat zo is, zal moeten beoordeeld worden of dit in een verwerkersovereenkomst moet worden verwerkt.
CIBG geeft in reactie op het concept rapport aan dat dit in de verwerkersovereenkomsten na 1 juli is geregeld. Dit hebben wij niet nader onderzocht.

Voorts is opgenomen dat de hostingpartij zich conformeert aan de "Gedragscode Retransitie" versie 1.2. zoals op 15 mei 2014 is vastgesteld door het Platform Outsourcing Nederland (PON). Het is de ADR niet duidelijk of hiermee de vertrouwelijkheid van de gegevens gewaarborgd is. Het teruggeven van gegevens is van belang maar voor de vertrouwelijkheid is ook van belang dat de gegevens niet (gekopieerd) achterblijven. CIBG geeft in reactie op het concept rapport aan dat dit in de verwerkersovereenkomsten na 1 juli is geregeld. Dit hebben wij niet nader onderzocht.

3.9.1 *Maatregelen ten aanzien van autorisaties hostingpartij in opzet aanwezig*

In de DAP staan afspraken betreffende autorisaties op hoofdlijnen opgenomen.

- Alle gebruikers en beheeraccounts die door hostingpartij worden gebruikt, dienen als zodanig te zijn gelabeld;
- Alle service accounts dienen als zodanig te zijn gelabeld;
- Alle gebruikersaccounts die niet expliciet op naam zijn gesteld dienen als zodanig te zijn gelabeld;
- Alle accounts met verhoogde privileges dienen als zodanig te zijn gelabeld;
- Alle ongebruikte leveranciers accounts dienen te worden geblokkeerd;
- Alle ongebruikte CIBG accounts dienen in overleg te worden geblokkeerd;
- Er wordt actief gemonitord op conflicterende rollen binnen de beheeromgeving;
- Blokkade van ongebruikte accounts vindt na 45 dagen plaats;
- Verwijdering van ongebruikte accounts vindt na 120 dagen plaats.
- Rapportage over Toegang Loginformatie kan worden aangevraagd.

Overweeg of deze maatregelen afdoende zijn, deze maatregelen bieden geen waarborgen over welke rechten de beheerders daadwerkelijk toepassen. En of het bijvoorbeeld mogelijk is om ongehinderd kopieën van data te maken.

3.9.2 *Maatregelen t.a.v. Personeel bij hostingpartij in opzet aangetroffen*

In DAP is onder andere aangegeven dat van alle ten behoeve van de aan CIBG te leveren diensten werkzame medewerkers met mogelijke toegang tot CIBG gegevens een geheimhoudingsverklaring en een Verklaring Omtrent Gedrag hebben getekend.

3.9.3 *Een aantal maatregelen bij de hostingpartij is niet aangetroffen*

Voorbeelden daarvan zijn:

- Maatregelen voor digitale bestanden en uitwisseling daarvan niet aangetroffen. Er zijn geen maatregelen ten aanzien van uitwisseling van digitale bestanden aangetroffen. Denk hierbij ook aan vertrouwelijke (incident) rapportages of specifieke testen.
- Er zijn geen maatregelen aangetroffen ten aanzien van fysiek archief. Het is niet waarschijnlijk dat er een fysiek archief wordt aangehouden bij de hostingpartji. CIBG stelt dat er met zekerheid geen fysiek archief aanwezig zal zijn bij KPN.
- Maatregelen over het gebruik van externe gegevensdragers worden niet aangetroffen. Mogelijk wordt er geen gebruik gemaakt externe

gegevensdragers. ADR adviseert om dit expliciet op te nemen in de afspraken met de hostingpartij.

3.10 Samenvatting bevindingen vraag vier

Deze paragraaf is een samenvatting van de bevindingen voor vraag vier.
Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?

Wij hebben ten aanzien voor de door ons geïnventariseerde bedrijfsmiddelen geen specifieke procedures aangetroffen. Mogelijk zijn die er wel maar voor ons niet heel duidelijk herkenbaar. Wij verwachten dat gelet het ontvangen memo van CIBG dat CIBG dit overzicht met haar eigen review werkzaamheden zal verkrijgen. Er staat "Met het oog op het live gaan van het nieuwe systeem op 1 juli 2020 voert het CIBG een interne review uit, bestaande uit:
- interviews
- een toets op de aantoonbaarheid van het voldoen aan de nu geldende baseline."
ADR heeft deze uitkomsten van de review en de exacte duiding op dit moment niet nader onderzocht.

Een aantal maatregelen, die bijdragen aan de vertrouwelijkheid van het nieuwe donorregister i.c. het systeem zelf is in de ontvangen documentatie aangetroffen. Voorbeelden zijn de maatregelen in de Project Start Architectuur met daarin verwijzing naar het toepassen dan database encryptie, de Secure Software Development documentatie en de opzet van de inrichting van de autorisaties van het nieuwe systeem.

De maatregelen ten aanzien van personeel van CIBG zullen niet veranderen bij de invoering van het nieuwe systeem. Deze maatregelen zijn reeds beschreven in paragraaf 2.3.2

De maatregelen die wij aantreffen in de actuele afspraken met leveranciers, zoals Belastingdienst Heerlen (BD-H), Belastingdienst Apeldoorn (BD-A) en de hostingpartij, zijn divers. In de meeste gevallen worden maatregelen ten aanzien van autorisatiebeheer en personeel onderkend. Echter maatregelen voor de omgang met externe gegevensdragers of voor vernietiging van gegevens worden niet altijd beschreven. Door de afwezigheid van een informatiebeveiligingsplan voor het nieuwe Donorregister hebben we bij CIBG niet alle maatregelen aangetroffen. In onderstaande tabel is globaal aangegeven of wij de maatregelen in opzet hebben aangetroffen (beschreven zijn).
Een * betekent maatregelen aangetroffen, maar er zijn nog aandachtspunten.

	Opzet maatregelen afspraken met leveranciers			
Maatregelen in het kader van	CIBG	BD-H	BD-A	Hosting partij
Autorisatiebeheer (BIO 9)	Aangetroffen	Aangetroffen*	Niet aangetroffen	Aangetroffen
Beheer bedrijfsmiddelen				
Uitwisseling van bestanden	n.v.t.	Aangetroffen*	Niet aangetroffen	Niet aangetroffen
Externe gegevensdragers (BIO 8)	Niet expliciet aangetroffen	Aangetroffen*	Niet aangetroffen	Niet aangetroffen
Vernietiging archief	Niet expliciet aangetroffen	Aangetroffen*	Niet aangetroffen	Niet aangetroffen*
Personeel				
VOG	Aangetroffen	Aangetroffen	Beperkt aangetroffen	Aangetroffen

4 Handelingsperspectief

In dit hoofdstuk wordt handelingsperspectief gegeven voor het Donorregister ten aanzien van informatiebeveiliging in het algemeen en heel specifieke adviezen ten aanzien van de Algemene Verordening Gegevensbescherming voor het Donorregister.

4.1 Actualiseer informatiebeveiligingsplan en maatregelen voor informatiebeveiliging Donorregister en zie toe op naleving

Gelet op de bevindingen is het handelingsperspectief breder dan alleen de omgang met externe gegevensdragers. De maatregelen voor externe gegevensdragers zijn onderdeel van het informatiebeveiligingsplan. We adviseren conform het beleid voorschrijft een actuele risico analyse uit te voeren. Geef daarbij extra aandacht op de rol van het systeem in het proces. In de meest recente versie van de quickscan is het geïnventariseerd als *ondersteunend* systeem voor een strategisch proces. Actualiseer op basis van deze risico analyse het informatiebeveiligingsplan voor het donorregister. Dit plan zal gelang de situatie betrekking moeten hebben op het oude èn het nieuwe donorregister.
Als onderdeel van de werkzaamheden voor het actualiseren van dit plan adviseren wij

- inzichtelijk te maken welke bedrijfsmiddelen (en daarmee ook mogelijk externe gegevensdragers) worden gebruikt voor het nieuwe donorregister en oude donorregister en deze op te nemen in het beveiligingsplan. Vervolgens zal geclassificeerd moeten worden welke beveiligingseisen, waaronder de hoogte van vertrouwelijkheid, voor de betreffende bedrijfsmiddelen in relatie tot het nieuwe donorregister vereist zijn. En welke maatregelen daarvoor passend zijn en wie verantwoordelijk is voor betreffende bedrijfsmiddel / uitvoeren van de maatregelen;
- te zorgen dat dit plan aansluit op het actuele beleidsplan van CIBG en op de meest recente versie van het BIO;
- om (verwijzingen naar) passende (nieuwe en bestaande) maatregelen op te nemen ten einde afdoende bescherming te bieden en op welke wijze verantwoordelijkheden belegd zijn;
- dit plan bij veranderingen, maar zeker minimaal jaarlijks, te reviewen en te actualiseren;
- te verwijzen naar of integreren van maatregelen die vanuit de AVG worden verwacht (voor heel specifieke adviezen zie ook paragraaf 4.2).

Ten aanzien van de aangetroffen situatie zoals in dit rapport aangegeven en de uitkomsten van de te treffen maatregelen bevelen wij aan om bestaande afspraken met leveranciers te heroverwegen.
Voorts attenderen wij u op de maatregel die in de BIO genoemd staat, betreffende naleving (18.2.2.) en deze na te leven: "De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging."

4.2 Specifiek handelingsperspectief lettende op Algemene Verordening Gegevensbescherming

Als gevolg van het mogelijke verlies van de externe gegevensdragers zijn mogelijk ook persoonsgegevens verloren gegaan. Teneinde inzicht te krijgen in de waarborgen voor de vertrouwelijkheid van de persoonsgegevens is de AVG in

beschouwing genomen. Resultaten van de beschouwing leest u in bijlage 1. Hieronder zijn de adviezen opgenomen.

4.2.1 *Bewaak uniformiteit persoonsgegevens*

CIBG heeft per juli 2020 bij de in gebruik name van het nieuwe Donorregister DORA, aanpassingen doorgevoerd in de soort persoonsgegevens.
De ADR adviseert CIBG om goede afwegingen te blijven maken bij de informatie die wordt verwerkt en onderbouwingen daarvan vast te leggen. Tevens is het goed om de uniformiteit van de persoonsgegevens en andere informatie in verwerkersovereenkomsten/c.q. -afspraken en het register van verwerkingen te bewaken.

4.2.2 *Toegang tot persoonsgegevens blijvend monitoren*

Tot juli 2020 hadden 122 medewerkers van het CIBG en de Nederlandse Transplantatie Stichting (NTS), toegang tot de persoonsgegevens in het Donorregister, dit was niet overeenkomstig de informatie hierover uit de brochure. Per juli 2020 is dit aantal tot maximaal 40 CIBG-medewerkers teruggebracht. De directe toegang tot het donorregister door medewerkers van NTS, Eurotransplant, KPN en de belastingdiensten Heerlen en Apeldoorn, de autorisaties van deze partijen zijn door CIBG geduid en aangescherpt.
De ADR adviseert om de getroffen maatregelen blijvend te monitoren, afwegingen in dit kader te blijven maken en hierover transparant te communiceren.

4.2.3 *Actualiseer en inventariseer (potentiële) verwerkersovereenkomsten*

De ADR heeft vastgesteld dat de *verwerkersovereenkomsten-/afspraken* met KPN en de belastingdienst Heerlen en Apeldoorn niet op orde zijn en dat CIBG halfjaarlijkse controles wil gaan toepassen op de actualiteit van verwerkers.
De ADR adviseert CIBG om een omgevingsverkenning uit te voeren m.b.t. de (keten-)partners met wie CIBG voor het Donorregister samenwerkt en met wie deze (keten-)partners zelf samenwerkingsverbanden onderhouden in relatie tot het Donorregister. Van daaruit kan de analyse plaatsvinden wie persoonsgegevens verwerkt/laat verwerken en kan worden vastgesteld welke overeenkomsten in dat kader met wie van toepassing zijn. Vervolgens dienen de potentiële overeenkomsten materieel en formeel juist te worden opgesteld en regelmatig te worden bezien op actualiteit.

4.2.4 *Implementeer bewaartermijnen voor de papieren registratieformulieren*

Tot juli 2020 had CIBG, *bewaartermijnen* niet geïmplementeerd en werden persoonsgegevens langer bewaard dan de vigerende bewaartermijn van drie jaar. Vanaf juli 2020 heeft CIBG de bewaartermijn verlengd van drie naar tien jaar vanwege de behoefte van de opdrachtgever aan beleidsmatig onderzoek. Voor de digitale registratie is de bewaartermijn per juli 2020 wel geïmplementeerd maar voor papieren registratie nog niet: deze wordt eind 2021/begin 2022 verwacht.
De ADR adviseert om het verwijderproces voor de papieren registraties zo snel mogelijk te implementeren.

