

aan DB
van Erik Bruinsma

onderwerp Voortgangsrapportage 3 Agenda Privacy
datum 22 maart 2022

Inleiding

Het DB heeft in de vergadering van maart 2021 de Agenda Privacybescherming vastgesteld. In de vergadering van 13 december is het DB akkoord gegaan met een nieuwe opzet van de Voortgangsrapportage met daarin een duidelijke scheiding tussen externe en interne ontwikkelingen, strategisch beleid en operationele/aankomende acties.

De diverse acties worden binnen de afzonderlijke divisies uitgevoerd, waarbij CSB een coördinerende rol heeft. Het DB krijgt maandelijks een voortgangsrapportage ter bespreking.

A. Externe en interne ontwikkelingen

Dit gedeelte geeft een vooruitblik over komende wetgeving, maatschappelijk ontwikkelingen of interne vragen die mogelijk impact kunnen hebben op het Privacybeleid van het CBS. Het DB kan proactief acties verbinden aan deze ontwikkelingen indien zij dit nodig achten.

➤ 1 (extern): DPIA ZOOM

Voor de heroverweging Zoom wachtte het CBS nog op de DPIA van SURF (ministerie JenV) dat recentelijk (17 maart) gepubliceerd is. Daarin wordt gesteld dat alle hoge databeschermingsrisico's zijn opgelost. Er zijn nog zes lage risico's, maar die kunnen overheidsorganisaties zelf ondervangen. Zie ook de toelichting op intranet: <https://cbsintranet/Paginas/Veilig-videobellen-met-Zoom.aspx>.

➤ 2 (extern): Hoofdpijnen beleid voor digitalisering

Op 8 maart 2022 is de Kamerbrief 'Hoofdpijnen beleid voor digitalisering' uitgestuurd waarin de ambitie en doelen staan voor de digitale transitie van onze samenleving. Deze hoofdpijnen komen voort uit het coalitieakkoord en zijn het startpunt voor de kabinetsbrede werkagenda Digitalisering. Voor het Privacybeleid betekent dit verdere stappen door het kabinet om privacy en gegevensbescherming verder te versterken, zoals:

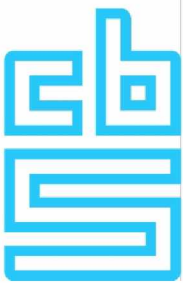
- geen gezichtsherkenning toepassen zonder strenge wettelijke afbakening en controle;
- het stimuleren van privacy-by-design technologie, bijvoorbeeld bij een breed bruikbare digitale identiteit;
- het ondersteunen van door de AP goedgekeurde gedragscodes en de invoering van certificeringsmechanismen om zo de goede bescherming van persoonsgegevens te bevorderen;
- de verdere inspanning naleving van de AVG door de overheid op orde te brengen (momenteel loopt er een onderzoek door het WODC, waarbij de (gebrekkige) naleving van de AVG door de overheid nader in kaart wordt gebracht);
- het kabinet beziet verder op welke wijze de functie van de FG kan worden versterkt.

➤ 3 (extern): Inzage BRP in MijnOverheid.nl

Vanaf 14 maart 2022 kunnen burgers daarom op MijnOverheid online inzien met welke (overheids)organisaties informatie uit de Basis Registratie Personen (BRP) worden gedeeld. Het CBS staat overigens niet in dit rijtje.

- Vraag aan DB: moet hier nog actie op genomen worden?

➤ 4 (intern): BSN Eindbeeld en verPRINnen



Op 21 maart is in het DB het BSN Eindbeeld vastgesteld (op nog wat tekstuele aanpassingen na) en tevens zijn de verbeterplannen voor reductie BSN vastgesteld. De stuurgroep en werkgroep voor de Actie verPRINnen zal toegevoegd worden als actiepunt onder B.

➤ **5. (intern): Bewaartermijnen**

Vanuit de privacy audit is afgelopen jaar aanbevolen om één CBS-brede procedure bewaartermijnen te maken. Hiervoor zijn al verschillende acties gestart.

- Vraag aan DB: actiehouders aanwijzen.

B. Strategisch

Dit gedeelte beschrijft de CBS brede beleidskaders en besluitstukken. In geel gemarkeerd zijn de aanpassingen ten opzichte van de vorige keer.

