

aan DB

van 5.1.2.e

onderwerp Voortgangsrapportage 1 Agenda Privacy

datum 25 januari 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): Motie Marijnissen

Naar aanleiding van het rapport 'Ongekend Onrecht' van de Parlementaire Ondervragingscommissie Kinderopvangtoeslag (POK) zijn in het debat van 19 januari 2021 meerdere moties aangenomen en toezeggingen gedaan aan de Kamer. In het kader van de motie Marijnissen heeft EZK het CBS gevraagd een inventarisatie te doen van alle verwerkingen rondom seksregistratie en aan afkomst gerelateerde indicatoren bij gebruik risicomodellen. Planning: 7 februari worden de 2 memo's ter kennisgeving langs het DB gestuurd.

➤ 2 (intern): Gender en seksregistratie

De motie en de follow-up van de vragen leiden tot meer vragen aan het CBS vanuit het rijk (denk aan de uitvraag BZK over de impact van eventuele wijzigingen van het gegeven geslacht in de BRP door mogelijke versoepeling van de transgenderwet en recent een uitvraag van EZK). Tevens heeft dit ook intern CBS tot vragen en acties geleid rondom onze eigen dataverzameling en uitvraag van gender in enquêtes. Als organisatie willen we inclusief zijn, ook in de verzameling en rapportage over gender en tegelijkertijd moeten we rekening houden met/voorbereid zijn op mogelijke toekomstige wijzigingen in overheidsregistraties. Een recente interne uitvraag over de globale impact van wijzigingen rond het gegeven geslacht heeft uitgewezen dat die groot zal zijn. CBS breed is het belangrijk om eenduidige begrippen te gebruiken.

- **Vraag aan DB:** wil het DB opdracht geven tot een CBS brede inventarisatie van de ontwikkelingen, impact en uitdagingen rondom input en output van seksregistratie op de korte en lange termijn?
- **Voorgestelde actiehouder:** SER (i.s.m. werkgroep DRI en CSB).

➤ 3 (extern): Leveranciersmanagement

Dit wordt een van de speerpunten in het privacybeleid voor 2022 van EZK. CIO-office van EZK constateert dat, naast de verwerkersovereenkomsten, het ook noodzakelijk is om richtlijnen op te stellen m.b.t. leveranciersmanagement voor privacy en IB. De CIO-office wil een aanzet geven tot een meer systematische toetsing van de wijze waarop verwerkers de gemaakte afspraken naleven voor zowel privacy als IB (denk aan externe audit vragen aan verwerkers).



➤ **4 (Extern en intern): Privacy audit**

Het CBS is wederom privacy gecertificeerd. Er zijn 8 aanbevelingen gedaan (zie de memo, bijlage 1).

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. Dinsdag 25/2 is er een voortgangsoverleg.**

Actiehouder: BIM

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

Laatste update: november 2021.

Planning: maart

2. **Procesmonitor niet op orde.** De procesmonitor is een lijst met alle primaire en secundaire processen van het CBS. Deze lijst was in de vorm van een spreadsheet en betreft zowel statistische als niet-statistische processen. Het vormt daarmee de procesboekhouding van het CBS.

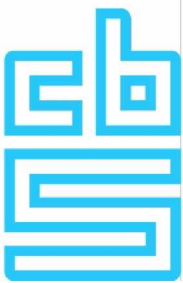
De procesmonitor is niet compleet en niet actueel waardoor er geen goed overzicht is van processen en eigenaren. In de Stuurgroep Continu Verbeteren van 7 juli is het plan van aanpak voor een procesmonitor 2.0 (PM2.0) goedgekeurd en de uitvoering daarvan voortvarend opgepakt.

Acties december 2021:

- Invoeren prototype PM2.0 in december 2021.
- Door ontwikkelen prototype naar completere procesmonitor.
- 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.



Vraag aan DB: wil het DB een actiehouder aanwijzen voor de CBS brede opvolging van de verbeterpunten PM?

Voorstel actiehouder: BIM?

Actiehouder nu: Proceseigenaren via opdracht top (CCV) naar hoofddirecteuren en rapportage naar procescoördinatoren.

Betrokkenen: Alle divisies en proceseigenaren en procescoördinatoren

Laatste update: december 2021.

Planning: opschonen procesmonitor is nog 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.

Laatste update: december 2021. De acties zijn in december afgerond en deze actie zou van de Agenda gehaald worden.

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: december 2021.

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

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: juni 2021.

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. Daarvoor zijn afgelopen jaar de volgende acties uitgevoerd:

- Standaard rechtenstructuur Varonis is onderzocht en daar is een rapport van verschenen (werkgroep SER, EBN, DRI en functioneel beheer);
- 2 metingen (maart en september) om een CBS breed beeld te krijgen over het aantal medewerkers dat toegang heeft tot BSN.
- Mogelijkheid terugdringen van BSN toegangen met Quick wins (rapport in november meegestuurd).

**Acties:**

1. Reduceren BSN toegangen met 33% door middel van de Quick wins en scenario's inventarisatie verdere reductie BSN toegangen.
2. Toekomstvisie met eindbeeld BSN toegangen.
3. Naast BSN ook NAW toegangen meenemen in de reductie.

Actiehouder: SER (CSB voor het eindbeeld BSN)

Betrokkenen: verschillende werkgroepen bij alle divisies

Laatste update: december 2021

Planning: medio februari (actie 2) en februari-maart (actie 1).

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) en wordt eind dit jaar publiekelijk gemaakt. Gezien de privacy vraag moet hierop gewacht worden voor een compleet advies.