4.2.5 *Maak PIA-review onderdeel van het changeproces*

Het uitvoeren van een Privacy Impact Assessment (PIA) is volgens CIBG niet verplicht aan de hand van de criteria, maar CIBG heeft toch in totaal twee PIA's uitgevoerd in 2019 en in 2020. Het donorregister bestaat sinds 1998 en de eerste PIA is in 2019 uitgevoerd, daarmee heeft CIBG in 2019 inzicht gekregen op het risicoprofiel van de verwerking van persoonsgegevens voor het donorregister.
De ADR adviseert CIBG om de PIA een vast onderdeel van het changemanagement-proces te laten zijn. Dit past bij het ontwikkelstadium van het nieuwe Donorregister per juli 2020.

4.2.6 *Houdt thema datalekken blijvend onder de aandacht*

CIBG zet in op de preventie van *datalekken* richting medewerkers en behandelt het risico op datalekken in de PIA's. De verwerkersovereenkomsten met de belastingdiensten (2018) geven inzicht in hierover gemaakte afspraken. KPN verwijst naar verouderde wet- en regelgeving (in het kader van de Wbp). CIBG kent drie datalekken voor het donorregister in de periode van april 2018 tot juli 2020.
De ADR adviseert om, naast hetgeen is geadviseerd over de verwerkersovereen-komsten, het onderwerp blijvend onder de aandacht te brengen en te houden bij medewerkers, verwerkers en samenwerkende partijen ter voorkoming van datalekken en om bewustwording te vergroten.

4.2.7 *Zie toe op naleving van afspraken van verwerking persoonsgegevens bij leveranciers gedurende en bij beëindiging van de overeenkomst*

CIBG verantwoordt zich intern per kwartaal over Privacy.
De verantwoording door verwerkers aan CIBG over de met hen gemaakte afspraken is nog niet ten uitvoer gekomen. CIBG heeft aangegeven hieraan te gaan werken.
CIBG heeft niet duidelijk gemaakt hoe is omgegaan met de persoonsgegevens van CIBG bij het beëindigen van de overeenkomst met CAPgemini eind 2018.
De ADR adviseert CIBG om - naast het maken van goede afspraken in het kader van de verwerking van persoonsgegevens - dat het CIBG zich periodiek laat informeren door leveranciers over de goede uitvoering van de overeengekomen werkzaamhe-den cf. gemaakte afspraken. CIBG kan hierin een eigen actieve rol vervullen bij de naleving van de afspraken gedurende en bij beëindiging van die samenwerking.
Daarnaast adviseert de ADR het CIBG dringend om nader onderzoek te doen naar de omgang met de persoonsgegevens van CIBG bij het beëindigen van de overeenkomst met CAPgemini eind 2018. Indien - onverhoopt - persoonsgegevens niet goed zijn terugbezorgd/vernietigd, dan kan er potentieel sprake zijn van een inbreuk op de vertrouwelijkheid van de persoonsgegevens c.q. een datalek.

5 Verantwoording onderzoek

5.1 Werkzaamheden en afbakening

Context van (de uitvoering van) het onderzoek
Na consultatie heeft de ADR op donderdag 12 maart 2020 het intakegesprek gevoerd met CIBG met betrekking tot (de aanleiding van) dit onderzoek. Vanaf maandag 16 maart 2020 mocht er vanwege COVID-19 niet meer op kantoor worden gewerkt. Dat is tot op heden (november 2020) de situatie. Dit houdt in dat het gehele onderzoek bij de onderzoekers thuis is verricht en de overleggen daarover tussen de onderzoekers en de afstemming met het CIBG via de applicatie Webex zijn verricht. Ondanks de beperkingen die dit met zich meebrengt, zijn de onderlinge contacten en die met het CIBG goed en constructief verlopen.

Tijdens de intake voor het ADR-onderzoek werkte CIBG aan een intern onderzoek, naar de toedracht van de vermissing van de externe gegevensdragers, dat zijn weerslag heeft gekregen in het 'Feitenrelaas vermissing externe gegevensdragers Donorregister', dat op 16 maart 2020 definitief is vastgesteld. CIBG heeft oktober 2020 laten weten dat de externe gegevensdragers nog steeds zijn vermist en er geen signalen zijn waaruit blijkt dat zij in 'verkeerde handen zijn gevallen'.

Proces van de uitvoering van het onderzoek
Op 9 april 2020 is de onderzoeksopdracht (met daarin elementen uit het feitenrelaas van CIBG verwerkt) door de opdrachtgever: de pSG van VWS, ondertekend.
Op 25 en 26 mei 2020 heeft de ADR met functionarissen van CIBG voor, respectievelijk het AVG-deel als het Informatiebeveiligingsdeel (BIR/BIO) gesproken over de vragen van de ADR ten aanzien van de documentatie. Deze vragen zijn deels in de gesprekken beantwoord en deels na de gesprekken schriftelijk beantwoord.

De ADR heeft twee concept-onderzoeksrapporten met het CIBG gedeeld, die door CIBG zijn voorzien van reacties en waar van toepassing voorzien van aanvullende documentatie, toelichting dan wel uitleg.
Het eerste concept-onderzoeksrapport heeft de ADR op 16 juni 2020 aan CIBG gestuurd. Op 3 juli 2020 heeft CIBG haar reactie gestuurd met aanvullende documentatie.
Op 11 september 2020 heeft de ADR het tweede concept-onderzoeksrapport aan CIBG gestuurd. Op 13 oktober heeft CIBG haar reactie gestuurd met een begeleidend memo met bespreekpunten voor het gesprek dat op 16 oktober 2020 hierover heeft plaatsgehad.

Gedurende het onderzoeksproces vond op 1 juli 2020 de implementatie van de nieuwe donorwet en daarmee de implementatie van het nieuwe donorregister DORA plaats. Op grond daarvan heeft CIBG tijdens het onderzoek documenten aangeleverd die (zowel of alleen) betrekking hadden op de situatie van vóór als de situatie na 1 juli 2020.
De primaire onderzoeksperiode liep van 12 maart tot en met 12 juni 2020. Voor zover de ADR de documenten die betrekking hadden op de situatie na juli 2020 in het onderzoek heeft betrokken, is hieraan duiding gegeven bij de beschrijving van de bevindingen.

CIBG heeft gedurende de onderzoeksperiode reeds een aantal bevindingen van de ADR opgepakt en verbeteringen doorgevoerd.

Relatie met de onderzoeksopdracht

Het doel van dit onderzoek was om conform de onderzoeksopdracht, om de door CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevens-dragers te onderzoeken. Dit om het CIBG via handelingsperspectief in staat te stellen om mogelijke verbeteringen door te voeren en daarmee het risico van herhaling van het datalek (gezien de invoering van het nieuwe Donorregister per juli 2020) te mitigeren.

De ADR heeft de gehanteerde werkwijzen en procedures overeenkomstig de beschrijving in de onderzoeksopdracht geïnventariseerd. De focus is gelegd op de vertrouwelijkheid van de data (en daarbinnen de persoons-gegevens) die op externe gegevensdragers is opgeslagen en de maatregelen die moeten voorkomen (beschermen) dat zwakheden in de omgang met externe gegevensdragers worden benut.
De ADR heeft onderzocht of de informatie uit de procedures en werkwijzen, passende maatregelen kennen (opzet) en of deze worden nageleefd (bestaan).

De volgende vragen zijn beantwoord in het onderzoek:
1.) Zijn de door het CIBG gehanteerde werkwijze, procedures voor de omgang met externe gegevensdragers in overeenstemming met richtlijnen vanuit de toenmalige BIR en zijn deze nageleefd in de periode vanaf de totstandkoming van de externe gegevensdragers tot nu?
2.) Welke eis wordt gesteld aan de gegevens ten aanzien van vertrouwelijkheid in het nieuwe Donorregister?
3.) Van welke bedrijfsmiddelen wordt voor de gegevens van het nieuwe Donorregister gebruik gemaakt (denk aan bijv. papieren antwoordformulieren, back up schijven, databases etc.)?
4.) Op welke wijze wordt invulling gegeven aan maatregelen t.a.v. de bedrijfsmiddelen om aan de eisen te voldoen in opzet?

Referentiekader voor het onderzoek vormde – conform de onderzoeksopdracht - de Baseline Informatiebeveiliging Rijksdienst (BIR) zoals die gold in de aanloop naar de casus van de twee externe harde schijven. Voor aanbevelingen is gebruik gemaakt van de Baseline Informatiebeveiliging Overheid (BIO), die per 2020 van kracht is. (voornamelijk de hoofdstukken: Beheer van bedrijfsmiddelen (H.8), Toegangsbeveiliging (H 9) en Cryptografie (H10)).

Aanvullend op hetgeen in de onderzoeksopdracht is geformuleerd, heeft de ADR – teneinde inzicht te krijgen in de waarborgen voor de vertrouwelijkheid van de persoonsgegevens - het onderzoek mede vormgegeven vanuit thema's van de Algemene Verordening Gegevensbescherming (AVG) die per 25 mei 2018 van kracht is. Daar waar van toepassing heeft de ADR gerefereerd aan de Wet bescherming persoonsgegevens (Wbp) die van kracht was vóór de inwerkingtreding van de AVG.
De ADR heeft de volgende thema's onderzocht:
Grondslag voor verwerking van persoonsgegevens, (Bijzondere) Persoonsgegevens, Verwerking van persoonsgegevens, Register van verwerkingen (met de bewaarter-mijnen), Verwerkersovereenkomsten (Bewerkersovereenkomsten: Wbp), Privacy Impact Assessments (PIA's), Processen datalekken en de Verantwoordingsplicht.
In hoofdstuk 4 leest u de adviezen die vanuit dit AVG-onderzoek zijn geformuleerd en in bijlage 1 van dit onderzoeksrapport leest u de onderzoeksresultaten.

5.2 Gehanteerde Standaard

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

Met dit onderzoek wordt geen zekerheid in de vorm van een oordeel of conclusie verschaft omdat het een onderzoeksopdracht betreft.

5.3 Verspreiding rapport

De opdrachtgever, mevrouw A.I. Norville pSG van VWS, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de 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 de website.

6 Ondertekening

Den Haag, 11 december 2020

Auditmanager
Auditdienst Rijk

Bijlage 1: Management reactie 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

26 januari 2021

Managementreactie

Het CIBG heeft begin maart 2020 de ADR verzocht om onderzoek te doen naar hoe de vermissing van twee externe harde schijven met daarop de back-up van 6,9 miljoen donorformulieren heeft kunnen gebeuren, met het oog op voorkoming hiervan in de toekomst.

Het onderzoek van de ADR vond plaats in een periode waarin het CIBG bezig was met de bouw van een nieuw donorregistersysteem voor de invoering van de nieuwe donorwet. Dit nieuwe Donorregister inclusief een nieuw IT-systeem ("DORA") verving het oude Donorregister op 1 juli 2020. Vanwege het tijdelijk naast elkaar bestaan van twee registers, één in uitvoering en één in opzet, heeft de ADR onderzoek gedaan naar beide registers. Inmiddels is het oude Donorregister op 1 juli 2020 geheel vervangen door het nieuwe Donorregister.

De ADR heeft geconstateerd dat het CIBG het informatiebeveiligingsplan voor het oude Donorregister niet meer had geactualiseerd sinds 2011 en dat maatregelen, procedures en werkwijzen voor de omgang met externe gegevensdragers onvoldoende waren uitgewerkt. Specifiek heeft de ADR geconstateerd dat procedures en werkinstructies voor het bewaren en vernietigen van externe gegevensdragers niet of onvoldoende aanwezig waren. Er bestond geen sleutelprotocol, logboek of vernietigingsprotocol voor externe gegevensdragers. Hierdoor heeft het kunnen gebeuren dat de twee harde schijven zijn verdwenen, zonder dat kan worden nagegaan wat er precies is gebeurd met die schijven. Wij vinden dit een ernstige constatering. De burger moet kunnen vertrouwen op een zorgvuldige en goed beveiligde omgang met persoonsgegevens in het Donorregister. De sturing op de naleving van de regels is onvoldoende geweest. Dit had niet mogen gebeuren. Tot op heden is er geen enkele melding bij ons bekend dat gegevens in verkeerde handen zijn gevallen en/of dat er misbruik van is gemaakt.

Zowel de vermissing zelf, als de inzichten uit het onderzoek van de ADR, hebben ervoor gezorgd dat we al tijdens het onderzoek zijn gestart met het verbeteren van de informatiebeveiliging van het nieuwe Donorregister, dat per 1 juli 2020 in werking trad. Het informatiebeveiligingsplan is geactualiseerd, er is een risicoanalyse uitgevoerd, overeenkomsten met leveranciers zijn aangepast en er zijn actiehouders benoemd om uitvoering te geven aan alle maatregelen die vanuit de BIO en de AVG worden verwacht. Inmiddels zijn de meeste maatregelen geïmplementeerd; we zijn voor het Donorregister volledig in control. Vanaf nu richten we onze aandacht op de verdere uitvoering van de maatregelen en het integreren van de maatregelen in de plan-do-check-act (pdca) cyclus. Als op termijn de nieuwe donorwet wordt geëvalueerd, zijn we voornemens om de informatiebeveiliging van het Donorregister daarbij mee te nemen. Daarnaast worden de getroffen maatregelen getoetst in de reguliere pdca-cyclus.