Actie 1 Verbeterplannen audit 2020 en 2021

De vier voornaamste verbeterpunten uit de privacy-audit 2020 staan hieronder. Bij de procesmonitor zijn ook de aanbevelingen van de audit 2021 meegenomen.

1. **Aantoonbaar onderhouden van rechten in Varonis.** De webapplicatie Varonis wordt binnen het CBS gebruikt om op een transparante manier de toegang tot de mappen (mappenstructuur, het beheer daarvan en de procedures daar omheen) te regelen, zonder dat er regelmatig een beroep gedaan hoeft te worden op BIT (ServiceDesk).

De verantwoordelijkheid voor het actualiseren van de rechten ligt daardoor bij de map eigenaren. Interne verschuivingen vormen een zwakke schakel wanneer dit niet geactualiseerd wordt. Personen die uit dienst treden worden namelijk automatisch verwijderd (geblokkeerd). Elk kwartaal doet Varonis periodiek een bericht uit naar alle map-eigenaren met de vraag om de rechten te actualiseren. De check of rechten goed zijn toegekend ligt exclusief bij de proceseigenaar en is inherent aan het door CBS gekozen model van gedelegeerd autorisatie management.

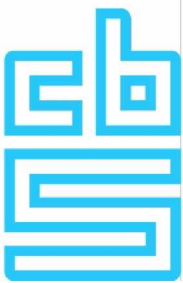
Acties:

- SAL heeft een script geschreven om nu (quick win) de rechten goed te onderhouden elk kwartaal en heeft met SSC gesproken om dit door te ontwikkelen tot een CBS breed script, door alle teams te gebruiken. Middels een POC gaan BIT en SAL samen onderzoeken of ze tot een verbeterde versie van de 'SAL scripts' kunnen komen om daarna voor het hele CBS tot een betere én gebruiksvriendelijkere controle van de Varonis rechten te komen.
- Er is gestart met een PoC. Er is een voortgangsoverleg geweest waarin onderstaande afspraken zijn gemaakt:
 1. Doel vaststellen. Doel is om de Varonis rechten controle tool die nu door SAL gebruikt wordt breder in te zetten. Idee is dat op basis van automatische controles "vlaggetjes" gezet worden bij verdachte regels bij de rechten rapportages. Op deze manier kan de proceseigenaar gericht een controle doen.
 2. Functionele behoefte in kaart brengen. 5.1.2.e en 5.1.2.e maken een voorstel en sturen dat uiterlijk 1 april naar het werkgroepje. 5.1.2.e en 5.1.2.e geven binnen 1 week reactie.
 3. Parallel aan de eerste stap is de technische haalbaarheid bepalen.
 4. Controle door FG (5.1.2.e). Hierbij "GO/NO-GO". Eventuele feedback verwerken.
 5. Uitvoeren PoC. Hierbij een GO/NO-GO.
 6. Bij positieve PoC overdracht naar BIT.
 7. Uitrol CBS breed.

Actiehouders: BIM

Betrokkenen: SAL en SSC (BIT, CISO), daarna rest CBS.

Laatste update: maart 2022.



Planning: april nieuwe update

2. **Procesmonitor niet op orde.** De procesmonitor is een lijst met alle primaire en secundaire processen van het CBS (zowel statistische als niet-statistische processen). Het vormt daarmee de procesboekhouding van het CBS. Deze lijst was in de vorm van een spreadsheet. De procesmonitor is afgelopen najaar door ontwikkeld naar een nieuw prototype, procesmonitor 2.0 (PM2.0).

Acties:

- Q1 2022: Door ontwikkelen prototype naar completere procesmonitor; er is een concept notitie herziening scope procesmonitor - een procesmonitor inclusief besturende processen en projecten - uitgezet voor bespreking. Ook denk de werkgroep PM2.0 na over de praktische invulling van de opname van besturende processen en projecten.
- Borgen proces om prototype PM2.0 actueel te houden

Vanuit de privacy audit 2021 zijn de volgende aandachtspunten gekomen:

- Opschoning baselinetoetsen;
- Opschoning persoonsgegevens in de procesmonitor.

In januari is besloten dat er een Chief Quality Officer komt die onder CSB valt en verantwoordelijk wordt voor de doorontwikkeling van de procesmonitor.

Actiehouders:

- Door ontwikkelen PM2.0: CSB (Chief Quality Officer)
- Opschoning en rapportage: procescoördinatoren

Betrokkenen: Alle divisies en proceseigenaren en procescoördinatoren

Laatste update: maart 2022.

