

aan DB
van Erik Bruinsma

onderwerp Voortgangsrapportage 4 Agenda Privacy juni
datum 7 juni 2022

Inleiding

Het DB heeft in de vergadering van maart 2021 de Agenda Privacybescherming vastgesteld. Maandelijks rapporteert de CPO over de voortgang van de Privacy Agenda. Daarin wordt aandacht besteed aan 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): Voorstel data act en reactie AP

Op 23 februari heeft de Europese Commissie de Data Act voorgesteld, een nieuwe verordening met regels over de toegang tot en het gebruik van data die in alle economische sectoren van de Europese Unie gegenereerd worden. Met de nieuwe regels hoopt de Commissie obstakels voor de toegang tot data weg te nemen. Eén van de maartregelen betreft: “Middelen voor overheidsinstanties om toegang te krijgen tot data die in het bezit zijn van de particuliere sector en die noodzakelijk zijn voor specifieke doeleinden van algemeen belang. Dit is met name in het geval van algemene noodsituaties (exceptional needs), zoals overstromingen en bosbranden, of om een wettelijk mandaat uit te voeren indien data niet op andere wijze beschikbaar zijn”.

- De European Data Protection Board (EDPB) heeft in een gezamenlijk advies benadrukt dat de Data Act geen afbreuk mag doen aan de bescherming van persoonsgegevens die de Algemene verordening gegevensbescherming (AVG) biedt. Ook vinden ze dat overheden geen te ruime bevoegdheid moeten krijgen om persoonsgegevens op te eisen van private partijen. Voor het CBS is vooral het gedeelte Business to Governance (B2G) interessant, maar de data act geeft op dit moment nog geen ruimte voor de reguliere productie van statistiek. Dit zou volgens het CBS wel mogelijk moeten zijn, passend binnen de AVG.

➤ 2. (extern) Boete AP Belastingdienst en BZ

De belastingdienst heeft een boete gekregen van 3,7 miljoen vanwege de illegale verwerking van persoonsgegevens in de Fraude Signalering Voorziening (FSV).

- Een aantal factoren speelde daarbij een belangrijke rol: geen verwerkingsgrondslag, onvoldoende beveiliging en de FG was niet betrokken bij de uitgevoerde risicoanalyses. Het boetebesluit geeft een goed beeld van de wijze waarop de AP haar afwegingen maakt.

BZ heeft een boete gekregen van een half miljoen voor het feit dat de beveiliging van het Nationaal Visum Informatie Systeem onvoldoende was.

BZ werkt nu aan een overzicht van best practices en handvatten ten aanzien van onderzoeken naar gegevensverwerking door de AP. Als het overzicht van BZ klaar zal CBS kijken wat we hiervan kunnen leren.

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

In de Privacy Agenda van maart werd gevraagd waarom het CBS niet zichtbaar is in het rijtje (overheids)organisaties die informatie uit de Basis Registratie Personen (BRP) ontvangen. De



reden blijkt van technische aard te zijn. RvIG geeft aan dat het CBS de BRP integraal krijgt en daardoor geen afnemersindicaties krijgt waardoor het door de software niet in de overzichten meegenomen kan worden. Dit geldt niet alleen voor het CBS en aanpassing vergt een grote aanpassing in de software van RvIG. Het CBS neemt daarom op dit moment geen actie hierop.

➤ **4 (intern): three lines of defence**

Er is een volgende stap gezet in de implementatie van de three lines of defence, door een gezamenlijke cursus waarin aandacht was voor de rolverdeling en taken en het opzetten van een actieplan voor gezamenlijke doelen en actie van de PC en CPO. Zie hiervoor ook Bijlage 1 'Privacy governance terugblik 2021 en actiepunten 2022.docx'.

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:

- Het automatiseren van de rechtencontrole op basis van het script dat bij SAL gebruikt wordt blijkt in praktijk lastiger dan gehoopt. Op dit moment wordt een andere route bekeken, namelijk of de rechtencontrole gedelegeerd kan worden naar de projectleiders van de betreffende projecten en/of processen. Als dat kan, zal dat niet leiden tot minder werk, maar dan zou wel betekenen dat het werk niet meer allemaal bij de teamhoofden ligt.
- De vraag hoe wij het rechtenbeheer beter op orde kunnen krijgen is een hele complexe vraag dat door SSC wordt opgepakt en op de Agenda IB een plek moet krijgen. De vragen die hier vanuit SSC spelen zijn:
 1. Hoe kunnen we terug naar een enkel account voor de meeste CBSers?
 2. Hoe beheren we autorisaties binnen applicaties en hoe organiseren we dat? (Denodo).
 3. Houden we vast aan gedelegeerd Autorisatie Mgt? Of gaan we dat centraliseren?
 4. Hoe krijgen we inzicht in wat een persoon met meerdere accounts aan autorisaties heeft

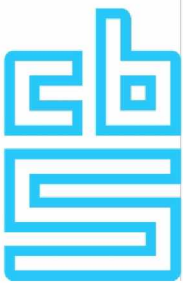
Dit zijn hele zware projecten die veel vragen van Business en IT. De CISO geeft aan dat hiervoor een gerenommeerde, externe partij voor aangetrokken moet worden.

