

aan DB
van Erik Bruinsma

onderwerp Voortgangsrapportage Q3 Agenda Privacy okt 2023

datum 17 oktober 2023

Inleiding

Per kwartaal 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.

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 (intern): vraag Autoriteit Persoonsgegevens (AP): CBS open data en AI/algoritmen

Donderdag 22 juni was er een bestuurlijk overleg tussen de AP en de DG van het CBS. In dat overleg heeft de AP aan het CBS het volgende gevraagd: delen jullie als CBS de zorgen rondom de toenemende inzet van algoritmen en AI op een wijze die nadelig kan zijn voor betrokkenen? Zo ja, kan het CBS (als grootste leverancier van open data) niet een rol spelen in de samenleving als het gaat om gebruik van open data voor AI en algoritmen? Het CBS heeft aangegeven dat open data voor iedereen beschikbaar is en het CBS geen invloed heeft op het gebruik ervan door andere organisaties. Wel heeft het CBS toegezegd eens na te denken over onze communicatie over het gebruik van onze open data voor AI en algoritmen. De CPO heeft een werkgroep geformeerd met verschillende experts vanuit methodologie en communicatie om hierover na te denken. Daaruit zijn 2 aanbevelingen voor het DB gekomen:

1. het is belangrijk dat er aandacht komt voor gebruik van open data van het CBS door Large Language Models (LLM's) zoals ChatGPT en andere AI gedreven systemen. LLM's zijn niet meer weg te denken uit de huidige samenleving. Gebruik faciliteren en zorgen dat dit soort systemen onze open data weten te vinden heeft de voorkeur boven het beperken en waarschuwen. Ook al is onze open data (nog) niet gemaakt voor dit doel, de kwaliteit is vaak beter dan andere potentiële databronnen van onbekende betrouwbaarheid. Daarom is het volgens de werkgroep belangrijk de informatievoorziening hierover uit te breiden;
2. er is binnen het CBS behoefte aan duidelijk beleid rondom gebruik en toepassing van AI al dan niet met gebruik van CBS open data. Er is binnen het CBS een ChatGPT (LLM) afstemmingsoverleg. Aanbeveling van deze werkgroep is om de vraag voor strategisch beleid op het brede vlak van AI en CBS open data bij deze groep neer te leggen.

➤ 2 (intern): proactief gesprek met de AP over energiedata

Om de effecten van het klimaatbeleid en de energietransitie te kunnen beoordelen is betrouwbare en actuele informatie nodig over de energie die huishoudens en bedrijven verbruiken en de kosten ervan. Het CBS is bezig met de uitvraag van slimme meterdata. Het CBS gaat met de AP in gesprek om dit initiatief toe te lichten. Ook wordt er onderzocht of de AP en het CBS samen kunnen optrekken als het gaat om de samenleving te informeren over dataleveringen voor statistisch gebruik en de rol van het CBS daarin.



- **3 (intern): datalek melding sollicitaties en melding bij AP**
Het CBS heeft een datalek melding gedaan bij de AP in verband met een datalek. Bestanden geüpload door sollicitanten, zoals motivatiebrieven en cv's, worden langer bewaard dan volgens het bewaarbeleid van het CBS mag. Overleg met de leverancier heeft vooralsnog niet tot verbetering geleid, wel tot een patch die het probleem voor nieuwe sollicitanten zou moeten oplossen.
- **4 (extern): adequaatheidsbesluit EU – VS**
De Europese Commissie heeft op 10 juli 2023 een nieuw adequaatheidsbesluit genomen over de gegevensstromen tussen de EU en de VS. Het CBS werd direct benaderd door Stanford University met de vraag of het CBS zijn beleid ten aanzien van toegang tot microdata jegens de VS heeft aangepast. In beginsel is het adequaatheidsbesluit alleen van toepassing op bedrijven die onder toezicht staan van de FTC (federal trade commission) en die zich kunnen registreren op <https://www.dataprivacyframework.gov/>. Universiteiten lijken er niet onder te vallen. Op dit moment is er dus nog geen reden voor herziening van het RA beleid.
- **5 (extern): De AP stelt een onderzoek in naar de Dienst Uitvoering Onderwijs (DUO).**
Aanleiding hiervoor zijn berichten in de media over misstanden bij de fraudecontrole van uitwonende studenten, die discriminerend zou zijn.

3. Strategisch

1. Privacybeleid CBS

- In de auditbevindingen 2022 is geconstateerd dat het (gedocumenteerde) privacybeleid niet jaarlijks door het management wordt geëvalueerd en goedgekeurd. Als actiepunt was vastgesteld dat er een integraal Privacybeleid geschreven wordt voor het CBS.
- Het DB wordt gevraagd het privacybeleid te bespreken en vast te stellen (zie bijlage 1).