Planning: Vacature CQO is uit. Opschonen procesmonitor is een doorlopend proces.

3. **Registratie Verwerkersovereenkomsten.** De inrichting van het proces m.b.t. verwerken van contracten en de daarbij horende signalen richting de contracteigenaar m.b.t. aflopen van contracten is voor de zomer opnieuw ingericht en live gegaan. Bij nieuwe overeenkomsten is het automatisch in het werkproces opgenomen. Momenteel wordt gewerkt aan het handmatig aanvullen en opschonen van bestaande contracten uit de oude database. Daarin ontbrak bv informatie m.b.t. looptijden, het was verkeerd ingevoerd of de contracteigenaren werkten niet meer bij het CBS. Ook waren er contracten apart opgeslagen in het dossier van de inkooprelatie.

Privacy audit 2021:

- Herstelactie uitvoeren om te onderzoeken welke leveranciers, wie persoonsgegevens verwerkt en of met deze partijen een verwerkersovereenkomst is afgesloten.

Actiehouder: BIM

Laatste update: januari 2022.

Planning en resultaat: checken wat er nog moet gebeuren aangezien de acties in december voltooit waren en de privacy audit in oktober plaats vond.

4. **Bewaartermijnen.** Vanuit de privacy audit 2021 werd geconstateerd dat verschillende directieniveaus verschillende vormen van 'procedures bewaartermijnen' hebben. Uitzonderingen zijn niet altijd vastgelegd, ook de criteria voor uitzonderingen zijn niet duidelijk. De aanbeveling vanuit de audit is om één CBS-brede procedure bewaartermijnen te maken, met daarbij op eenduidige wijze vastleggen van uitzonderingen, evenals planning en geldigheid.

Actiehouder: moet nog afgestemd worden.

Laatste update: maart 2022.

Planning en resultaat: SER is al gestart met een overzichtsdocument bewaartermijnen SER. Dit zou als basis gebruikt kunnen worden. Daarnaast wordt er ook gewerkt aan het vaststellen van de bewaartermijnen bij de nieuwe B&I architectuur door SER.



Actie 2 Communicatiestrategie

Voor een volgende stap in de communicatiestrategie is afgesproken dat de CPO samen met CCN en de PC een memo maakt van de doelgroepen die te onderscheiden zijn, met de daarbij behorende onderwerpen waarover gecommuniceerd moet worden. Daarop zal een prioritering en strategie ontwikkeld worden.

Actiehouder: CPO, PC en CCN

Laatste update: januari 2022.

Planning en resultaat: Voorjaar inventarisatie doelgroepen en onderwerpen.

Actie 3 BSN-toegang

Beleid binnen het CBS is dat het aantal medewerkers dat toegang heeft tot de BSN minimaal is en dat data die we ontvangen, zo vroeg mogelijk worden ontdaan van BSN en worden vervangen door een RIN. In de praktijk weten we dat een aantal processen gebruik maakt van de BSN bij het controleren van data, en/of voor het uitvoeren van een productieproces. Gevraagd is om het aantal medewerkers dat toegang heeft tot BSN-nummers zoveel mogelijk te reduceren, en daar waar toegang noodzakelijk is dat duidelijk te beargumenteren en vast te leggen.

Acties:

1. Toekomstvisie met eindbeeld BSN toegangen.
2. Verbeterplannen divisies terugdringen BSN

Actiehouder: SER voor de verbeterplannen en CSB voor het eindbeeld BSN.

Betrokkenen: verschillende werkgroepen bij alle divisies

Laatste update: maart 2022.

Planning en resultaat: maandag 21 maart besproken en vastgesteld in het DB.

Actie 4 Herooverweging Zoom

Na een jaar thuiswerken en de introductie van Zoom als video-conferencing tool en naar aanleiding van een gesprek met PrivacyFirst is op 10 mei door het DB besloten om een herooverweging van het gebruik van Zoom te doen. Deze herooverweging kon in september nog niet als besluitstuk meegestuurd worden voor de DB-vergadering omdat de opmerkingen van de FG nog niet verwerkt waren. Ook nu loopt het advies nog vertraging op omdat het CBS wil wachten op de reactie van SURF, die namens JenV voor ZOOM een DPIA heeft laten uitvoeren. Dit onderzoek is uitgevoerd door de privacycompany (doen alle privacy onderzoeken zoals MS, Google etc.). Gezien de privacy vraag moet hierop gewacht worden voor een compleet advies.