Actiehouder: BIM

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

Laatste update: juni 2022.

Planning: ???



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).

Doorontwikkeling van PM 2.0 wordt, door het wegvallen van 5.1.2.e getemporeerd tot de komst van de CQO. Grote stappen zullen niet gezet kunnen worden. Opschoning van de (huidige) procesmonitor vindt wel plaats en de proceseigenaren is gevraagd om –waar nog nodig- hun baseline toetsen op te schonen.

Acties:

- 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: juni 2022.

Planning: ???

3. **Registratie Verwerkersovereenkomsten.**

Een aanbeveling vanuit de **Privacy audit 2021** was:

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

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. Inmiddels is de opschoonactie m.b.t. contracten afgerond. Alle ontbrekende data m.b.t. contractinformatie is aangevuld, signalen en taken m.b.t. opzegging/verlengingen zijn actief en alle contractdocumenten die bij ons bekend zijn verwerkt. Alle nieuwe contractdocumenten die geadministreerd moeten worden dient men in CASPER vanuit het Inkoopportaal aan te leveren via de knop “inkoopcontract registreren”. De aanvrager zal dan via CASPER een melding krijgen als de taak verwerkt is. Bij het registreren van een inkoopcontract (door de contractverantwoordelijke/budgethouder) wordt gevraagd of er sprake is van een verwerkersovereenkomst. Verantwoordelijkheid ligt bij de contractverantwoordelijke die bij twijfel advies kan vragen aan CSB juridisch.

Actie: CAD is gevraagd of hiermee aan de privacy audit is voldaan. Dat is nog niet het geval. Daarom heeft de CPO i.o.m. team Bedrijfsadministratie en de PC de volgende acties geformuleerd:

- CPO en PC leveren een stukje tekst dat bij Casper komt te staan over wanneer leveringsovereenkomsten nodig zijn en bij wie ze meer informatie kunnen opvragen.
- CPO en PC kijken hoe ze kunnen bijdragen aan de awareness binnen de divisies.
- CPO en PC kijken gezamenlijk of er een korte instructie/hand-out gemaakt kan worden.

Actiehouder: BIM



Laatste update: juni 2022.

Planning en resultaat: augustus 2022.

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. Aanbeveling: maak één CBS-brede procedure bewaartermijnen met daarin de uitzonderingen, planning en geldigheid vastgelegd.

Acties:

1. SER heeft een document bewaartermijnen afgerond. Deze wordt door de PC en CPO naast de bestaande documentatie van de andere divisies gelegd. Dit resulteert in een globaal CBS breed overzicht met verwijzingen naar de geüpdatet documentatie van de divisies zelf en een factsheet als hulpmiddel (betreft alleen bewaartermijnen persoonsgegevens).
2. Er is gestart zijn met het formuleren van de nieuwe bewaartermijnen die passen bij de nieuwe B&I architectuur.

Actiehouder: CSB

Laatste update: juni 2022.

Planning en resultaat: update in juli.

Actie 2 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 aanpassen n.a.v. opmerkingen DB 28 maart en opstellen uitvraagformulier + voorbeeld rapportage voor meenemen in de cyclus jaarplan.
2. Het DB is akkoord met het verder uitwerken van het geschetste verPRIN beleid. Een stuurgroep en werkgroep zijn ondertussen voortvarend van start gegaan.

Actiehouder: SER voor het verPRINbeleid en CSB voor het eindbeeld BSN met uitvraag en rapportageformulier.

Betrokkenen: verschillende werkgroepen bij alle divisies

Laatste update: juni 2022.

Planning en resultaat: in de volgende voortgangsrapportage is het Eindbeeld BSN aangepast en ligt er een uitvraagformulier en voorbeeldrapportage ter vaststelling voor het DB voor daadwerkelijke uitvraag na de zomer om mee te nemen in de cyclus van het jaarplan. Ook zal er een versie gereed zijn van de uitwerking van het verPRINbeleid. De werkgroep verPRINnen verwacht in september een notitie gereed te hebben voor het DB gereed met de resultaten en voorstellen voor besluitvorming.

Actie 3 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 2021 door het DB besloten om een herooverweging van het gebruik van Zoom te doen. Deze herooverweging heeft vertraging opgelopen omdat het CBS wilde 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.). SURF heeft 17 maart het advies gepubliceerd.

Actie: Beleidsstuk herooverweging Zoom 25 april in DB vastgesteld.

Actiehouder: BIM



Laatste update: juni 2022.

Planning: 25 april vastgesteld en kan van de agenda gehaald worden.

C. Tactisch en operationeel

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

Actie 4 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 het resterende proces op het gebied van strafrecht geborgd is. Voor de medische data wordt nog gewerkt aan dataminimalisatie van drie databronnen. In Q3 2022 worden er hiervoor twee afgerond en de laatste in Q4.

Actie: Acties herontwerp strafrechtgegevens en medische gegevens liggen op schema.

Actiehouder: SER

Laatste update: juni 2022.

Planning: Implementatie 2022.