Half januari is een afrondende meeting tussen ZOOM en SURF. Dan heeft SURF nog 3 a 4 weken nodig om hun rapport gereed te maken, pas daarna krijgt het CBS beschikking over het advies en kan dat meenemen in de eigen herooverweging Zoom.

Actie: Beleidsstuk herooverweging Zoom.

Actiehouder: BIM

Laatste update: november 2021.

Planning: ter vaststelling DB februari/maart 2022.

Actie 5 Beleid logging en monitoring

Beleidsstuk over het loggings-en monitoringsbeleid en onderliggende documenten zijn in het DB van 13 december ingebracht. Het beleid gaat daarmee de kaders stellen waarbinnen bijvoorbeeld het Security Service Center meerjarig loggings- en monitoringsoftware kan inregelen. Dit beleidsstuk is nog niet compleet en zal verder aangepast worden (met name het gedeelte rondom monitoring moet nog aangevuld worden).

Actie: Voltooien beleidsstuk L&M.

Actiehouder: BIM (wordt meegenomen in de Agenda Informatiebeveiliging en van deze lijst gevoerd).

Betrokkenen: SSC (CISO)

Laatste update: december 2021

Planning: Q1.

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. Er is een brede inventarisatie van databronnen gedaan (zie de memo in het DB van 13 september 2021). Op basis van de aanbevelingen wordt gestart met het aanpassen



van processen waarvoor geldt dat er op het gebied van dataminimalisatie nog stappen gezet moeten worden. Op het gebied van statistieken over strafrecht loopt dit proces wat langer en zijn er al acties gestart. Hierbij komt een aantal vragen naar voren met betrekking tot de impact op de onderzoeksmogelijkheden binnen RA-omgeving, extra druk bij databronhouders, communicatie richting databronhouders, impact op beantwoording van ad hoc beleidsvragen e.d. Met CSB-J wordt daarom nader afgestemd over de kaders m.b.t. maximale borging dataminimalisatie. Tegelijkertijd wordt, samen met DRI en de FG, nagedacht over maatregelen om dataminimalisatie structureel beter te borgen. Het verhogen van de awareness onder medewerkers vormt hierbij een belangrijk onderdeel.

Het afstemmen met databronhouders is gecontinueerd. Voor eind 2021 is conform planning met alle dataleveranciers afgestemd. Meest complexe statistiek om de minimalisatie door te voeren zijn de rechtbankstrafzaken. Inhoudelijk onderzoek loopt en voorbereidingen worden getroffen om in 2022 de benodigde aanpassingen door te kunnen voeren.

Actie: In Q4 zijn de resterende gesprekken met bronhouders gevoerd en in Q4-2021 en Q1 2022 gestart met het aanpassen van de bijbehorende productiesystemen. De implementatie/uitwerking vindt in 2022 plaats, daar is ook extra budget voor aangevraagd om dit te realiseren.

Actiehouder: SER

Laatste update: december 2021.

- Status is grotendeels hetzelfde. Nieuw is dat CBK scripts heeft gemaakt om overtollige variabelen direct na binnenkomst van zogenaamde ZBO bestanden met medische informatie te verwijderen. Hiermee is voor de medische data een verdere stap gezet naar dataminimalisatie.

Planning: december 2021, 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. De inhoud van de training is voorbesproken met de CPO/PC's en wordt op maat voor CBS gemaakt.

Het DT SER heeft in december 2021 een beschrijving van de privacy governance binnen SER en haar positionering binnen het CBS vastgesteld. Dit zal periodiek worden geëvalueerd.

Acties: Actualisatie kaders privacy governance.

Planning: eerste actualisatie Q1 2022.

Actiehouder: CSB (CPO en PC)

Betrokkenen: Alle divisies (PC)

Laatste update: november 2021.

Planning: Q1 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.

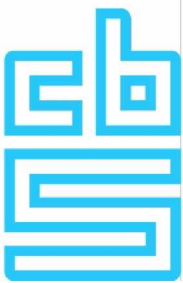
Afgelopen jaar zijn er wat acties gestart voor het vergroten van de interne awareness, zoals de toolkit waarmee CBS-ers in hun output privacybescherming een plek konden geven. Omdat het CBS niet goed, maar excellent wil zijn op het gebied van privacy wordt aanbevolen om de inspanningen op dit gebied onverminderd voort te zetten. In het voorjaar van 2022 zullen awareness sessies binnen de divisies plaatsvinden waarbij de privacy coördinatoren zullen/kunnen ondersteunen/faciliteren.

Acties:

- Blijvende aandacht voor privacy in de output van het CBS;
- Awareness sessies binnen alle divisies.

Actiehouder: CCN en alle divisies

Laatste update: november 2021



Betrokkenen: CPO, PC, BPO

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.

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: november 2021.

Planning: Q1 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: Q1 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: Q1 2022

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:

- Er is door DRI al een overleg gepland om het toekomstige wachtwoordbeleid vorm te geven. Daar zitten o.a. ook de FG's bij.
- Het aandachtspunt wat betreft uitvraag van bijzondere persoonsgegevens (waar al een standpunt over is ingenomen) zal worden ingebracht in het vervolgtraject van actualisering van het inlogbeleid.

In januari is de beleidswerkgroep inlogbeleid bij elkaar gekomen. Voor-ingevulde vragenlijsten met bijzondere persoonsgegevens komen niet voor. Uitvraag bijzondere persoonsgegevens bij lege vragenlijsten is nog een uitzoekpunt.

Actiehouder: DRI

Laatste update: december 2021

Planning: februari 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.

Laatste update: december 2021

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

Vervolg

De volgende rapportage volgt 28 februari 2022.