SURF heeft 17 maart het advies gepubliceerd.

Actie: Beleidsstuk herooverweging Zoom.

Actiehouder: BIM

Laatste update: maart 2021.

Planning: ter vaststelling DB medio april 2022.



C. Tactisch en operationeel

Dit gedeelte beschrijft alle lopende acties of aankomende acties waar op dit moment geen nieuwe ontwikkelingen te melden zijn.

Actie 6 Dataminimalisatie

Naar aanleiding van een gesprek met PrivacyFirst heeft het CBS onderzocht of de dataminimalisatie van bijzondere persoonsgegevens (medische gegevens, strafrechtelijke gegevens) maximaal geborgd is in de processen. Met betrekking tot de strafrechtgegevens is een DPIA traject gestart en is aangegeven welke data het CBS nodig heeft voor de statistieken. Eind 2021 is gestart met een herontwerp van het hele proces, waarin dataminimalisatie wordt meegenomen. Dit herontwerp zal eind 2022 zijn afgerond, waarna de dataminimalisatie voor de resterende processen op het gebied van strafrecht geborgd is.

Actie: Herontwerp strafrechtgegevens ligt op schema. Dataminimalisatie met betrekking tot dataleveringen door het Centraal Administratie Kantoor (gezondheidsdata) is gerealiseerd.

Actiehouder: SER

Laatste update: maart 2022.

Planning: Implementatie 2022.

Actie 7 Borgen up-to-date houden beleid en three lines of defence

Governance is ingericht, evenals een overlegstructuur tussen PC, PO, FG en CPO. Begin 2022 zullen de PC en de CPO gezamenlijk een privacy training volgen. Deze is ondertussen uitgekozen en betreft een cursus die ook aandacht besteedt aan de verschillende rollen binnen een organisatie. CPO heeft een presentatie gemaakt voor geïnteresseerde teams en DT's over privacy en de three lines of defence. Deze is al gehouden bij CCN (DT en Corporate), BIM (DT), CAD en CSB.

De hoofddirectie SER heeft in maart een document vastgesteld waarin de privacy governance van SER is beschreven. Dit gaat uiteraard uit van de three line of defense zoals die CBS-breed worden ingezet.

Acties: Actualisatie kaders privacy governance.

Planning: april 2022 update.

Actiehouder: CSB (CPO en PC)

Betrokkenen: Alle divisies (PC)

Laatste update: maart 2022.

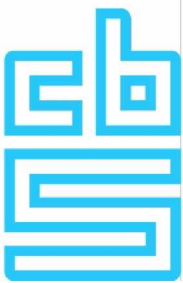
Planning: april 2022

Actie 8 Intern awareness programma

Een managersmeeting over privacy is afgelopen november de aftrap geweest naar awareness sessies per divisie, sector en teams voor 2022. In het voorjaar van 2022 zullen awareness sessies binnen de divisies plaatsvinden waarbij de privacy coördinatoren zullen/kunnen ondersteunen/faciliteren.

Acties:

- SER: In januari hebben het DT SER en de SER PC's gesproken over de vervolgaanpak voor het awarenessprogramma. Daarbij wordt momenteel uitgegaan van een aanpak die uitgaat van bijeenkomsten op divisie- en op teamniveau, planning is vóór de zomer van 2022. De PC's spelen een belangrijke rol bij de organisatie hiervan. Daarnaast is het idee om te kijken naar CBS-brede privacytrainingen voor medewerkers en continue activiteiten gericht op het bevorderen van de awareness.
- CCN: CCN divisieteam heeft een presentatie gehad van de CPO over privacy, privacybeleid en de verschillende rollen binnen de privacy governance. CPO en CCN Corporate met privacy coördinator van CCN gaan samen met enkele andere PC's een communicatieplan opstellen.
- BIM: 22 maart komen de CPO en PC BIM een korte presentatie geven in het DT over privacybeleid.