Actie 5 Borgen up-to-date houden beleid en three lines of defence

Governance is ingericht, evenals een overlegstructuur tussen PC, PO, FG en CPO. Per Divisie worden aparte uitwerkingen van de governance structuur en taken vastgesteld.

Eind maart 2022 hebben de PC, CPO, FG, juristen en CAD gezamenlijk een privacy training gevolgd. CPO heeft een presentatie gemaakt voor geïnteresseerde teams, werkgroepen en DT's en voor gebruik PC die de awareness sessies binnen de divisies organiseren. Ook is er een document met gezamenlijke doelen en acties opgesteld, zie bijlage 1.

Acties:

- Notitie met terugblik en actiepunten privacy governance voor de PC en CPO (bijlage 1). Dit is een aanbeveling die voortkomt uit de Privacy audit 2021.

Actiehouder: CSB (CPO en PC)

Betrokkenen: Alle divisies (PC)

Laatste update: juni 2022.

Planning: uitvoering 2022, evaluatie eind 2022.

Actie 6 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:

- CPO en PC: start met inrichten nieuwe intranetsite.
- SER: In maart heeft het DT SER ingestemd met een voorstel van de SER PC's over vervolgaanpak voor het awarenessprogramma. Daarbij zal er sprake zijn van bijeenkomsten op divisieniveau, gevolgd door sessies op teamniveau. De divisiebrede bijeenkomsten vinden plaats op 20 en 21 juni. 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. **Start bijeenkomst heeft plaatsgevonden, communicatieplan wordt nu opgesteld door CCN.**
- BIM: 22 maart heeft de CPO en PC BIM een korte presentatie gegeven 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 directeuren 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 ("facsheets", 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.
- **EBN: Na vaststelling van de privacy governance EBN wordt de interne awareness binnen de directies vergroot door hier binnen in de MT's verdere aandacht aan te besteden en de afzonderlijke teams hierin mee te nemen.**

Actiehouder: CCN en alle divisies

Laatste update: juni 2022.

Betrokkenen: CPO, PC, CCN.

Actie 7 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.

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

Actie:

- Nieuwe procedure voor datalekken wordt opgesteld waarmee ook facilitaire zaken in worden meegenomen. **Deze nieuwe procedure zal gepaard gaan met een korte handout.**
- Inrichting in Topdesk. **Op dit moment worden alle technische zaken ingericht.**
- **Reguliere evaluatie datalekken CBS. Het datalekregister is ook bedoeld als leerinstrument (maatregelen nemen om soortgelijke datalekken in de toekomst te voorkomen). Reguliere evaluaties helpen hierbij.**

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

Betrokkenen: SSC en facilitair.

Laatste update: juni 2022.

Planning: Augustus 2022.

Acties 8: 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 9 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 10 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)
 - Er heeft inmiddels een hackathon plaatsgevonden i.s.m. POPNET (Universiteit Leiden en UvA) op 3 mei 2022. Het doel van deze hackathon was om ervaring op te doen met het organiseren van een hackathon waar privacy/anonimiteit/onthulling centraal staat (i.p.v. een tool of een onderzoek)
 - De uitkomsten en de ervaringen van deze hackathon zullen gebruikt worden om op een later tijdstip een hackathon te organiseren waarbij studenten onderzoeken hoe goed de beveiliging van de CBS open data in de praktijk is.
 - Aan de nog te houden hackathon zitten meer juridische en communicatieve kanten: wat te doen als er onverhoopt iets onthuld wordt? Wie communiceert wat en op welk moment? Moeten studenten een verklaring ondertekenen?

Zie ook: [Hoe anoniem ben je? - Blog Statistische Beveiliging](#)

3. Actualiseren crisismanagementplan en organiseren van een crisisoefening (actie voor Beveiligingscoördinator/CSB)

Actiehouders: DRI

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

Laatste update: juni 2022

Planning: Actie 2 begin mei afgerond?

Actie 11 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. Daarvoor wordt een pilot voorbereid.
- Er wordt gewerkt aan een beleidsnotitie voor het DB met het voorstel in de toekomst met hogere betrouwbaarheidsniveaus te kunnen werken en daar naar toe te groeien door authenticatie via DigiD en eHerkenning mogelijk te maken.

Actiehouder: DRI

Laatste update: juni 2022.

Planning: augustus volgende update.

Actie 12 Extra stap vereist bij gebruik standard contractual clauses (SCC) RA-toegang derde landen.

Alle contracten zijn inmiddels aangepast zijn. Voor de derdelanden (landen die niet vallen onder de AVG of een adequaatheidsbesluit hebben) zou aanvullend onderzoek nodig zijn. In Bijlage 2 'Voorstel derdelanden zonder aangepaste SCC.docx' wordt het DB gevraagd in te stemmen met het advies geen aanvullend beleid te maken.

Actie: Memo maken aanvullend beleid derdelanden zonder aangepaste SCC.

Actiehouder: CSB

Betrokkenen: DRI

Laatste update: juni 2022

Planning: Besluit DB juni 2022.

Actie 13 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 14: 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: Q3.

Vervolg

De volgende rapportage volgt in augustus 2022.