We hebben informatiebeveiliging ook bekeken vanuit een breder perspectief. Daarbij merken we op dat het CIBG moet voldoen aan veel en complexe regelgeving op gebied van informatiebeveiliging. Goede implementatie van alle regels vraagt om een lange adem en een gestructureerde aanpak. Het CIBG geeft informatiebeveiliging daarom meer prioriteit, capaciteit en aandacht in de vorm van een meerjarenprogramma. Hiermee willen we informatiebeveiliging voor de gehele organisatie naar een hoger ambitieniveau tillen.

Het programma zal minimaal twee jaar duren en bestaat uit de volgende drie hoofdthema's:

1. *Creëren van bewustzijn van het belang van informatiebeveiliging*: Dit is een voorwaarde om al onze inspanningen op dit gebied te laten slagen. We willen dit bewustzijn in alle lagen van de organisatie verbeteren door o.a. cursussen en actieve kennisdeling.

2. *Verduidelijken taken, rollen en verantwoordelijkheden*: de processen, procedures en het eigenaarschap op gebied van informatiebeveiliging moeten zowel op papier als in de praktijk verder invulling krijgen, zodat op individueel niveau duidelijk is wat er verwacht wordt.

3. *Inregelen van checks en balances:* we gaan meer sturen op naleving (toezicht en controles) en zorgen ervoor dat dit is ingebed in de jaarlijkse planning & control cyclus. Hiermee zorgen we dat plannen en procedures actueel blijven.

Het CIBG zal zich tegenover VWS verantwoorden over de programmadoelstellingen en –resultaten.

Tot slot wil het CIBG haar waardering uitspreken over het werk en de inzet van de ADR in dit onderzoek. Er is met veel zorgvuldigheid gehandeld en dit heeft geleid tot een zeer gedetailleerde rapportage. Het CIBG vindt de inzichten die dit onderzoek heeft opgeleverd zeer waardevol voor de verdere vormgeving van informatiebeveiliging. Momenteel vindt nog overleg plaats met de ADR over het uitvoeren van een vervolgonderzoek om invulling te geven aan de motie van Pia Dijkstra.[1]

Namens de directie van het CIBG,

N.A. Laagland
Directeur CIBG

[1] Motie om de ADR te verzoeken de gehele informatiebeveiliging van het Donorregister bij het CIBG te onderzoeken;
https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z13346&did=2020D28311

Bijlage 2 Onderzoeksresultaten Algemene Verordening Gegevensbescherming (AVG)

vervullen bij de naleving van de afspraken gedurende en bij beëindiging van die samenwerking.—72

1 Onderzoeksresultaten Algemene Verordening Gegevensbescherming (AVG)

In het kader van de vertrouwelijkheid van het Donorregister is tijdens het onderzoek de wijze waarop de AVG wordt toegepast in beschouwing genomen. Hierbij is inzicht geboden in de situatie van voor en na juli 2020. Het handelingsperspectief dat uit de bevindingen volgt, leest u in hoofdstuk 4.

1.1 In werking treden AVG en Persoonsgegevens

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt sindsdien niet meer.

De AVG heeft onder meer gezorgd voor:

- Versterking en uitbreiding van de privacy-rechten;
- Meer verantwoordelijkheden voor organisaties;
- Dezelfde, stevige bevoegdheden voor alle Europese privacy-toezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

Onder de AVG heeft een organisatie meer verplichtingen bij het verwerken van persoonsgegevens, omdat de organisatie de verantwoordelijkheid heeft om aan te tonen dat de organisatie zich aan de wet houdt: de verantwoordingsplicht. Deze plicht houdt in dat de organisatie met documenten moet kunnen aantonen dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen. Organisaties kunnen ook verplicht zijn om een Data Protection Impact Assessment uit te voeren (DPIA).

1.2 De grondslag voor verwerking van persoonsgegevens aangetroffen.

De Autoriteit Persoonsgegevens (AP) raadt aan om de grondslag van de verwerking te vermelden in de Privacyverklaring, in het Privacybeleid en eventueel in het Verwerkingsregister. De grondslag hebben wij in de volgende documenten aangetroffen:

- Privacy verklaring:
  Het CIBG heeft in de **Privacyverklaring** op haar website aangegeven dat het CIBG, persoonsgegevens verwerkt voor een wettelijke reden en voor een doel: *'Het CIBG verwerkt persoonsgegevens wanneer er een wettelijke reden is om ze te mogen verwerken of op basis van toestemming. Daarbij zorgen we ervoor dat persoonsgegevens alleen verwerkt worden voor het specifieke doel waarvoor ze verzameld zijn'.* Tevens staat op de website dat in het Donorregister wordt geregistreerd welke organen iemand wil afstaan na zijn overlijden, of de persoonsgegevens van de persoon die dit na het overlijden mag bepalen voor de overledene.[2]
- Privacybeleid (VWS):
  In de Privacy Governance (2018), (met daarin **Privacybeleid**) gericht op het VWS-kerndepartement en haar concernonderdelen staat de grondslag van verwerking opgenomen. Voor het voldoen aan de privacywetgeving

[2] https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport/privacy

geldt onverminderd dat elk VWS-onderdeel haar eigen bestuurlijke verantwoordelijkheid heeft.

- Verwerkingsregister:
  In M 729 (Verwerking van Persoonsgegevens: extract **Verwerkingsregister**) en het na 1 juli 2020 geldende document M 8740 staat dat de grondslag volgt uit de WOD en de rechtsgrond een wettelijke verplichting is.
- PIA's (hierover leest u in 1.7 meer):
  Ook de PIA's van oktober 2019 en mei 2020, verwijzen naar de rechtsgrond voor het registreren van persoonsgegevens in het Donorregister. *'Dit volgt uit artikel 10 van de Wet op de Orgaandonatie (WOD). In deze wet is in hoofdstuk 3 de wetgeving ten aanzien van het ter beschikking stellen van organen na overlijden opgenomen. Daarin is geregeld wat er geregistreerd kan worden met een van de 4 keuzes (artikel 9 lid 2). Wie zich kan registreren artikel 9 lid 1. In artikel 10 lid 1 en 3 staat wie er een donorformulier krijgt toegezonden. In het Besluit donorregister staan de regels die betrekking hebben op het donorformulier en het donorregister. Daaruit volgt ook welke gegevens mogen worden verwerkt, de - op het formulier uit te vragen persoonsgegevens - staan namelijk in de bijlage bij het Besluit donorregister'.*

1.3 Aanpassingen noodzakelijk door andere persoonsgegevens in het nieuwe Donorregister

De persoonsgegevens die voor en na invoering van het nieuwe Donorregister per juli 2020 verwerkt worden, verschillen. Dit vraagt om aandacht en eenduidigheid in het verwerkingsregister en de verwerkingsovereenkomsten.

1.3.1 *Persoonsgegevens huidige Donorregister*

De persoonsgegevens die in het huidige Donorformulier (voor juli 2020) worden gevraagd en verwerkt zijn: Voorletter(s), Tussenvoegsel, Achternaam, Geboorte-datum, Geslacht, Burger Service Nummer (BSN), Straat, Huisnummer, Postcode en Plaats van de persoon die het formulier zelf invult.

Daarnaast worden de persoonsgegevens gevraagd en verwerkt van *de persoon die is aangewezen* als de persoon die beslist - na het overlijden van de persoon die het betreft - of diens organen en weefsels beschikbaar zijn voor transplantatie. Het gaat om: Voorletter(s), Tussenvoegsel, Achternaam, Straat, Huisnummer, Postcode en Plaats, Land en twee telefoonnummers.

1.3.2 *Persoonsgegevens nieuwe Donorregister*

De persoonsgegevens die in het nieuwe Donorformulier (na juli 2020) worden gevraagd zijn met uitzondering van 'Geslacht' (dit wordt niet meer gevraagd) bij de betrokkene, identiek aan de persoonsgegevens in het vóór juli 2020 gebruikte Donorformulier.

Wat is verder anders in het nieuwe Donorformulier vanaf juli 2020?

- In het nieuwe Donorformulier wordt gevraagd of de persoon alle (genoemde) organen en weefsels wil doneren of alleen die organen en weefsels die de persoon daaronder heeft aangekruist terwijl bij het oude Donorformulier werd gevraagd of de persoon al dan niet organen en weefsels ter beschikking wil stellen en daarbij moest aankruisen welke organen/weefsel de persoon NIET beschikbaar wil stellen.
- Er wordt gevraagd naar toestemming om het orgaan of weefsel - in geval tijdens de donatie blijkt dat artsen een orgaan of weefsel toch niet kunnen gebruiken - te mogen gebruiken voor transplantatieonderzoek.
- Er is een extra weefsel als keuze toegevoegd: 'zenuwweefsel'.

1.3.3 *CIBG heeft invulling gegeven aan de omgang met persoonsgegevens in relatie tot wilsonbekwamen en geconcludeerd dat er geen sprake is van bijzondere persoonsgegevens.*

- In het Staatsblad van het Koninkrijk der Nederlanden Jaargang van (28 maart) 2018, staat onder meer het volgende:

Artikel I

'De Wet op de orgaandonatie wordt als volgt gewijzigd: In artikel 9 wordt aan het slot van het eerste lid een volzin toegevoegd, luidende: De wettelijk vertegenwoordiger van een meerderjarige die niet in staat is tot een redelijke waardering van zijn belangen ter zake van orgaandonatie kan namens hem toestemming verlenen tot het na zijn overlijden verwijderen van zijn organen of bepaalde door de wettelijke vertegenwoordiger aan te wijzen organen, dan wel daartegen bezwaar maken'.

In de PIA Oud (voor juli 2020) wordt geconcludeerd dat er geen sprake is van verwerking van bijzondere persoonsgegevens.

In de PIA Nieuw (vanaf juli 2020) staat dat de voorziening in de nieuwe donorwet om voor iemand anders een registratie te kunnen doen, met name is gericht op wilsonbekwame personen. De grondslag daarvoor is in de Wet op de orgaandonatie geregeld, voor zover deze zal luiden na inwerkingtreding van de nieuwe donorwet en voor zover het om gewone persoonsgegevens gaat. Vervolgens wordt aangegeven dat: *Voor de aantekening dat iemand een registratie voor een ander heeft gedaan, zal worden voorzien in een aanvullende wettelijke grondslag in het Besluit donorregister.* Tevens wordt aangegeven dat een registratie die door iemand voor een ander is gedaan, een gezondheidsgegeven kan zijn indien die ander wilsonbekwaam is. (In 1.7 leest u meer over PIA's).

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling weergegeven op de PIA Donorregister na juli 2020.

Hoewel de wetgeving hier ruimte voor biedt, in de vorm van vertegenwoordiging bij wilsonbekwamen, worden er in de praktijk geen bijzondere persoonsgegevens verwerkt door het Donorregister.

1.3.4 *Verwerkingsregister en vigerende verwerkersovereenkomsten verschillen, per juli 2020 worden aanpassingen door CIBG doorgevoerd.*

In M729 (Verwerking van Persoonsgegevens: extract verwerkingsregister) tot juli 2020, staat dat er geen bijzondere persoonsgegevens worden verwerkt. In relatie tot de vigerende verwerkersovereenkomst met de Belastingdienst Heerlen staat dat ook 'Medische gegevens' worden verwerkt en in de vigerende verwerkersovereenkomst met KPN staan BSN en geboortedatum niet opgenomen als te verwerken gegevens.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling weergegeven op de PIA Donorregister na juli 2020.

In M8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister) vanaf 1 juli 2020, staat eveneens dat geen bijzondere persoonsgegevens worden verwerkt. Ingaande juli 2020 heeft CIBG nieuwe (concept-)verwerkersafspraken opgeleverd. In het nieuwe concept verwerkersafspraken met Belastingdienst Heerlen staan 'Medische gegevens' niet meer vermeld. Een nieuw concept verwerkersovereenkomst met KPN is door de ADR nog niet ontvangen.

In 1.5 leest u meer over verwerkersovereenkomsten.

1.3.5 *Handelingsperspectief: blijf goede afwegingen maken bij de informatie die wordt verwerkt (bijzondere) persoonsgegevens en leg de onderbou-wingen vast.*

De aanvulling op de PIA Donorregister vanaf juli 2020, met betrekking tot de vermeende verwerking van bijzondere persoonsgegevens (wilsonbekwamen) is daarvan een goed voorbeeld. Tevens is het goed om de uniformiteit van de informatie/gegevens in verwerkersovereenkomsten-/cq –afspraken, register van verwerkingen etc. te bewaken.

1.4 Aandacht gewenst voor aantal medewerkers dat kan verwerken

Door middel van het Donorregistratieformulier digitaal of op papier kan de burger zijn keuze aangeven voor de registratie in het Donorregister. De persoonsgegevens worden centraal opgeslagen in een door het CIBG opgezet digitaal registratie-systeem. In de PIA voor het Donorregister vanaf juli 2020 staat dat Persoons-gegevens worden verwerkt ten behoeve van:

- Het versturen van brieven aan Nederlands ingezetenen van 18 jaar en ouder, met het verzoek zich te registreren.
- Het versturen van een herinneringsbrief in het geval op de eerste brief niet binnen zes weken gereageerd is.
- Het registreren van de persoon in het Donorregister.
- Het versturen van een registratiebevestiging aan de geregistreerde.
- Het raadplegen door NTS bij (een verwacht) overlijden van de persoon.
- Het genereren van registratiegegevens voor beleidsdoeleinden (zoals b.v. hoeveel mensen zich actief hebben geregistreerd, met welke keuze en welke verdeling over leeftijdsgroepen en/of gemeentecode gebied in Nederland). Deze gegevens zijn niet herleidbaar tot individuele personen.
- Voor correspondentie n.a.v. foutief ingevuld donorformulieren.