2. Awareness

De volgende acties per divisie zijn uitgevoerd:

- **SER:** de eerste ronde awareness sessies bij SER is inmiddels volledig afgerond. Alle teams zijn bezocht door de privacy- en IB-coördinatoren en er heeft een afsluitende sessie met het DT plaatsgevonden. Dat had het karakter van een awareness sessie, maar ook zijn de uitkomsten van de teambijeenkomsten daar besproken. Voor een dergelijke terugkoppeling zijn ook de diverse MT's bezocht. Er wordt nu gewerkt aan een plan voor vervolgbijeenkomsten. Uitgangspunt is om awareness permanente aandacht te blijven geven;
- **DRI:** de waarde stromen van DRI hebben ieder hun specifieke awareness aspecten. Beveiligingsaspecten, datalekprocedure en waar je verder als medewerker op moet letten krijgen aandacht vanuit de checklists die via de hoofden zijn gedeeld met de medewerkers. Bij DRD en bij innovatie DVZ is met name aandacht voor Privacy by Design en het mitigeren van risico's in aanvullende processen via de DPIA. Bij DBD is al enkele jaren veel aandacht voor beveiliging en privacyborging bij beleidsstatistieken en RA. In het primaire waarnemen bij DVZ is dataminimalisatie inherent aan de manier van werken en de vertaling van de informatiebehoefte naar vragenlijsten. Daarnaast zijn de veiligheid van de dataopslag en strakke sturing op wie bij welke data mag bij de secundaire waarneming via up- en downloads belangrijke aandachtspunten. Dit zijn voorbeelden van maatregelen binnen DRI (cf. inventarisatie) waar de awareness vraag al is geland en waar het vooral gaat om borging en continuïteit van de maatregelen;
- **EBN:** de resterende teams binnen EBN worden bezocht voor awareness bijeenkomsten zodat eind 2023 alle EBN teams bezocht zijn. In Q4 wordt verder gekeken naar de opvolging van de aanbevelingen aan de teams die in het eerste halfjaar bezocht zijn;



- **CCN:** via intern Slack kanaal is er op regelmatige momenten aandacht aan privacy besteed;
- **BIM:** binnen BIM verlopen de awareness planning naar verwachting. Voortgang ligt op 65%. Verwachting is dat alle teams binnen BIM in november 2023 hebben deelgenomen.

3. Privacygovernance

De privacygovernance volgens het 3 lines model is nu twee jaar in werking. De meeste directies (op BIM na) hebben ondertussen de governance verder uitgewerkt voor hun eigen divisie. De lijntjes tussen de privacy coördinatoren, de CPO, de juristen en de FG zijn effectief en snel. Ook zijn de privacy coördinatoren goed zichtbaar in de organisatie. Deze zichtbaarheid heeft echter ook geleid tot meer werk en meer verschillende taken. Zo zijn er dubbelrollen in aandachtsgebieden (Privacy, Informatiebeveiliging en Kwaliteit) en is de scheiding tussen uitvoering en advies (eerste en tweede lijn) niet altijd even duidelijk. Nu we twee jaar ervaring hebben opgedaan en we de volgende fase van volwassenheid ingaan is het belangrijk de huidige stand van zaken te analyseren en te evalueren. CSB heeft hiervoor een opdracht geschreven.

Daarnaast hebben de CPO, CQO en de CISO een eerste gezamenlijke coördinatorenendag gehouden op 13 september. Deze bijeenkomst had als doel de onderlinge samenwerking te versterken en te leren van elkaar (het delen van best practices).

Opvolging Privacy audit

4. Implementatie bewaar-en vernietigingstermijnen divisies

Aanbeveling: een omspannende, eenduidige en CBS brede procedure bewaartermijnen dient te worden geïmplementeerd binnen alle directies waarbij verplicht wordt gesteld op eensluidende en eenduidige wijze de uitzonderingen t.a.v. de bewaartermijnen vast te leggen en periodiek te her beoordelen.