- DRI: DRI heeft een inventarisatie gemaakt van trajecten waar geanticipeerd wordt op privacy aspecten. Hieruit is af te leiden dat er al veel awareness is en dat het breed uitzetten van awareness sessies in zekere zin achterhaald is. De PC heeft overleggen met de directeurs van DRI om verder af te stemmen wat er nog aan awareness gedaan kan worden. De verwachting is dat aandacht vooral zal uitgaan naar duidelijkheid over en een goed invulling van de privacy governance. En naar de behoefte om medewerkers via documentatie ("factsheets", CBS breed) te informeren over hoe in de verschillende situaties (thuis, op werk, buiten kantoor, binnen de werkprocessen en bij innovaties) om te gaan met privacy.

Actiehouder: CCN en alle divisies

Laatste update: maart 2022.

Betrokkenen: CPO, PC, CCN.

Actie 9 Datalekprocedure Topdeskmeldingen

Uit een onderzoek van de FG naar Topdeskmeldingen komen een paar verbeterpunten. Het gaat hier met name om het volgen van de PDCA om tot verbetering te komen. De indruk is dat het merendeel van de beveiligingsincidenten, en daarmee mogelijke datalekken, niet aangemeld worden in Topdesk. Verder zou er meer gericht gezocht kunnen worden bij mogelijke concentratiepunten, bijvoorbeeld aan loketten waar hardware voor medewerkers vervangen worden (bij DRI en IT-service desk). Een verbeteractie is inmiddels doorgevoerd: in Casper is een extra knop gemaakt waarmee medewerkers een (vermoedelijk) datalek kunnen melden. Deze melding wordt via een interface doorgeleid naar Topdesk (waar nu nog wel wat praktisch ingeregeld moet worden). In de awareness-campagne zal hier aandacht aan worden besteden alsmede in de reguliere communicatie. Ook heeft de FG geconstateerd dat de procedure voor toegangspassen bij verlies nog speciale aandacht verdient. Tevens aandacht voor de vraag hoe veilig de pas is.

Actie:

- Nieuwe procedure voor datalekken wordt opgesteld waarmee ook facilitaire zaken in worden meegenomen.

Recentelijk is er een rapport van de ADR verschenen over de afhandeling van datalekken bij Financiën. De focus van de aanbevelingen lagen vooral op de opvolging van datalekken, het na kunnen gaan welke maatregelen daadwerkelijk zijn getroffen. Deze aanbevelingen kunnen ertoe leiden dat de beveiliging van de gegevens (verder) wordt verbeterd, en herhaling van (dezelfde soort) lekken wordt voorkomen. Deze aanbevelingen zullen meegenomen worden in de nieuwe procedure datalekken.

Audit 2021: Aanbevelingen FG mei 2021 niet overgenomen en procedure wordt niet herzien.

Actiehouder: CSB en BIM (CPO ism SSC en facilitair)

Betrokkenen: SSC en facilitair.

Laatste update: maart 2022.

Planning: april 2022.

Actie 10 Kennismaking DG Belangengroepen

Verschillende acties zijn afgelopen jaar ingezet:

- Ethische sessie over OV-data met de privacy-belangenorganisaties.
- Community-dag gemeenten (UDC's) op 11 oktober met dit jaar als thema Privacy.
- Kennismaking DG met Bits of Freedom op 19 oktober.

Geen nieuwe kennismakingen bekend.

Acties 11: E-learning module Awareness 2.0. vernieuwen.

Voor een verder awareness programma heeft BIM geconcludeerd dat het niet zinvol is om de bestaande module aan te passen (eerder was sprake van aanpassing op 35 punten). De reden is dat dit te intensief is qua kosten en tijd. Er moet een nieuwe module ontwikkeld worden. Deze module is er in eerste instantie voor alle medewerkers. De nieuwe medewerkers maken deze nieuwe



module ook. De nieuw ontwikkelde module wordt in de loop van de tijd uitgebreid met nieuwe casuïstiek adhv de (nog te ontwikkelen) richtlijnen. Focus: eerst bewustwording, dan specifieker.

Actiehouder: BIM (SSC)

Betrokkenen: BPO en CCN (inhoudelijke input van SSC).

Laatste update: november 2021

Planning: Zodra SSC capaciteit heeft voor de inhoudelijke bijdrage kan het project starten.

Actie 12 Recht op inzage gegevens

In het DB is eerder in het kader van het actieprogramma Open op Orde gesproken over het recht op inzage van gegevens zoals vermeld in de AVG. CSB heeft de memo 'analyse huidige situatie inzageverzoeken' in november in het DB gebracht ter kennisgeving.