1.4.1 *Volgens de brochure 'Nieuwe Donorregister' tot juli 2020 is het aantal personen dat de keuze kan raadplegen beperkt, dit in tegenstelling tot de praktijk. Na juli 2020 is dit aantal teruggebracht.*

Volgens de brochure tot juli 2020, kunnen alleen artsen en verpleegkundigen in het ziekenhuis de keuze van betrokkenen zien en staat in de wet dat niemand anders in het Donorregister mag kijken: de wettelijke richtlijnen over privacy worden altijd gevolgd. In de brochure 'Nieuwe Donorregister' (oktober 2019) staat: *'Alleen artsen en verpleegkundigen in het ziekenhuis kunnen uw keuze zien'*. In dezelfde brochure staat bij de vraag of anderen de keuze van betrokkene kunnen zien, aangegeven: *'Uw keuze in het Donorregister is veilig. Alleen artsen en verpleegkundigen in het ziekenhuis kunnen uw keuze zien. Ze mogen dat alleen zien vlak voor uw overlijden of daarna. In de wet staat dat niemand anders in het Donorregister mag kijken. De wettelijke richtlijnen over privacy worden altijd gevolgd'.*

In de praktijk blijken in totaal 122 medewerkers (rollen) van het CIBG en NTS, toegang tot de persoonsgegevens te hebben. Medewerkers (rollen) van overige 'verwerkers' zijn nog niet meegeteld, zo staat in de PIA Oud en Nieuw (mei 2020). (Binnen 1.7 leest u meer over PIA's).

CIBG geeft als reactie gedurende het onderzoek dat er een Communicatieplan is en de brochure algemene informatie bevat. Er zijn beschermende maatregelen getroffen volgens CIBG.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling weergegeven op de PIA Donorregister na juli 2020.

In 'Privacy' op de website heeft CIBG is de tekst aangescherpt en aangepast. https://www.donorregister.nl/privacy

Volgens CIBG is vanaf het registreren van de persoon in het Donorregister, de keuze van de burger zichtbaar voor de medewerkers van het Donorregister. Verder staat in het memo van CIBG dat het aantal medewerkers dat toegang heeft tot de gegevens van 122 naar maximaal 40 CIBG-medewerkers is teruggebracht.

In de DPIA in hoofdstuk 8 staat het volgende: '*In totaal hebben 122 medewerkers (rollen) van het CIBG en NTS, namelijk Functioneel Beheerders, Medewerkers Klant Contactcenter, Registratiemedewerkers (Scan en NTS), toegang tot de persoons-gegevens. Deze personen hebben een geheimhoudingsverklaring ondertekend. De papieren dossiers worden opgeslagen in een afgesloten kast bij het CIBG.'* Deze

tekst is niet meer van toepassing op het nieuwe systeem en is per abuis in de DPIA opgenomen, licht CIBG toe, echter, gehandhaafd blijft dat alle medewerkers een geheimhoudingsverklaring ondertekenen.

1.4.2 *Volgens het verwerkingsregister (voor en na juli 2020) hebben meerdere partijen rechtstreeks toegang persoonsgegevens, de situatie na juli 2020 heeft CIBG genuanceerd*

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister) tot juli 2020 staat dat dat NTS, Eurotransplant en CBS 'Ontvangers' zijn van de informatie, en rechtstreekse toegang tot de persoonsgegevens is verstrekt aan onderstaande betrokkenen. De PIA's geven hier inhoudelijk verdere informatie over:

- *Personeel dat onder leiding van de verantwoordelijke staat*

De Minister van VWS is opdrachtgever en daarmee verwerkingsverantwoordelijke. CIBG is opdrachtnemer voor het beheren van het donorregister en treedt op als verwerkingsverantwoordelijke namens de minister. Het Ministerie ontvangt op verzoek *geanonimiseerde informatie,* zoals de verdeling over de keuzes, leeftijdsgroepen, het postcodegebied, het aantal actief geregistreerde mensen en hoeveel er met 'geen bezwaar' staan geregistreerd (vanaf juli 2020).

- *Personeel dat onder leiding van de verwerker staat*

VWS/CIBG heeft drie verwerkers onderkend in het kader van het Donorregister: Belastingdienst Heerlen en Apeldoorn en KPN. De registraties worden bij KPN opgeslagen.

- *Derden, namelijk: de Nederlandse Transplantatie Stichting (NTS)*

In de WOD wijst het Ministerie van VWS de NTS, formeel aan als orgaancentrum wiens medewerkers het donorregister raadplegen, weefseldonoren aannemen, deze screenen en weefsels toewijzen. Raadplegen van het register gebeurt door of in opdracht van een arts die contact opneemt met het orgaancentrum (NTS) (artikel 10 lid 3 Wod).

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

In M8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister - vanaf 1 juli 2020) staat net als in M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister - voor juli 2020) aangegeven dat rechtstreekse toegang tot de persoonsgegevens bestaat voor:

- Personeel dat onder leiding van de verantwoordelijke staat
- Personeel dat onder leiding van de verwerker staat
- Derden, namelijk: Nederlandse Transplantatie Stichting

CIBG heeft toegelicht dat:

- Voor het nieuwe systeem DORA geldt dat maximaal 40 medewerkers van het CIBG, toegang krijgen tot de gegevens. Hierbij heeft niet iedereen dezelfde rollen en bevoegdheden.
- De Belastingdienst heeft als verwerker geen rechtstreekse toegang tot het nieuwe systeem DORA. Medewerkers van BD Heerlen hebben indirect toegang tot de persoonsgegevens op de ingevulde formulieren bij het verwerken van de ontvangen post. Medewerkers van BD Apeldoorn hebben indirect toegang tot de persoonsgegevens bij het verzenden van de brieven en de registratiebevestigingen.
- KPN heeft geen directe toegang tot de persoonsgegevens in het Donorregister.

De NTS raadpleegt niet meer middels een autorisatie in het systeem. Raadpleging verloopt nu via een koppeling met een webservice waarbij de persoonsgegevens en de meest recente wilsbeschikking automatisch en zonder menselijk handelen worden opgehaald.

Eurotransplant is de organisatie die namens de NTS de wachtlijsten voor orgaantransplantatie beheert en regelt namens de NTS de objectieve toewijzing van

organen aan de meest geschikte patiënt. Eurotransplant is onderdeel van NTS en ontvangt daardoor indirect van CIBG,persoonsgegevens via de NTS, echter deze persoonsgegevens vallen onder de verantwoordelijkheid van de NTS. Eurotransplant heeft geen directe toegang tot de gegevens in het Donorregister.

Geheimhouding is onderdeel van de afspraken met NTS en de verwerkersafspraken met de Belastingdienst.

1.4.3 *Het is tot juli 2020 onduidelijk welke autorisatie NTS en Eurotransplant in Donorregister hebben, na juli is dit toegelicht.*

Uit de ontvangen documenten is tot juli 2020 niet duidelijk tot welk deel van het Donorregister, NTS (en Eurotransplant) toegang en/of inzage hebben. In onder meer de Project Start Architecture (PSA (oktober 2018) staat dat – met de NTS als tussenpartij – artsen (of iemand in hun opdracht) 24/7 wilsbeschikkingen uit het Donorregister kunnen raadplegen. Volgens CIBG is NTS/Eurotransplant (zelf) verwerkingsverantwoordelijke en zijn CIBG en NTS nog in gesprek over de grenzen binnen het Donorregister.

CIBG heeft aangegeven dat autorisatie vanuit NTS en Eurotransplant wordt gelogd en er afspraken zijn tussen NTS en Eurotransplant. Onduidelijk is in welke mate rechtstreekse toegang tot de persoonsgegevens (rollen/autorisaties) is verstrekt aan (het personeel van) NTS en Eurotransplant en welke maatregelen daarbij zijn getroffen. Uit de PIA's blijkt dat de applicatie niet van buitenaf benaderbaar is zonder juiste inlogcode en het juiste wachtwoord en dat alleen CIBG-medewerkers zijn geautoriseerd om het Donorregister te raadplegen. Na inloggen is de applicatie toegankelijk voor de medewerker. Hetzelfde geldt voor de thuiswerkomgeving.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

Hieruit blijkt dat de NTS, toegang krijgt tot de persoonsgegevens en de meest recente wilsbeschikking. Raadpleging verloopt via een koppeling door een web-service waarbij de persoonsgegevens en de meest recente wilsbeschikking automatisch en zonder menselijk handelen worden opgehaald. De NTS is afnemer van twee services van het CIBG waarmee het Donorregister benaderd kan worden, te weten: DORA-Vita webservice en het uitwijkportaal. Het Donorregister is 7 dagen x 24 uur beschikbaar, primair via de webservice. Wanneer de webservice niet te benaderen is, is het uitwijkportaal de work-a-round.

De NTS heeft in de nieuwe situatie geen directe autorisaties meer in het donorregister en vanaf het moment van raadpleging start de verwerkingsverantwoordelijkheid van de NTS.

Eurotransplant beheert namens de NTS de wachtlijsten voor orgaantransplantatie en regelt namens de NTS de objectieve toewijzing van organen aan de meest geschikte patiënt. Eurotransplant ontvangt persoonsgegevens via de NTS. Deze vallen onder de verantwoordelijkheid van de NTS. Eurotransplant heeft geen directe toegang tot de gegevens in het Donorregister en heeft geen autorisaties gekregen via CIBG.

1.4.4 *Handelingsperspectief: in het belang van de burger dient het aantal medewerkers dat diens gegevens verwerkt in het kader van de AVG tot een minimum beperkt te worden.*

CIBG heeft hiervoor per juli 2020 nadere maatregelen ingezet. Het is goed om deze blijvend te monitoren, afwegingen in dit kader te blijven maken en hierover transparant te communiceren.

1.5 Verwerkersovereenkomsten-/afspraken zijn niet op orde

In de PIA voor het nieuwe Donorregister staat dat CIBG optreedt als verwerkingsverantwoordelijke namens de minister. Rijksoverheidsorganisaties die bedrijven persoonsgegevens laten verwerken moeten volgens de AVG een Verwerkersovereenkomst opstellen. Indien er sprake is van opdrachten voor de verwerking van persoonsgegevens door andere onderdelen van de rechtspersoon Staat der Nederlanden, moet gebruik worden gemaakt van het model Verwerkersafspraken. In het kader van de Wbp was er nog sprake van een Bewerkersovereenkomst.

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister – voor juli 2020) staan drie verwerkers: KPN, Belastingdienst Heerlen en Belastingdienst Apeldoorn. Hetzelfde geldt voor M 8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister - per juli 2020).

1.5.1 *Verwerkersovereenkomst met KPN is al enige tijd verouderd*

KPN is vanaf 12 november 2018 tot heden verwerker voor het CIBG (m.b.t. Donorregister). Er dient dus een verwerkersovereenkomst aanwezig te zijn.

Tussen VWS/CIBG en KPN BV bestaat een verwerkersovereenkomst, die is gebaseerd op een oud model uit 2016, die verwijst naar verouderde wetten en richtsnoeren en waarvan de datum ondertekening niet duidelijk is.

Voor de vigerende verwerkersovereenkomst met KPN hebben wij de volgende observaties:

- De datum van de ondertekening daarvan blijkt niet uit het document.
- De verwerkersovereenkomst is inhoudelijk gedateerd/verouderd:
    - de te verwerken persoonsgegevens wijken af van die uit het verwerkingsregister: de BSN en de geboortedatum staan niet vermeld in de overeenkomst.
    - Er is gebruik gemaakt van Model ARBIT 2016 i.p.v. 2018 en er wordt nog gesproken over de Wbp, Cbp richtsnoeren en verwezen naar BIR 2012.

CIBG geeft hiervoor de volgende toelichting: *'De overeenkomsten zijn bij de aanbesteding in oktober 2017 in concept opgesteld. Hierbij is ook een bewerkersovereenkomst opgesteld en nagekeken door Juridische Zaken van het CIBG. De overgang van CAP naar KPN is uiteindelijk afgerond in november 2018, na de inwerkingtreding van de AVG. De overeenkomsten zijn voor ondertekening niet meer gecontroleerd, ook niet door de HIS. Hierdoor is gebruik gemaakt van een verouderd format'.*

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

Voor het nieuwe Donorregister wordt wederom gewerkt met KPN, de nieuwe verwerkersovereenkomst hebben wij niet gezien. CIBG geeft aan dat er wordt gewerkt aan een nieuwe verwerkersovereenkomst met KPN.