- **CBS breed:** er wordt gewerkt aan een opruimdag voor heel CBS. Door dit jaarlijks te doen is er een vast moment dat gegevens vernietigd worden en komt er regulier awareness voor bewaar-en vernietigingstermijnen.
- **SER:** de in 2022 vastgestelde SER-brede notitie rondom bewaartermijnen wordt op dit moment geactualiseerd en zal vervolgens ter vaststelling in het DT SER aangeboden worden. Ook zullen binnenkort de voorbereidingen gestart worden voor de opruimweek begin 2024. Bewaren en vernietigen is verder nadrukkelijk meegenomen in de awarenessbijeenkomsten bij SER. Samen met EBN is een notitie opgesteld waarin een voorstel gedaan wordt voor een CBS-brede werkwijze rond het registreren van uitzonderingen op bewaartermijnen. Deze zal binnen SER in eerste instantie aan de SER Kwaliteitsgroep voorgelegd worden en daarna aan het DT SER.
EBN: voor wat betreft het eenduidig registreren van afwijkingen ten aanzien van de bewaartermijnen wordt samen met SER gekeken waar de monitor bewaartermijnen aanpassing behoeft. Hiervoor is een memo opgesteld die binnen de kwaliteitsgroepen van SER en EBN gedeeld wordt. Vervolgens zal deze aan de afzonderlijke DT's worden voorgelegd. Verder wordt gekeken naar actualisatie van het bestaande bewaartermijnen beleid zijnde de uitvoering van het CBS beleid binnen EBN. Eventuele aanpassingen hierin zullen ter vaststelling aan het DT EBN aangeboden worden.
- **DRI:** er zijn al opruiminitiatieven geweest bij DRI. Bij DVZ worden die actief ingepland. DRI zal kijken hoe verder aangesloten kan worden bij de CBS brede opruimweek en het initiatief van EBN/SER om de noodzakelijke afwijkingen op bewaartermijnen in kaart te brengen en dit overzicht jaarlijks te actualiseren.



- **CCN:** in het laatste kwartaal zijn er op dit vlak binnen CCN geen extra acties geweest, anders dan het reguliere werk en processen op dit vlak.
- **BIM:** BIM ligt achter op planning met een vertaling van het divisiebeleid. Ad-hoc hebben (onder andere naar aanleiding van de privacy awareness sessies) binnen verschillende teams opruimdagen plaatsgevonden. Er vindt een dialoog plaats met de tweede lijn over de doelstelling van het beleid om dit verder te kunnen concretiseren voor BIM. Einddatum is verschoven naar 2023 Q4.

5. FG adviezen

Aanbeveling: de bevindingen van de FG dienen procesmatig en procedureel te worden opgevolgd. In totaal zijn er vier FG adviezen in het DB gebracht waarin aanbevelingen zijn gedaan, drie in april, één in september. Hierbij een terugkoppeling van de opvolging van de adviezen van april.

1. Advies FG over DPIA's

Gevraagde actie DB-leden in april:

a) Breng dit advies en de toekomstige stukken in de eigen divisies actief onder de aandacht. **SER:** de adviezen van de FG worden aangeboden aan en besproken in de SER Kwaliteitsgroep. Ook worden deze toegelicht door de privacy coördinator in het DT en besproken met de hoofddirecteur. Waar mogelijk (en relevant) is ook in de awareness bijeenkomsten aandacht gegeven aan inhoudelijke punten uit de adviezen.

EBN: de adviezen van de FG worden besproken in de werkgroep privacy EBN. Op verzoek van de hoofddirecteur worden deze voorzien van een oplegger binnen de hoofddirectie verspreid.

DRI: daar waar binnen DRI wordt gewerkt aan aanvullende processen (waarneeminnovatie, dataservices en de ondersteuning vanuit DRI binnen de CBS organisatie) zijn betrokkenen bekend met Privacy by Design en worden DPIAs toegepast om risico's te benoemen en te mitigeren. Er zijn inmiddels 9 DPIAs uitgevoerd/ in uitvoering binnen DRI.

CCN: n.v.t.

BIM: de adviezen van de FG worden via de privacycoördinator bij de hoofddirecteur onder de aandacht gebracht. In de doorontwikkeling van het Kwaliteitsmanagementsysteem (KMS) BIM wordt afgewogen of en hoe de FG adviezen geborgd worden in de organisatie.

b) Geef medewerking aan de actualisatie van de nieuwe standaard CBS DPIA door iemand uit de eerste lijn te benoemen die hier namens de hoofddirectie aan bijdraagt.

CSB: in overleg met de FG zal de CPO hiervoor het initiatief nemen en via de PC om input van de organisatie vragen.

c) Hoe gaat elke divisie ervoor zorgen dat de verwachte door externe factoren gestimuleerde 'wildgroei' aan DPIAs gaat worden ingeperkt? Hoe gaat tegelijkertijd worden geborgd dat voor relevante hoog risicoverwerkingen binnen het CBS wel periodiek een DPIA wordt uitgevoerd?