Actie: Actualiseren communicatie (o.a. van de website).

Actiehouder: CSB

Laatste update: november 2021

Planning: april 2022

Actie 13 Beleid onthullingsgevaar statistische informatie in de nabije toekomst

Op basis van een memo van de FG van juni 2021 waarin hij wijst op mogelijke toekomstige risico's op onthulling van data, heeft in juli 2021 een gesprek plaatsgevonden tussen de DG, pDG, FG en CPO ai. Daarin is afgesproken dat het Statistisch Beveiligingsoverleg (SBO) onder leiding van de Chief Methodology Officer (CMO) met een plan van aanpak komt om op korte termijn eens te testen hoe het staat met onze beveiliging, met name bij het combineren van openbare CBS-data.

Acties:

1. Plan van aanpak voor het testen op onthulling bij het combineren van openbare CBS-data (actie voor CMO en CPO)
2. Testen informatiebeveiliging door ethisch hacken (CISO)
3. Actualiseren crisismanagementplan en organiseren van een crisisoefening (actie voor Beveiligingscoördinator/CSB)

Actiehouders: DRI

Betrokkenen: SBO (Statistisch Beveiligingsoverleg), SSC, DRI.

Laatste update: december 2021

Planning: ???

Actie 14 Wachtwoordbeleid respondenten niet compliant

FG heeft aangegeven dat het wachtwoordbeleid respondenten niet compliant is (bijzondere persoonsgegevens, zoals bijvoorbeeld gezondheidsdata in enquêtes waarvoor 2 factor authenticatie voor nodig is).

Acties:

- De CBS-brede beleidswerkgroep inlogbeleid is bezig om het toekomstige wachtwoordbeleid vorm te geven. Daar zitten o.a. ook de FG bij.
- Het aandachtspunt betreft uitvraag van bijzondere persoonsgegevens bij lege vragenlijsten. Voor-ingevulde vragenlijsten met bijzondere persoonsgegevens komen niet voor.
- Gebruik van DigiD voor tweefactor authenticatie bij persoonsonderzoeken wordt onderzocht op haalbaarheid en wenselijkheid.

Actiehouder: DRI

Laatste update: maart 2022.

Planning: april volgende update.

Actie 15 Extra stap vereist bij gebruik standard contractual clauses (SCC) RA-toegang derde landen.

Alle contracten zijn inmiddels aangepast zijn. Dit is met beleid op te lossen, een memo hierover is in de maak.



Actie: Memo maken.

Actiehouder: CSB

Betrokkenen: DRI

Laatste update: december 2021

Planning: April 2022

Actie 16 Facilitair gebruik versus gebruik voor statistiek.

FG heeft geconstateerd dat de grens tussen facilitair gebruik versus statistisch gebruik persoonsgegevens niet altijd even duidelijk is. Hoe ver wil het CBS gaan met het gebruik van statistische gegevens voor optimalisering van het maken van statistieken?

Actie: De FG stelt een memo op met een casusbeschrijving, waarna gekeken wordt of en zo ja welke verdere acties nodig zijn.

Laatste update: november 2021

Actie 17: Beleidskader terugleveren responsdata.

Het CBS moet conform de Wet op het CBS en de AVG zeer zorgvuldig omgaan met gegevens over natuurlijke personen en bedrijven. In de praktijk komt het voor dat bij het benaderen van respondenten wordt gevraagd om historische antwoorden om de respondent te ondersteunen in het formuleren van nieuwe antwoorden. Ook komt het voor dat het CBS vragen heeft over afwijkingen tussen achtereenvolgende (historische en actuele) antwoorden en daarbij informatie over de eerste verstrekt. Dit laatste is recentelijk gebeurd waarbij het CBS op verzoek van de respondent zelf een antwoord heeft teruggekoppeld waarna de respondent een klacht indiende omdat het CBS vertrouwelijke informatie zou delen. De FG heeft hierop een advies geschreven 'inzake incidentele teruglevering responsdata'.

Actie: Maak een duidelijk expliciet beleid over (1) onder welke omstandigheden responsdata teruggeleverd mag worden, en (2) op welke manier dit mag gebeuren.

Actiehouder: CSB

Betrokkenen: EBN, DVZ.

Laatste update: februari 2022.

Planning: Q2.

Vervolg

De volgende rapportage volgt 25 april 2022.