1.5.2 *(Concept-)verwerkersafspraken met de Belastingdienst zijn voor verbetering vatbaar en bewerkersovereenkomsten zijn niet aangetroffen*

Omdat CIBG reeds lang samenwerkt met de Belastingdienst Heerlen en Apeldoorn zouden in het kader van de Wbp (tot 25 mei 2018) bewerkersovereenkomsten aanwezig moeten zijn. Deze zijn niet aangetroffen. Een aantal jaren terug werkte CIBG samen met Belastingdienst Kerkrade, hiervan is geen bewerkersovereenkomst/verwerkersovereenkomst-/afspraak aangetroffen.

Tussen VWS/CIBG en Belastingdienst Heerlen (Centrum voor Facilitaire Dienstverlening) bestaat een verwerkersafspraak (december 2018) en er bestaat een verwerkersafspraak tussen VWS/ CIBG en Belastingdienst Apeldoorn (Data Centre Services) (oktober 2018).

De vigerende verwerkersovereenkomst met Belastingdienst Heerlen bevat foutief een (bijzonder) persoonsgegeven: er staat bij de 'te verwerken gegevens' dat ook 'Medische gegevens' worden verwerkt, wat volgens de Privacy Officer van CIBG niet correct is.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

Voor het nieuwe Donorregister wordt wederom gewerkt met de belastingdienst.
Er bestaan nieuwe verwerkersafspraken - in concept/afrondend stadium - met de Belastingdienst Heerlen en Apeldoorn. Hierin staat 'Geslacht' aangegeven bij 'persoonsgegevens', dit gegeven is echter per juli 2020 niet meer van toepassing.
In de PIA Donorregister Nieuw staat: *'in sommige gevallen vult een burger zijn/haar BSN niet in. De backoffice van het CIBG probeert de burger te identificeren aan de hand van de andere persoonsgegevens. Wanneer dit niet lukt, wordt de route 'niet-correct ingevuld registratieformulier' gevolgd. In de verwerkersafspraken die het CIBG maakt met de BD Heerlen worden afspraken gemaakt over de beoordeling die de BD Heerlen zal doen'.*
Deze afspraken ziet de ADR niet concreet in de concept-verwerkersafspraken terug. CIBG heeft aangegeven dat concrete afspraken over de verwerking door de Belastingdienst Heerlen zijn opgenomen in het implementatieplan, gesloten tussen CIBG en de Belastingdienst Heerlen.

1.5.3 *Verwerkersovereenkomst tussen CIBG en firma Reisswolf (voor vernietiging van persoonsgegevens) is niet aanwezig: CIBG onderzoekt noodzaak daartoe en doet navraag bij de Belastingdienst over hun verwerkersovereenkomst met PostNL*

Op dit moment - en ook voor het nieuwe Donorregister - maakt CIBG via de Belastingdienst Heerlen - gebruik van de firma Reisswolf voor het vernietigen van de persoonsgegevens. Hiervoor is geen bewerkersovereenkomst/verwerkersovereenkomst, maar wordt gebruik gemaakt van het Rijksbrede contract met Reisswolf.

Uit ontvangen documentatie blijkt dat na opdracht - van de opdrachtgever - de fysieke documenten worden vernietigd door de firma Reisswolf, het gaat om 'gecertificeerde vernietiging'. Het verslag van vernietiging wordt opgeleverd aan de opdrachtgever volgens CIBG. Dit verslag is niet aan de ADR ter beschikking gesteld.

De firma Reisswolf is niet als Verwerker opgenomen in M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister – tot juli 2020) en wordt in geen van beide PIA's die de ADR heeft ontvangen genoemd.
CIBG heeft aangegeven dat de Belastingdienst Heerlen gebruik maakt van het Rijksbrede contract met Reisswolf, die is gecertificeerd en gecontracteerd voor de vernietiging van vertrouwelijke materialen. Volgens de Privacy Officer van CIBG had er wel een verwerkersovereenkomst moeten zijn of is sprake van een subverwerker via Belastingdienst Heerlen.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

De firma Reisswolf is evenmin als Verwerker opgenomen in M 8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister – na juli 2020).

De ADR had CIBG vragen gesteld over de inhoud van het Rijksbrede contract van Reisswolf en over de juridische constructie tussen de Belastingdienst Heerlen en Reisswolf als tussen CIBG en de Belastingdienst Heerlen een Verwerkers*afspraak* geldt (die binnen de Rijksoverheid wordt gehanteerd) en Reiswolff een private partij is.
CIBG heeft aangegeven juridisch onderzoek te laten doen naar de vraag of het nodig is om overeenkomsten af te sluiten met onderaannemers van hun leveranciers. Reisswolf is een organisatie waar rijksbreed gebruik van wordt gemaakt. Vergelijkbare partijen zijn FMH als toegangsbeheerder van de Hoftoren en Xerox als uitvoerder van de postkamers. Hier zijn vanuit het CIBG ook geen individuele verwerkersovereenkomsten mee afgesloten, omdat ervanuit is gegaan dat het CIBG onder de rijksbrede overeenkomsten valt.
Aangezien veel onderdelen van VWS c.q. het Rijk hier op vergelijkbare manier mee omgaan, zal dit punt worden voorgelegd aan de FG van VWS en de Privacy Adviseur Rijk voor advies. Indien nodig sluit het CIBG de noodzakelijke verwerkersovereenkomsten met voorgenoemde partijen, waaronder Reisswolf.

De ADR had CIBG vragen gesteld met betrekking tot het feit dat in de PIA Oud staat dat met PostNL geen verwerkersovereenkomst is gesloten en dat dat ook niet nodig is terwijl in de PIA Nieuw staat dat de Belastingdienst Heerlen een verwerkersovereenkomst heeft met PostNL, voor het versturen van brieven. Ook is de ADR niet duidelijk hoe de relatie zich verhoudt tussen CIBG (verwerkersverantwoordelijke) en PostNL ((sub-)verwerker?) refererend aan art. 7 van de verwerkersovereenkomst-/afspraak.
CIBG heeft aangegeven dat PostNL als logistieke dienstverlener geen verwerker van het CIBG is. Ze zijn zelf verwerkingsverantwoordelijke voor het verwerken van de persoonsgegevens die noodzakelijk zijn voor de dienstverlening: dit is conform standpunt AP. Onduidelijk is waarom de Belastingdienst wel een verwerkersovereenkomst heeft gesloten met PostNL. Vermoedelijk omdat ze gebruik maken van een zakelijke dienstverlening van PostNL waarbij ze meer doen dan sec verzending van poststukken. Dit wordt door CIBG nagevraagd bij de Belastingdienst.

1.5.4 *In het verleden was Capgemini (India) (sub-) verwerker voor CIBG, waarvoor eind 2014/ begin 2015 een overeenkomst is gesloten die niet is voorzien van de datum ondertekening en waarbij onzekerheid is over de bewerkersovereenkomst die voordien zou hebben gegolden vanmei 2011-eind 2014: deze is niet aangetroffen*
CAP was van 1 mei 2011 tot 13 december 2018 verwerker voor CIBG. Er dient dus een bewerkersovereenkomst en wellicht een verwerkersovereenkomst te zijn.
In het document NLmodel DTA NL (december 2014) of DTA CIBG 2015: overeenkomst inzake doorgifte van gegevens staat het volgende opgenomen:

> *'Om de diensten vallend onder de Overeenkomst te kunnen leveren aan de gegevensexporteur (*ADR: dit gaat om CIBG*),* ***heeft Capgemini Nederland bepaalde delen van deze diensten uitbesteed aan de groepsmaatschappij Capgemini India Pvt. Ltd. (de "gegevensimporteur").*** *Met betrekking tot deze uitbestede diensten zijn Capgemini Nederland en de gegevensimporteur een afzonderlijke opdracht ('Statement of Work') aangegaan onder de bestaande onderlinge hoofdovereenkomst ('Master Inter-Company Agreement'). Bij het uitvoeren van de uitbestede diensten* ***zal de gegevensimporteur als subverwerker mogelijk persoonsgegevens (dienen te) verwerken die afkomstig zijn uit de IT-systemen van de gegevensexporteur'.***

Hierbij zijn dus drie rollen: (1) de gegevensexporteur (CIBG), (2) de gegevensimporteur/verwerker (Capgemini NL) en (3) de gegevensimporteur/subverwerker (Capgemini India).

- Het document is niet voorzien van de datum waarop de overeenkomst feitelijk is gesloten (datum ondertekening).
- De ADR heeft – gezien het feit dat Capgemini reeds vanaf mei 2011 bewerker/verwerker is – geen bewerkersovereenkomst aangetroffen voor de periode 2011 tot aan 2014/2015.

1.5.5 *NTS is 'ontvanger' voor het CIBG en is zelf verwerkingsverantwoordelijke; zij hebben onderlinge afspraken in het kader van de AVG expliciet vastgelegd juni 2020*

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister – voor juli 2020) staan NTS, Eurotransplant en CBS gedefinieerd als categorieën van ontvangers.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

In M 8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister – na juli 2020) staan alleen NTS en CBS genoemd als ontvangers.

In het document Samenwerkingsafspraken (m.b.t. het Donorregister) tussen CIBG en de NTS (29 juni 2020), staat dat de NTS en het CIBG ieder verwerkingsverantwoordelijke zijn voor hun eigen deel in het proces van orgaandonatie. Partijen verklaren over en weer dat ze persoonsgegevens op behoorlijke, zorgvuldige en transparante wijze verwerken, in overeenstemming met de toepasselijke wet- en regelgeving. De NTS heeft in de nieuwe situatie geen directe autorisaties meer in het donorregister. Vanaf het moment van raadpleging start de verwerkingsverantwoordelijkheid van de NTS. Het CIBG is alleen verwerkingsverantwoordelijke voor de gegevens in het donorregister. Wanneer de NTS de wilsbeschikking raadpleegt t.b.v. orgaandonatie stopt de verantwoordelijkheid van het CIBG.

CIBG is verantwoordelijk voor de hosting van de (web-)applicatie DORA. De hosting is middels een Service Level Agreement (SLA) en een Dossier Afspraken en Procedures (DAP) uitbesteed aan KPN.

1.5.6 *Om de volledigheid van de verwerkers te borgen wil CIBG halfjaarlijks controle gaan uitoefenen*

CIBG heeft aangegeven dat er voor het vaststellen van de volledigheid van verwerkers in 2018 overleggen zijn gevoerd met de afdelingen. Het idee is om halfjaarlijks te gaan controleren of er nieuwe verwerkers zijn.

1.5.7 *Handelingsperspectief: CIBG is zelf voornemens om de volledigheid van de verwerkers te gaan borgen door halfjaarlijkse controles.*

De ADR zou CIBG willen aanreiken een omgevingsverkenning uit te voeren m.b.t. de (keten-)partners met wie CIBG voor het Donorregister samenwerkt en met wie deze (keten-)partners zelf samenwerkingsverbanden onderhouden in relatie tot het Donorregister. Van daaruit kan de analyse plaatsvinden wie persoonsgegevens verwerkt/laat verwerken en kan worden vastgesteld welke overeenkomsten in dat kader met wie van toepassing zijn. Vervolgens dienen de potentiële overeenkomsten materieel en formeel juist te worden opgesteld en regelmatig te worden bezien op actualiteit.

1.6 Verbeteringen voor het verwerkingsregister van CIBG zijn mogelijk.

1.6.1 *Verwerkingsregister van CIBG is niet openbaar*

In de Privacy Governance (incl. het Privacybeleid) van VWS (2018) staat, dat VWS het AVG-register gebruikt dat het ministerie van Economische Zaken en Klimaat heeft laten ontwikkelen. De AVG schrijft voor dat iedereen die persoonsgegevens verwerkt, hiervan registratie bijhoudt als onderdeel van de verantwoordingsplicht. In artikel 30 AVG staat precies welke gegevens er, naast de grondslag van de verwerking, in het register moeten staan. De registratie van verwerkingen gebeurt door de contactpersonen bij de VWS-directies en concernonderdelen; voor hen is het register verplicht. Hoedster van het Verwerkingsregister is de Privacy Officer VWS in casu: de Privacy Officer CIBG.

CIBG heeft ervoor gekozen om het Verwerkingsregister niet openbaar te maken, daarom zijn de gegevens niet terug te vinden op https://avgregisterrijksoverheid.nl

1.6.2 *In het verwerkingsregister – tot juli 2020 – zijn niet alle elementen juist vermeld; voor de situatie na juli 2020 zijn wijzigingen doorgevoerd*

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister – tot juli 2020) staat dat er geen sprake is van doorgifte van persoonsgegevens aan één of meer landen buiten de Europese Unie of aan een internationale organisatie.
Bij 'Beveiliging' wordt verwezen naar beveiligingsbeleid: dit bevat echter volgens de ADR geen maatregelen. Verzending gaat mogelijk wel over andere 'Netwerken', en niet via een eigen netwerk, er is geen sprake van 'Pseudonimisering' en 'Encryptie'. De ADR leest vanuit de documenten dat er wel in encryptie is voorzien.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

In M8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister –na juli 2020) is eveneens aangegeven dat er geen sprake is van doorgifte van persoons-gegevens aan één of meer landen buiten de Europese Unie of aan een internationale organisatie. Bij 'maatregelen' wordt aangegeven dat er vastgesteld beveiligings-beleid is dat ook is geïmplementeerd. Gegevensverzending gebeurt naast het eigen netwerk ook via een publiek netwerk. Bij 'pseudonimisering' staat aangegeven dat het BSN is verwerkt in de scancode onderaan de brief, waardoor de brief te koppe-len is aan een individueel persoon, maar het BSN niet herleidbaar is op het formu-lier. Encryptie wordt toegepast: de persoonsgegevens worden versleuteld tijdens verzending. In relatie hiermee is nog toegelicht door CIBG dat encryptie op alle omgevingen (acceptatie en productie) aan staat.

