

aan DB  
van Erik Bruinsma

onderwerp Voortgangsrapportage 2 Agenda Privacy  
datum 22 februari 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): Google analytics.

Google Analytics blijkt volgens de Oostenrijkse toezichthouder niet aan de AVG te voldoen. Ook de Franse gegevenswaakhond CNIL dreigt ermee Google Analytics te verbieden en de AP is een onderzoek gestart en geeft aan dat Google Analytics mogelijk binnenkort niet is toegestaan.

- De privacy coördinatoren hebben een snelle inventarisatie gedaan om te checken in hoeverre een verbod op Google Analytics het CBS raakt. CCN en DRI zijn al bezig om Google Analytics te vervangen door piwik-pro. EBN gebruikt Google Analytics nog wel voor de website Staat van het MKB. Mocht er dus een acute aanleiding zijn om de stekker uit Google Analytics te trekken, dan hebben we een alternatief draaiend, echter nog niet optimaal ingeregeld. CCN kan adviseren en ondersteunen wanneer er overgestapt moet worden op piwik-pro.

**Aandachtspunt:** Wanneer we overgaan op Piwik zetten we de actieve meting van Google uit. Maar we willen wel blijven beschikken over de historische data van de website. We maken nog regelmatig gebruik van data vanaf het begin van de nieuwe website (2016) voor tijdreeksen en trends. Om het reputatie- en boeterisico voor het CBS te mitigeren, moet Google Analytics in principe uiterlijk een week na een relevant AP-besluit of relevante rechterlijke uitspraak worden uitgeschakeld.

#### ➤ 2 (extern): Boetebesluit AP inzake de Toeslagenaffaire

De PO's van het CBS hebben gekeken of er lessen te leren zijn uit het onderzoek dat de AP deed inzake de Toeslagenaffaire. In het kort komen de volgende overtredingen naar voren die ook voor het CBS in het kader van Awareness relevant zijn.

- 1) Al dan niet noodzakelijk zijn van verwerkingen voor de vervulling van de wettelijke (publieke) taak.
- 2) Beginzelen van behoorlijkheid (bijv. discriminatie, profilering), juistheid en transparantie in de praktijk toepassen.
- 3) De vraag of er een minder vergaande vorm van verwerking mogelijk is (proportionaliteit en subsidiariteit).

Het boetebesluit geeft aanzet tot twee concrete actie, namelijk:



- het vergroten van awareness binnen het CBS op voornoemde drie punten in relatie tot alle output gerichte processen van het CBS;
- het waar nog noodzakelijk implementeren van deze drie punten in de output gerichte processen van het CBS

➤ **3 (extern): Privacytoezichthouders onderzoeken gebruik clouddiensten door overheidsinstellingen.**

Privacytoezichthouders in heel Europa starten een onderzoek naar het gebruik van clouddiensten door de landelijke overheden. Op basis van de uitkomsten van dit onderzoek kunnen de toezichthouders achterhalen waar de grootste privacyproblemen zitten bij het gebruik van clouddiensten door overheden.

- Dit heeft geen consequenties voor het CBS. Door het CBS ondersteunde clouddiensten moeten goedgekeurd zijn door BIT. Aan deze diensten is een zorgvuldig traject voorafgegaan waarin o.a. privacy en cloudbeleid (inclusief security) zijn getoetst.
- Ongeautoriseerd gebruik van clouddiensten zijn hier wel een risico.

➤ **4 (intern): Klacht terugleveren respons en advies FG.** 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'.

- **Advies FG:** Maak een duidelijk expliciet beleid over (1) onder welke omstandigheden responsdata teruggeleverd mag worden, en (2) op welke manier dit mag gebeuren.
- CPO zal dit oppakken i.o.m. de betrokken divisie.

## **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**

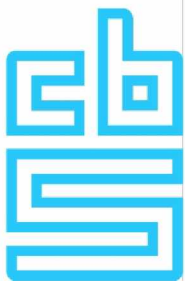
De vier voornaamste verbeterpunten uit de privacy-audit 2020 staan hieronder. Bij de procesmonitor zijn ook de aanbevelingen van de audit 2021 meegenomen.

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 22/2 is er een voortgangsoverleg.

**Actiehouder:** BIM

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

**Laatste update:** januari 2022.

**Planning:** maart nieuwe update.

**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 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.

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:** januari 2022.

**Planning:** CQO moet nog geworven worden. Opschonen procesmonitor is een doorlopend proces.

2. **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:** januari 2022.

**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:** 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:** januari 2022.

**Planning en resultaat:** ter bespreking en vaststelling DB maandag 14 maart.

### **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. Voor de herooverweging wil het CBS 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 kan elk moment het advies publiceren. Daarna kan het CBS het advies meenemen in de eigen herooverweging Zoom.

Relevant is wellicht het advies dat 22 februari is verschenen van Privacy Company, dat een DPIA heeft geschreven over de privacyrisico's van Microsoft Teams, OneDrive en SharePoint. Dit onderzoek was in opdracht van het Ministerie van Justitie en Veiligheid en SURF, de ICT-inkooporganisatie van hogescholen en universiteiten. De uitkomst is dat Microsoft maatregelen heeft getroffen om zes hoge risico's te verhelpen, maar dat organisaties deze clouddiensten niet mogen gebruiken voor de uitwisseling of opslag van gevoelige en bijzondere persoonsgegevens. Dat mag alleen als ze de inhoud kunnen versleutelen met eigen sleutels. Dit komt door het hoge risico van mogelijke toegang tot die gegevens vanuit de Verenigde Staten. Dit risico blijft ook bestaan als Microsoft vanaf volgend jaar vrijwel alle persoonsgegevens van haar Europese zakelijke klanten exclusief in Europese datacentra verwerkt.

**Actie:** Beleidsstuk herooverweging Zoom.

**Actiehouder:** BIM

**Laatste update:** januari 2021.

**Planning:** ter vaststelling DB maart 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.



**Actie:** 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.

**Actiehouder:** SER

**Laatste update:** januari 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 Corporate, CAD en CSB en staat ingepland bij BIM.

**Acties:** Actualisatie kaders privacy governance.

**Planning:** eerste actualisatie Q1 2022.

**Actiehouder:** CSB (CPO en PC)

**Betrokkenen:** Alle divisies (PC)

**Laatste update:** januari 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.
- EBN: De PC voert overleg over de aanpak van de Awareness strategie binnen EBN en heeft gewezen op de mogelijkheid om de CPO en PC een korte presentatie te laten geven in het DT over privacybeleid
- CCN: CCN corporate heeft een presentatie gehad van de CPO over privacy, privacybeleid en de verschillende rollen binnen de privacy governance. CPO en CCN Corporate gaan samen met enkele PC 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 ("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.

**Actiehouder:** CCN en alle divisies

**Laatste update:** januari 2022.





**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:** januari 2022.

**Planning:** maart 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:**

- 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:** januari 2022.

**Planning:** maart volgende update.

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

Alle contracten zijn inmiddels aangepast zijn. Voor lopende contracten geldt wel dat een aanscherping zou moeten komen, echter, de vraag is of een nieuw beleidskader proportioneel is aangezien het nog om slechts 3 landen gaat waarvan het contract afloopt. 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 maart 2022.