CSB: momenteel wordt er door de CPO een procedure DPIA opgesteld. Dit zal voor de divisies als leidraad dienen.

2. Advies FG over Samenwerkingen

a) Zorg voor overzicht van huidige en toekomstige samenwerkingen en check welke risico's aanwezig zijn en of hier een DPIA voor moet komen;

b) Borg bij langdurige samenwerkingen (> 2jaar) een periodieke herziening.

- **SER:** de FG heeft in een bijeenkomst met de accountmanagers het advies toegelicht. In overleg met de accountmanagers worden ook de CBS algemene voorwaarden geactualiseerd. Een aantal elementen uit het FG advies is hierin meegenomen. Uiteraard kunnen en zullen de privacy coördinatoren adviseren bij het opstellen van overeenkomsten.



- **EBN en DRI:** er dient nog met terugwerkende kracht een risico afweging op bestaande samenwerkingen (waar verwerking van P-gegevens aan de orde is) plaats te vinden. Waar risico's naar voren komen, zal worden vastgesteld of een DPIA aan de orde is om de risico's te mitigeren.
- **CCN:** n.v.t.
- **BIM:** er is geconstateerd dat er binnen BIM geen overzicht is van DPIA's. Er wordt daarom in 2023 Q4 gewerkt aan een inventarisatie om a) een overzicht van DPIA's te krijgen en b) welke samenwerkingen verbetering behoeven.

3. Advies FG over Persoonsgegevens.

Actie DB-leden: verbeter de kennis omtrent persoonsgegevens binnen de eigen divisie o.a. door brede bekendheid en uitleg/toelichting van dit advies.

- **SER en EBN:** tijdens de awarenessbijeenkomsten is nadrukkelijk stilgestaan bij persoonsgegevens en het verbeteren/opfrissen van de kennis hierover.
- **DRI:** dit is onderdeel van de privacy-checklist die is gedeeld. Daarnaast wacht DRI op het beschikbaar komen van de e-learning waar dit aan orde komt en waar medewerkers zullen worden gestimuleerd om jaarlijks hun expertise op te frissen (in de veronderstelling dat dit niet alleen beschikbaar komt binnen het inbound proces).
- **CCN:** n.v.t.
- **BIM:** in de Privacy Awareness sessies is expliciet aandacht voor de definitie van 'persoonsgegevens' en 'verwerken', met daarbij enkele praktische valkuilen die in de bedrijfsvoering kunnen ontstaan.

In september is het advies over dataminimalisatie in het DB vastgesteld. In de volgende privacyagenda zal hierover worden teruggekoppeld.

6. DPIA procedure

Aanbeveling: een eenduidig proces voor de uitvoering, toetsing en goedkeuring van DPIA's dient te worden ingericht.

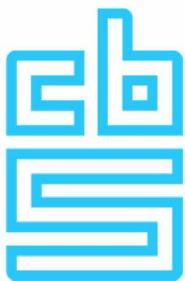
De CPO stelt samen met de PC een procedure DPIA op en neemt daarbij het advies van de FG ter harte. Planning is uitgesteld van Q3 naar Q4 2023. Onderdeel van de DPIA procedure is een quickscan. Deze wordt tegelijkertijd opgesteld door de CPO en de PC SER.

- De PC van SER en DRI hebben samen met de CPO een start gemaakt voor een standaard DPIA sjabloon.
- CSB heeft een cursus DPIA schrijven gegeven van 2 dagdelen in september. 15 personen hebben deelgenomen aan de cursus (1 BIM, 1 CSB, 5 DRI, 5 EBN en 3 SER). Er was hier veel animo voor dus er is nog een wachtlijst. De cursus zal via de CBS Academy structureel aangeboden worden.

7. Verbeterregister

Aanbeveling: Een eenduidig proces dient te worden ingericht om bijzonderheden uit zelfevaluaties, interne- en externe audits en interne controles op te volgen.

- **CSB:** CPO heeft samen met de CQO en de CISO een CBS-breed verbeterregister opgesteld. Deze wordt voor de privacy verbeterpunten per kwartaal bijgewerkt, tegelijkertijd met de Privacyagenda.
- **CCN** heeft een verbeterbacklog aangemaakt voor CCN. Hierin staan nu alle verbeterinitiatieven op één plaats samen voor het overzicht. Op het gebied van privacy staat er bij CCN niets meer open op dit moment.
- **SER:** vanuit SER wordt het CBS-brede verbeterregister gevuld en gemonitord. De verbeterpunten worden onder meer besproken in de SER directiebeoordelingen. Daarnaast onderhoudt SER zelf een dashboard met verbeterpunten.