1.6.3 *Bewaartermijn: CIBG heeft per juli 2020 de bewaartermijn verlengd van drie naar tien jaar vanwege de behoefte van de opdrachtgever aan beleidsmatig onderzoek.*

In de PIA Oud staat – als toelichting - aangegeven dat:

> De privacyregelgeving geeft **als beginsel** dat persoonsgegevens **niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is.** *Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd.* Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn. *Bij overheidsverwerkingen moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden.* Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodiek toetsen aan het beginsel van opslagbeperking. Hierbij

moet rekening worden gehouden met andere regelgeving over bewaartermijnen zoals de Archiefwet 1995.

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister – tot juli 2020) staat bij 'Bewaartermijn': 'tot drie jaar na overlijden van betrokkene'. Grondslag voor bewaartermijn is de archiefwet, maar hoe de termijn bij het begin van het Donorregister is vastgesteld op drie jaar is bij CIBG onduidelijk.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

In M 8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister) – na juli 2020 - staat voor nederlands ingezetenen vanaf 12 jaar bij 'Bewaartermijn' aangegeven: 'tot tien jaar na overlijden van betrokkene'. Voor de 'aangewezen persoon' geldt een bewaartermijn van drie jaar na overlijden van de geregistreerde persoon.
CIBG heeft aangegeven dat de genoemde bewaartermijn voor de 'aangewezen persoon' niet correct is opgenomen in het verwerkingsregister en dat CIBG deze zal aanpassen naar eveneens tien jaar: de contactgegevens van de aangewezen persoon zijn namelijk onderdeel van de registratie van de betrokkene.

De bewaartermijn is per juli 2020 door het CIBG aangepast van drie naar tien jaar. CIBG geeft als toelichting: de grondslag van de bewaartermijn is de archiefwet. Van deze bewaartermijn mag worden afgeweken als hier een goede reden voor is. Voor de nieuwe situatie na 1 juli 2020 heeft CIBG gekozen om hiervan af te wijken, vanwege de behoefte van de opdrachtgever aan beleidsmatig onderzoek.
De eigenaar van het archief is uiteindelijk de zorgdrager c.q., de Minister. De verantwoordelijke/beheerder voor het archief is het afdelingshoofd Donorregister.

1.6.4 *Voor juli 2020 was het verwijderproces van de papieren formulieren niet ingericht en werden deze langer dan noodzakelijk en zonder grondslag bewaard.*
Doordat het verwijderproces niet was ingericht is het digitaliseringsproject gestart. Vanaf juli 2020 wordt het verwijderproces van de papieren formulieren in kaart gebracht en na aansluiting op EDRMS (eind 2021/begin 2022), wordt geen fysiek archief meer opgebouwd

De PIA Oud zegt dat 'de papieren dossiers worden opgeslagen bij het CIBG in een afgesloten kast (in de kelder in Heerlen), die wordt afgesloten aan het eind van de dag. Zodra de formulieren gescand zijn worden ze gearchiveerd'. Er bestaan volgens CIBG, werkinstructies. De PIA Nieuw (mei 2020) voegt nog toe dat, als de substitutie-proef van de gescande formulieren akkoord is, de formulieren na verwerking kunnen worden vernietigd. Zij zullen wel tijdelijk (aantal weken) in het archief van de scanlocatie bewaard moeten blijven. Ook staat hierin dat er nog afspraken worden gemaakt over het digitaal archiveren en vervolgens vernietigen van het papieren archief.

Bij de papieren formulieren is niet vanaf het begin de bewaartermijn bijgehouden en na verloop van tijd waren er te veel formulieren om deze alsnog handmatig te doorlopen. CIBG verwerkt dus - na de 3 jaar - de gegevens langer dan noodzakelijk en zonder grondslag; dat is de reden waarom het digitaliseringsproject is gestart.

Voor deze kwestie en de situatie na juli 2020 heeft CIBG aanvullende documentatie/ informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

In 'aanvulling DPIA Donorregister na juli 2020 per 30 juni 2020' staat dat er geen papieren dossiers meer opgeslagen worden op de afdeling zelf. Het Donorregister

gaat vanaf 1 juli 2020 digitaal werken, waardoor de kasten niet meer zullen worden gebruikt.

Het CIBG heeft in dit kader toegelicht dat het verwijderproces van de fysieke formulieren nog in kaart wordt gebracht. Zodra CIBG het Donorregister kan aansluiten op het EDRMS (dit is momenteel (oktober 2020) voorzien voor eind 2021/begin 2022), wordt er geen fysiek archief meer opgebouwd en hoeft CIBG die documenten ook niet meer 10 jaar te bewaren: die termijn wordt voor digitale registratie wel gehanteerd.

Overigens bewaart de Belastingdienst Heerlen productiebestanden tot drie maanden na oplevering aan de opdrachtgever op de Server en op USB-storage, waarvoor een tijdelijke (fysieke) opslag (met aparte nummering) in een apart gedeelte van het archief is gereserveerd. Belastingdienst Heerlen hanteert deze termijn van drie maanden met alle andere klanten die de belastingdienst heeft.

1.6.5 *Voor juli 2020 was het verwijderproces van de digitale registratie niet ingericht.*

Gegevens werden weliswaar uit het donorregister verwijderd, waren niet meer raadpleegbaar, maar bleven na drie jaar nog bewaard. Vanaf juli 2020 is het verwijderproces ingericht

Voor juli 2020 was het verwijderproces niet ingericht en werden gegevens na overlijden, emigreren of bij uitoefening van het recht op gegevenswissing uit het donorregister verwijderd, waren dan niet meer raadpleegbaar, maar bleven na drie jaar nog bewaard.

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister – tot juli 2020) staat dat het verwijderen niet is geïmplementeerd. Dit wordt meegenomen in het lopende project Actief Donor Registratie (ADR). Het (oude) systeem ODISYS is destijds niet zo geprogrammeerd dat bij overlijden of uitschrijven de bewaartermijnen volgens de archiefwet automatisch worden toegepast.

In de PIA Oud staat dat de gegevens in het donorregister worden bewaard zolang de registratie actief is plus een bewaartermijn van 3 jaren, op grond van de Archiefwet. *De gegevens worden na 3 jaar echter niet verwijderd. Ook van personen die emigreren, overlijden of hun recht op gegevenswissing ten uitvoer brengen, worden de gegevens wel uit het register verwijderd maar blijven de gegevens bewaard.* Het verwijderproces is niet/nooit ingericht. Na een verwijdering uit het register is de registratie niet meer raadpleegbaar.

In de PIA Nieuw (mei 2020) staat dat gegevens in het donorregister worden bewaard zolang de geregistreerde nog in leven is. Een geregistreerde wordt uit het donorregister verwijderd als deze naar het buitenland verhuist of in het geval van overlijden, zodra de wijziging is door-gevoerd in het BRP[3]. Het CIBG krijgt vanuit het BRP dagelijks mutaties waarvoor zij is geautoriseerd doorgestuurd. De registratie is niet meer raadpleegbaar zodra de wijziging is doorgevoerd in het BRP en het CIBG de mutatie heeft verwerkt.

Vanaf juli 2020 is het verwijderproces ingericht en worden gegevens na overlijden en emigreren volgens selectielijsten uit het register verwijderd, blijven tien jaar bewaard en worden op persoonsniveau vervolgens automatische verwijderd middels een technische service die bewaartermijnen controleert en voor vernietiging zorgt.

[3] Voor de informatie voor de aanschrijving van de doelgroepen (18-jarigen en nieuw ingezetenen) gebruikt CIBG, informatie uit de Basisregistratie personen (BRP). Hiertoe bestaat een Autorisatiebesluit (Autorisatiebesluit Selectieverstrekking Agentschap CIBG, Rijksdienst voor Identiteitsgegevens van 4 december 2017).

CIBG heeft de ADR gedurende het onderzoek toegelicht dat in het nieuwe systeem automatische verwijdering plaatsvindt op persoonsniveau, hiervoor is een technische service die controleert of de bewaartermijnen zijn verstreken en deze service regelt de vernietiging. Ieder bestand heeft een unieke ID.
CIBG heeft de ADR aan het einde van het onderzoek toegelicht dat in het nieuwe Donorregister de gegevens na overlijden en emigreren volgens de selectielijsten uit het register worden verwijderd. De registratie blijft 10 jaar bewaard voor beleidsmatig onderzoek. Deze termijnen zijn vastgelegd in de selectielijst van het CIBG en zijn vastgesteld op grond van de archiefwet.

1.6.6 *De minderjarige (12 tot 18-jarigen) die zich vrijwillig heeft geregistreerd in het Donorregister kan zichzelf ook verwijderen vanaf juli 2020, de gegevens blijven ook dan 10 jaar bewaard op grond van de archiefwet.*

In de PIA Nieuw (mei 2020) staat dat een minderjarige van twaalf jaar of ouder die zich (vrijwillig) heeft geregistreerd in het donorregister de registratie wel kan verwijderen; deze registratie van een minderjarige is namelijk vrijwillig. Het CIBG heeft toegelicht - voor de situatie na juli 2020 - dat de functionaliteit voor 12 tot 18-jarigen om zichzelf te verwijderen is ingebouwd in het nieuwe Donorregister. Zowel via DigiD als op papier kunnen burgers in deze leeftijdscategorie zichzelf verwijderen uit het Donorregister.

In het M 8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister – juli 2020) nederlands ingezetenen staat vanaf betrokkenen vanaf 12 jaar bij 'Bewaartermijn' aangegeven: 'tot tien jaar na overlijden van betrokkene'.

Op verzoek van de ADR heeft het CIBG bevestigd dat minderjarigen zich vrijwillig kunnen registreren in het Donorregister. Zij kunnen zich ook weer laten verwijderen uit het register en zijn daarin dan niet meer raadpleegbaar. Wel blijven hun gegevens 10 jaar bewaard op grond van de archiefwet.

1.6.7 *Handelingsperspectief: het verwijderproces voor de papieren registratieformulieren dient zo snel mogelijk te worden geïmplementeerd en is nu voorzien eind 2021/begin 2022.*

1.7 PIA is voor Donorregister niet verplicht volgens CIBG aan de hand van de criteria maar wordt wel uitgevoerd, voor het eerst in 2019

1.7.1 *Bepaling noodzaak/wenselijkheid PIA is in 2017 niet uitgevoerd*

De Quick-Scan (QS) Informatiebeveiliging Donorregister (december 2017) heeft onder andere als doel om op een snelle en eenduidige wijze inzicht te krijgen of voor het proces de AVG in voldoende mate is geïmplementeerd en of er een Gegevensbescherming Effecten Beoordeling/(D)PIA wenselijk of noodzakelijk is, zo staat in de inleiding van het document. De QS is voor de AVG uiteindelijk niet uitgevoerd en daarmee de bepaling voor de noodzaak/wenselijkheid van een (D)PIA[4] in 2017.

1.7.2 *CIBG concludeert op basis van de criteria dat een PIA niet verplicht is maar kiest ervoor deze uit te voeren*

In M 729 (Verwerking van Persoonsgegevens: extract verwerkingsregister - tot juli 2020) staat dat:
-Geen sprake is van een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan

[4] In het nederlands wordt DPIA vertaald als: gegevensbeschermingseffectbeoordeling (GEB). Maar PIA, DPIA en GEB worden door elkaar gebruikt, al is de PIA de bekendste afkorting.

voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
-Geen sprake is van grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.
-Geen sprake is van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.
-De soort verwerking houdt, in het bijzonder als het gaat om een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan om andere redenen waarschijnlijk geen hoog risico in voor de rechten, vrijheden van natuurlijke personen.

CIBG concludeert dat een PIA *niet verplicht* is maar kiest ervoor deze *wel* uit te voeren gezien de grootschalige verwerking van persoonsgegevens.

In M8740 (Verwerking van Persoonsgegevens: extract verwerkingsregister) na juli 2020 staat deze zelfde afweging verwoord.