- **EBN:** maakt gebruik van het centrale verbeterregister en geeft daar periodieke terugkoppeling over aan het DT. Dit komt ook terug in de Q-rapportages.
- **DRI:** vult en monitort haar verbeterpunten ook in het centrale verbeterregister. Dat dient als uitgangspunt voor de voortgangsinformatie over verbeterpunten in de kwartaalrapportage van DRI.
- **BIM:** sinds augustus 2023 vinden er binnen BIM maandelijks geplande KMS bila's plaats tussen de privacycoördinator (tevens kwaliteits- en ib-coördinator) en de sectordirecteuren en hoofd directeur. Vast agendapunt is onder anderen respectievelijk het bespreken van de voortgang van openstaande (audit)bevindingen in het centraal verbeterregister (CVA) en terugkoppeling over deze voortgang met de mogelijkheid tot escalatie.

8. Directiebeoordeling

Aanbeveling: de periodieke beoordeling van de operationele effectiviteit van privacymaatregelen dient te worden verbeterd.

- De CPO heeft de CQO ondersteund bij het opstellen van het framework directiebeoordelingen voor het privacygedeelte.
- De directiebeoordelingen zijn afgerond.

9. CBS-brede risicoanalyses

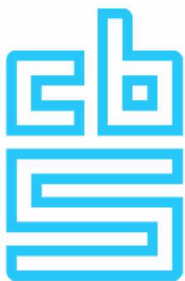
Aanbeveling: de risicoanalyse(methodiek) dient te worden aangepast aan best practices zoals (bijvoorbeeld) de ISO 31000 (Risicomanagement - principes en richtlijnen).

- Vanuit de AVG is een DPIA de tool om een risicoanalyse uit te voeren en de risico's te mitigeren. Het proces hiervoor wordt in Q4 uitgewerkt.

4. Overzicht Actiepunten

Hieronder een overzicht over de stand van zaken rondom de actiepunten op de Privacy Agenda.

	Actie en status	Planning	Actie houder
1	E-learning module Awareness IB en cursus privacybescherming. De E-learning is bijna gereed voor gebruik. CCN heeft samen met de CPO een opzet voor een introductiefilmpje privacybescherming gemaakt. Deze is medio november gereed. Vanaf januari kan de introductiecursus voor nieuwe medewerkers meegenomen worden in de Academy.	Q4 2023	BIM voor E-learning CSB voor introductiecursus privacy nieuwe medewerkers
2	CBS- breed beleid opstellen ten aanzien van bestaande medewerkers, stagiaires en trainees bij het CBS gedurende de diensttijd ten aanzien van IB en privacy, en niet alleen bij indiensttreding. Dit punt is op verzoek van de DG op de privacy Agenda gezet. Dit beleid wordt verder vormgegeven door de beveiligingscoördinator en de CISO en wordt van deze actielijst gehaald.	Start Q4 2023	CSB
3	VerPRINnen In bijlage 2 informeert de stuurgroep verPRINnen over de voortgang van het project.	Lopend	SER



4	Beleidskader terugleveren responsdata bedrijven Maak een duidelijk expliciet beleid over (1) onder welke omstandigheden responsdata teruggeleverd mag worden, en (2) op welke manier dit mag gebeuren. Met DVZ is hierover overleg gevoerd. Concept beleidskader wordt voorgelegd aan de teams van SER en EBN die verantwoordelijk zijn voor het relatiebeheer bedrijven. Ondertussen ook gesproken met teams binnen EBN en de collega's voor de bedrijvenportals voor oplossingen in huidige knelpunten.	Q4 2023	CSB
5	CBS-breed pseudonimiseerbeleid (middellange termijn) Om het veiligheidsniveau op de middellange termijn te verhogen worden verschillende actielijnen uitgezet om verPRINnen nader te onderzoeken. Eén van de actielijnen is het formuleren van een CBS-breed pseudonimiseerbeleid.	Start Q4 2023	CSB
6	Beleid omtrent productiedata op niet productie omgeving. EZK heeft hiervoor een concept beleidsstuk geschreven. De CPO zal voor het CBS beleid kijken of we hierop kunnen aansluiten.	Start Q4 2023	CSB
7	Actualiseren crisismanagementplan en organiseren van een crisisoefening. Er is per 1 april een crisiscoördinator aangesteld. Het datalek van Nebu heeft het CBS laten inzien dat er een crisismanagementplan moet komen voor een CBS datalek met grote gevolgen.	Start Q4 2023	CSB
8	Update CBS DPIA	Start Q1 2024	CSB

Vervolg

De volgende rapportage is januari-februari 2024