1.7.3 *CIBG heeft in 2019 en in 2020 - voor het eerst - een PIA uitgevoerd voor het Donorregister en zag eerder geen aanleiding om een PIA uit te voeren*

Het Donorregister is sinds 1998 opgericht om uitvoering te geven aan de Wet op de orgaandonatie (WOD). In het regeerakkoord (PvdA/VVD-2012) is vastgelegd dat de uitvoering van een PIA een vanzelfsprekende maatregel is bij de bouw van systemen en het aanleggen van databestanden. De Quick-Scan Informatiebeveiliging Donorregister (2017) heeft zoals vermeld geen inzicht gegeven op de vraag of er een PIA/GEB wenselijk/noodzakelijk is of niet. CIBG heeft de ADR toegelicht dat CIBG geen aanleiding heeft gezien om vóór 2019 een PIA uit te voeren.

CIBG heeft in totaal twee PIA's Donorregister uitgevoerd (in 2019 en 2020). Bij de start van het project voor de nieuwe donorwet is besloten om toch een PIA uit te voeren op het proces. Dit betekende een PIA voor nieuw en oud.

- De PIA Oud is oktober 2019 vastgesteld en ondertekend door een manager van CIBG (afd. R&K). Er blijkt niet uit de PIA Oud of de adviezen van de FG en de CIO zijn gevraagd, gegeven of verwerkt. Bij de betrokken velden uit het format staat bij beide functionarissen 'n.v.t.' ingevuld.

Voor de situatie na juli 2020 heeft CIBG aanvullende documentatie/informatie ter beschikking gesteld aan de ADR en heeft op dit punt toegelicht dat na overleg met de FG destijds is afgesproken om de PIA Oud alleen intern af te stemmen en vast te stellen.

- De PIA Nieuw dateert van 12 mei 2020:

1. heeft nog geen datum vaststelling, maar gaat vastgesteld worden door de directeur van de directie Geneesmiddelen en Medische Technologie.
2. advies van de FG VWS (februari 2020) en het overzicht van de opvolging daarvan is bijgevoegd bij de PIA Nieuw.
3. De naam van de CIO staat wel in het format maar onduidelijk is of diens advies/oordeel daadwerkelijk is gevraagd, gegeven of verwerkt.
4. de inleiding van deze PIA was nog niet aangepast aan de actualiteit:

In deze inleiding staat:
'Vanaf 1 juli 2020 ontvangt iedereen die 18 jaar of ouder is en nog niet in het register staat een brief met het verzoek zich te registreren met een van de volgende keuzes: 1. ja, ik geef toestemming 2. Nee, ik geef geen toestemming 3. Mijn partner of familie beslist 4. Een door mij gekozen persoon beslist. Is er na zes weken nog geen reactie ontvangen, dan wordt er een herinnering verstuurd. Registreert iemand zich niet dan wordt hij zes weken na het verzenden van de

herinneringsbrief met 'geen bezwaar tegen orgaan- of weefseldonatie' geregistreerd in het Donorregister.

Op 7 mei 2020 heeft Minister Van Rijn aangekondigd dat, wie op 1 juli 2020 nog geen keuze heeft gemaakt, pas vanaf september een brief krijgt die waarschuwt dat hij of zij te boek komt te staan als iemand zonder bezwaar tegen orgaandonatie (dit i.v.m. Covid-19). ADR: het is raadzaam om de tekst (en zo nodig het betrokken proces daarvan) aan te passen aan de actualiteit.

5. duiding van een aanvullende wettelijke grondslag ontbrak en
6. de specifieke bescherming aan kinderen zoals de AVG beoogt was niet in de PIA's geduid.

Voor deze kwesties en de situatie na juli 2020 heeft CIBG aanvullende documentatie /informatie ter beschikking gesteld aan de ADR. In een memo van 30 juni 2020 heeft CIBG een aanvulling gegeven op de PIA Donorregister na juli 2020.

1. De PIA Nieuw is inmiddels vastgesteld door de directeur Directie Geneesmiddelen en Medische Technologie.
2. Behoeft geen aanvulling.
3. Navraag leerde dat het voorleggen aan de CIO niet nodig was bij CIBG.
4. Aanpassing van de inleiding wordt behandeld in het memo van CIBG 30 juni.
5. Duiding van de aanvullende wettelijke grondslag wordt behandeld in het memo van 30 juni en is verder behandeld in 1.3.3. van dit document.
6. De specifieke bescherming aan kinderen zoals de AVG beoogt is niet in de PIA's geduid, maar is in art. 9.1 van de WOD reeds geregeld.

In artikel 9.1 van de WOD staat: Meerderjarigen en minderjarigen van twaalf jaar of ouder, die in staat zijn tot een redelijke waardering van hun belangen ter zake, kunnen toestemming verlenen tot het na hun overlijden verwijderen van hun organen of bepaalde door hen aan te wijzen organen, dan wel daartegen bezwaar maken.

1.8 Handelingsperspectief: het Donorregister bestaat sinds 1998 en is met een PIA - voor het eerst in 2019 - onderzocht op het risicoprofiel van de verwerking van persoonsgegevens. Het lijkt raadzaam om de PIA een vast onderdeel van het changemanagementproces te laten zijn: dit past bij het ontwikkelstadium van het nieuwe Donorregister per juli 2020.CIBG zet in op preventie van datalekken

Voor het Donorregister zijn drie datalekken bij het CIBG bekend vanuit de periode april 2018 tot juli 2020. Geen van deze datalekken was afkomstig van bewerkers/ verwerkers.
De directie van CIBG werkt aan een cultuur waarin openheid, reflectie en lerend vermogen centraal staan en treft ter preventie van datalekken maatregelen voor medewerkers. Het datalek met de externe gegevensdragers bij het Donorregister heeft ertoe geleid dat CIBG hoge urgentie voelt om inspanningen op het gebied van informatiebeveiliging te versnellen, zo staat in een memo van 8 mei 2020.

1.8.1 *CIBG treft maatregelen ter voorkoming van datalekken door medewerkers*

CIBG zet preventief in op maatregelen ter voorkoming van datalekken, door het vergroten van veiligheidsbewustzijn en het bijbehorend gedrag van medewerkers. Nieuwe medewerkers wordt verzocht in de eerste werkweek om de "*de gedragscode integriteit Rijk*" (2017/2018) en "*de gedragsregeling digitale werkomgeving*" (juni 2016) te lezen. Ook staat er informatie op de intranetsite van CIBG. Zij zijn verplicht om binnen 14 dagen de AVG-module (van de CIBG-academie) te volgen, af te ronden en ondertekenen een verklaring omtrent integriteit en digitaal werken. Met een test over integriteit en vertrouwelijke informatie rondt CIBG de introductie af.

In de gedragscode Integriteit Rijk (2017/2018) wordt betrouwbaarheid vertaald in zorgvuldigheid in relatie tot mensen en middelen en de zichtbaarheid van de ambtenaar behandeld, in relatie tot diens handelen, vaardigheden en eigen verantwoordelijkheid. De gedragsregeling voor de digitale werkomgeving (juni 2016) behandelt onder meer het vervoer van informatie op betrouwbare gegevensdragers, zorgvuldig gebruik van voorzieningen, handelen bij verlies of diefstal van vertrouwelijke informatie en attent zijn op en melden van incidenten en kwetsbaarheden.

1.8.2 *In de PIA's van oktober 2019 en mei 2020 wordt in het kader van risicoanalyse de waarschijnlijkheid van een (en ook het actuele) Datalek meegewogen*

In de PIA's wordt in het kader van de risicoanalyse, de waarschijnlijkheid van het optreden en de impact van een Datalek meegewogen. In de PIA Nieuw wordt een aantal scenario's onderkend m.b.t. Datalekken: zoals het lekken van informatie door het CIBG of door de NTS, door b.v. onzorgvuldig gebruik of hackers. Lekken van informatie tijdens het vervoer naar de archieflocatie of op de archieflocatie b.v. door onzorgvuldig gebruik, tijdens verzending van brieven van en/of naar betrokkene. Op basis van de ervaringen met het Donorregister en het Orgaancentrum (raadplegen) acht CIBG de kans dat bovenstaande zich zal voordoen, nihil. Beveiliging krijgt meer aandacht, daardoor wordt het niveau ervan verhoogd voor het Donorregister.

Voor de situatie na juli 2020 heeft CIBG aanvullende documentatie/informatie ter beschikking gesteld aan de ADR. CIBG heeft op dit punt toegelicht dat n.a.v. het recente datalek bij CIBG de tekst in de PIA is aangepast voordat deze definitief is vastgesteld door de directie GMT. In de nieuwe PIA staat het volgende:
De kans dat bovenstaande zich zal voordoen is klein, maar niet ondenkbaar. Recente ontwikkelingen, het verliezen van twee harde schijven door het Donor--register, hebben dit helaas aangetoond. Naar aanleiding van het incident worden de processen nogmaals bekeken op eventuele risico's. Ook wordt er een externe audit uitgevoerd door de ADR. Eventuele aanbevelingen die hieruit komen, worden doorgevoerd. Daarbij is er extra aandacht voor de beveiliging van het Nieuwe Donorregister en gaat de beveiliging naar een hoger niveau dan nu het geval is.

1.8.3 *De (bewerkers-)overeenkomst met Capgemini (2011 – eind 2018) beschrijft hoe de beveiliging in het kader van de verwerking van persoonsgegevens is geregeld met technische en organisatorische maatregelen*

Capgemini was van 1 mei 2011 tot 13 december 2018 verwerker voor CIBG. In de overeenkomst, document NLmodel DTA NL (december 2014) of DTA CIBG 2015 staat de definitie van technische en organisatorische beveiligingsmaatregelen (1F), en dat de gegevensimporteur (CAP India), de gegevens-exporteur (CIBG) onverwijld ervan in kennis stelt wanneer iemand per ongeluk of op ongeoorloofde wijze toegang tot de gegevens heeft gehad (bepaling 5 Dii), er wordt gewerkt in de zin van de Wbp (begeleidende nota) en in aanhangsel 2 staat nog een extra beschrijving van technische en organisatorische maatregelen die door Capgemini India zijn getroffen (vallen buiten de SLA of contract).
In de beveiligingsovereenkomst met Capgemini (2015) staan volgens CIBG onder 3.10 algemene afspraken over het afhandelen van beveiligingsincidenten (datalekken zijn hiervan een sub).

1.8.4 *Afspraken met Belastingdienst Heerlen, Belastingdienst Apeldoorn, Belastingdienst Kerkrade en Reisswolf over Datalekken van vóór 2018 zijn onbekend*

De verwerkersovereenkomsten met de Belastingdienst Heerlen en Apeldoorn zijn (eind) december 2018 gesloten. Daarvoor was sprake van bewerkersovereenkomsten (Wbp), deze heeft de ADR niet ingezien waardoor inzicht ontbreekt in procedures, afspraken en maatregelen voor de Meldplicht Datalekken van 2016 tussen CIBG en de Belastingdiensten Heerlen en Apeldoorn.
Eerder in dit rapport is reeds vermeld dat de ADR geen enkele overeenkomst heeft aangetroffen met de firma Reiswolff, en de Belastingdienst Kerkrade. Daarmee is geen inzicht in de procedure en afspraken en maatregelen rond de Meldplicht Datalekken tussen hen en CIBG.

1.8.5 *In verwerkersovereenkomsten met Belastingdiensten Apeldoorn, Heerlen en KPN staan afspraken over de inbreuk in verband met persoonsgegevens. KPN refereert daarbij aan verouderde wet- en regelgeving.*

In de verwerkersovereenkomsten staan geen afspraken over de feitelijke melding aan de Autoriteit Persoonsgegevens, maar op grond van de AVG is de verwerkingsverantwoordelijke daartoe verplicht. Andere afspraken zijn wel aangetroffen. In de verwerkingsovereenkomsten met de Belastingdiensten Apeldoorn, Belastingdienst Heerlen en KPN staat onder meer:

- de definitie van een inbreuk in verband met persoonsgegevens (lid 1.3) (KPN: lid 1.2),
- de afspraak over het informeren van de verwerkersverantwoordelijke zonder onredelijke vertraging (lid 5.5) (m.b.t. technisch en organisatorische maatregelen) en
- lid 9. (het informeren ook over ontwikkelingen m.b.t. inbreuk) met verwijzing naar bijlage 3, die vermeldt:

> **3.1 Departementale procedure**
> Inbreuken in verband met Persoonsgegevens dienen zo snel mogelijk door de Opdrachtnemer, en in ieder geval binnen 24 uur nadat ze geconstateerd zijn, aan de Opdrachtgever te worden gerapporteerd via CMGDatatekregister@minvws.nl. Tevens verleent Opdrachtnemer waar nodig volledige medewerking aan de adequate informatieverstrekking aan betrokkenen in het kader van de Meldplicht Datalekken. Na melding rapporteert de Opdrachtnemer wekelijks over de afhandeling van de Inbreuk in verband met Persoonsgegevens en de maatregelen om de gevolgen van het incident te beperken en herhaling te voorkomen, zodat de Opdrachtgever op de hoogte blijft van de stand van zaken.
> In onderling overleg kan besloten worden dat verdere rapportage niet meer nodig is, dit wordt dan schriftelijk vastgelegd.
>
> **3.2 Informatie die ten minste door Verwerker moet worden verstrekt**
> -Aard van de Inbreuk in verband met Persoonsgegevens
> -De Persoonsgegevens en Betrokkene
> -Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
> -Maatregelen die Verwerker heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

- Bijlage 2, met de technische en organisatorische maatregelen, hier geeft KPN een verwijzing naar – de verouderde – BIR 2012.
- Bijlage 3 Art. 3.1 hier verwijst KPN naar verouderde wet- en regelgeving: de Wbp en de Cbp zoals reeds eerder in hoofdstuk 4 vermeld. Maar Art. 3.2 kent dezelfde informatie voor KPN als in de verwerkersovereenkomsten met de Belastingdiensten.
- Art. 10 van de verwerkersovereenkomsten vermeldt afspraken over het terugbezorgen of wissen van persoonsgegevens na afloop van de dienstverlening. Verder staat er vermeld dat de opdrachtgever de Inbreuken in verband met Persoonsgegevens beoordeelt die worden gerapporteerd door de Opdrachtnemer of subbewerkers.

1.8.6 *Voor het oude Donorregister zijn drie datalekken bekend over de periode van april 2018 tot juli 2020; geen van deze datalekken was afkomstig van bewerkers/ verwerkers*

CIBG geeft aan dat er drie Datalekken bij het Donorregister (klantvraag, verkeerde brief en zoekraken externe schijven) zijn geweest. Geen van deze datalekken was afkomstig van bewerkers/verwerkers. Het datalekregister heeft de ADR niet ingezien, omdat hiervoor geen noodzaak werd onderkend door de ADR.

1.8.7 *Handelingsperspectief: naast hetgeen de ADR heeft aangereikt binnen 1.5.7 ten aanzien van de verwerkersovereenkomsten, lijkt het raadzaam om het onderwerp blijvend onder de aandacht te brengen en te houden bij medewerkers, verwerkers en samenwerkende partijen ter voorkoming van datalekken en om bewustwording te vergroten*

1.9 CIBG verantwoordt zich intern per kwartaal over Privacy

De verantwoording van verwerkers ontbreekt en is daarin dus niet opgenomen, CIBG gaat hieraan werken CIBG heeft niet duidelijk gemaakt hoe is omgegaan met de persoonsgegevens van CIBG bij het beëindigen van de overeenkomst met CAPgemini eind 2018

Binnen CIBG wordt per kwartaal over Privacy verantwoording afgelegd. De informatie over de verantwoording van de verwerkers van de persoonsgegevens van het Donorregister aan CIBG heeft daarin nog geen plaats. CIBG voert zelf jaarlijks een verantwoordingsgesprek in het kader van Privacy met VWS.

CIBG heeft in dit onderzoek niet geduid hoe bij de beëindiging van de overeenkomst met Capgemini op 13 december 2018, is omgegaan met de persoonsgegevens waarover Capgemini vanuit de rol van (sub-)verwerker beschikte. Over 2018 is geen geen auditrapport of TPM door CIBG ontvangen. Indien het CIBG – na nader onderzoek - niet duidelijk is of en hoe alle bestaande (kopieën van) (persoons-) gegevens veilig zijn terug bezorgd of vernietigd is mogelijk sprake van een datalek.

1.9.1 *Bij CIBG wordt per kwartaal intern verantwoording afgelegd over Privacy, de verantwoording van verwerkers ontbreekt*

De verantwoording van verwerkers ontbreekt omdat CIBG nog niet beschikt over de periodieke/jaarlijks verantwoording over de technische en organisatorische maatregelen van hen: CIBG gaat hier uitvoering aan geven. Hierdoor heeft CIBG minder zekerheid over de bescherming van die persoonsgegevens.

In Privacy-governance (incl. Beleid) van VWS (2018) staat dat privacy-compliance wordt opgenomen in de bestaande P&C-rapportagecyclus van VWS. Hiertoe is VWS in 2019 een project gestart. Omdat de bescherming van persoonsgegevens nauw samenhangt met de beveiliging van informatie - en daarmee het proces In Control Verklaring op informatiebeveili-ging – integreert VWS beide rapportages. Opname wordt voorbereid via het jaarlijk-se draaiboek en wordt effectief vanaf 2019, zo werd beoogd.

Bij CIBG wordt over het thema Privacy verantwoording afgelegd tijdens onder meer de kwartaalgesprekken die - tussen elk afdelingshoofd met het directieteam van CIBG - worden gehouden. Voor 2020-2021 is hiervoor volgens CIBG een Privacyplan opgesteld door de Privacy Officer CIBG. Zo heeft CIBG de ADR laten weten.

CIBG heeft jaarlijks een gesprek met de Functionaris Gegevensbescherming en de Chief Privacy Officer van VWS voor de jaarlijkse verantwoording. Dit proces is in ontwikkeling en wordt verder geprofessionaliseerd door VWS.

VWS maakt afspraken over maatregelen met partijen als softwareleveranciers en datacenters en controleert of externe partijen deze afspraken nakomen, zo stelt VWS op haar site. De afspraken hiertoe zijn vastgelegd binnen artikel 11 van de (concept-)verwerkersafspraken/overeenkomst met de Belastingdienst Heerlen, Apeldoorn en KPN.

CIBG heeft als Verwerkingsverantwoordelijke geen informatie of documentatie, waaruit blijkt dat Verwerkers zich periodiek/jaarlijks verantwoorden over de technische en organisatorische maatregelen - in het kader van de verwerking van persoonsgegevens - en de effectiviteit daarvan, dan wel dat CIBG hierop audits heeft laten uitvoeren bij verwerkers.

De ADR heeft begrepen uit de toelichting van het CIBG, dat er nog geen sprake is geweest van naleving van/sturing op de verantwoording over de gemaakte afspraken door de verwerkers. Dit houdt in dat CIBG momenteel minder zekerheid heeft over passende technische en organisatorische maatregelen, te treffen door verwerkers, ter bescherming van de persoonsgegevens van CIBG.

1.9.2 *CIBG heeft in dit onderzoek niet geduid hoe bij de beëindiging van de overeenkomst met Capgemini op 13 december 2018, is omgegaan met de persoonsgegevens waarover Capgemini vanuit de rol van (sub-)verwerker beschikte. In het laatste jaar van de overeenkomst met Capgemini is geen auditrapport of TPM door CIBG ontvangen.*

CIBG heeft de overeenkomst met Capgemini (India) 13 december 2018 beëindigd. CIBG heeft in dit onderzoek niet geduid hoe is omgegaan met de persoonsgegevens van CIBG waarover Capgemini beschikte vanuit de rol van (sub-)verwerker bij het einde van de overeenkomst.
Er is over 2018 geen auditrapport of Third Party Mededeling (TPM) van Capgemini ontvangen.

In de **Beveiligingsovereenkomst** met Capgemini (maart 2015) staat:

> Artikel 3.12. Naleving
> -Bij **beëindiging of wijziging** van de dienstverlening worden op verzoek van VWS **alle gegevens** waarvoor VWS verantwoordelijk is en/of waarvan VWS, eigenaar is **tijdig en in bruikbaar formaat overgedragen aan VWS.**

In de **overeenkomst tussen CIBG en** Capgemini (India), document DTA CIBG 2015 staat in bep.12: *Verplichting na de beëindiging van de verwerking van persoonsgegevens*

> De partijen komen overeen dat de gegevensimporteur en de subverwerker na het beëindigen van de verlening van de gegevensverwerkingsdiensten **alle doorgegeven persoonsgegevens en kopieën daarvan aan de gegevensexporteur terugbezorgen of,** indien de gegevensexporteur dat verkiest, **alle persoonsgegevens vernietigen en aan de gegevensexporteur verklaren dat de vernietiging heeft plaatsgevonden,** tenzij de op de gegevensimporteur toepasselijke wetgeving hem verbiedt alle of een gedeelte van de doorgegeven persoonsgegevens terug te bezorgen of te vernietigen. In dat geval garandeert de gegevensimporteur dat hij de vertrouwelijkheid van de doorgegeven persoonsgegevens zal respecteren en dat hij de doorgegeven gegevens niet verder actief zal verwerken.

> De gegevensimporteur en de subverwerker garanderen dat zij gegevensexporteur en/of de toezichthoudende op verzoek van de autoriteit hun verwerkingsvoorzieningen voor een controle van de in lid 1 bedoelde maatregelen beschikbaar zullen stellen.

Het is de ADR onduidelijk welke (controle-)maatregelen door CIBG zijn getroffen om zekerheid te krijgen dat alle bestaande (kopieën van) gegevens veilig zijn terugbezorgd of zijn vernietigd bij de beëindiging van de dienstverlening door CAPgemini. Indien het CIBG – na nader onderzoek - niet duidelijk is of en hoe alle bestaande (kopieën van) (persoons-) gegevens veilig zijn terug bezorgd of vernietigd is mogelijk sprake van een datalek.

In de ICV van CIBG over 2018 (januari 2019) staat dat CIBG een non-compliance constateert omdat er geen auditrapporten of TPM's zijn ontvangen van Capgemini waaruit blijkt dat de controls voor informatieveiligheid aanwezig zijn en overeenkomstig de eisen functioneren. Het is de ADR onduidelijk waarom juist in het jaar waarin de overeenkomst wordt beëindigd geen auditrapport of TPM is ontvangen/gevraagd.

1.9.3 *Handelingsperspectief: naast het maken van goede afspraken (zie: 1.5.7) in het kader van de verwerking van persoonsgegevens van CIBG, is het raadzaam dat CIBG zich periodiek laat informeren over de goede uitvoering van de overeengekomen werkzaamheden cf. gemaakte afspraken. CIBG kan hierin een eigen actieve rol vervullen bij de naleving van de afspraken gedurende en bij beëindiging van die samenwerking.*

CIBG heeft gedurende dit onderzoek niet duidelijk gemaakt hoe is omgegaan met de persoonsgegevens van CIBG bij het beëindigen van de overeenkomst met CAPgemini eind 2018. De ADR adviseert CIBG dringend om hier nader onderzoek naar te doen. Indien - onverhoopt - persoonsgegevens niet goed zijn terugbezorgd/ vernietigd, dan kan er potentieel sprake zijn van een inbreuk op de vertrouwelijkheid van de persoonsgegevens c.q. een datalek.

Bijlage 3 Tabel Principes en maatregelen ontwikkeling nieuwe donorregister

In de PSA hebben wij onderstaande maatregelen / principes aangetroffen, die gerelateerd zijn aan beveiliging. We hebben niet onderzocht of deze daadwerkelijk zijn gevolgd tijdens het project.

Onder technologie:

SQL Server 2016+	De database. Toepassen van de Always Encrypted functie voor dataencryptie.

Onder beveiliging

Nr.	**Implicatie**
S-PR-01 **Project technologie principe** BIR is van toepassing	Het systeem voldoet aan de Baseline Informatiebeveiliging Rijksdienst (BIR)
S-PR-02 **Project technologie principe** CIBG SSD Richtlijnen	De richtlijnen staan beschreven in het meegeleverde document CIBG_secure_software_development V2_5.pdf
S-PR-03 **Project technologie principe** Geen testdata met privacy gevoelige gegevens	Er mag in de ontwikkel, test en acceptatie omgeving geen gebruik worden gemaakt van data met privacy gevoelige gegevens.
S-PR-04 **Project technologie principe** Uitwisseling van privacy gevoelige en/of vertrouwelijke gegevens via systeemkoppelingen alleen aan vertrouwde partijen.	Privacygevoelige en/of vertrouwelijke gegevens kunnen alleen worden uitgewisseld met vertrouwde partijen waar een wettelijke doelbinding voor is vastgelegd en een verwerkerovereenkomst is afgesloten. Privacy by Default en Privacy by Design conform AVG wordt toegepast.
S-PR-05 **Project technologie principe** Koppelvlak (Autorisatie)	Autorisatie wordt gecontroleerd met behulp van het koppelvlak. Rollen worden gedefinieerd in Identity Manager

Onder beheer o.a. volgende principe opgenomen:

M-PR-06 Monitoring moet mogelijk zijn	Het systeem logt (instelbaar) relevante operaties/transacties conform de CIBG standaard.

Project principes

Project principes voor applicaties **Nr.**	**Project applicatie principe**	**Implicatie**
PA1 **Bovenliggend principe** NORA AP06	De dienst maakt gebruik van standaard oplossingen	Voor het ophalen van DigiD, eIDAS en BRP gegevens zal gebruik gemaakt worden van de standaard oplossingen die hiervoor aanwezig zijn op het koppelvlak. Voor het uitwisselen van gegevens met NTS zal Digikoppeling[4] worden gebruikt.
PA2 **Bovenliggend principe**	De dienst maakt gebruik van open standaarden[5]	De website zal voldoen aan de vigerende regelgeving m.b.t. toegankelijkheid. Op dit moment

NORA AP08		betreft dit de Webrichtlijnen[6]. Brieven worden opgeslagen in PDF/A-1 formaat[7].
PA3 Bovenliggend principe NORA AP40	De onweerlegbaarheid van berichtenuitwisseling wordt gegarandeerd door wederzijdse authenticatie en door versleuteling van elektronische handtekeningen.	De berichtenuitwisseling met NTS zal via een webservice (Digikoppeling) verlopen middels een PKIO-certificaat om de onweerlegbaarheid te borgen.

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