



aan DB
van Erik Bruinsma

onderwerp Voortgangsrapportage Q2 Agenda Privacy jul 2023
datum 4 juli 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): implementatie privacyvriendelijk alternatief tracking cookies van reCAPTCHA**
 - Google reCAPTCHA bij formulieren (bewijs dat u geen robot bent) plaatst tracking cookies. Dit is gemeld in de Privacyagenda van Q1 2023. Ondertussen is voortgang geboekt doordat het selectietraject voor een privacyvriendelijke tool is afgerond en goedgekeurd.
- **2 (extern): datalek bij softwareleverancier Nebu (meer dan 150 organisaties geraakt)**
 - Dit is ter kennisgeving ingebracht in het DB van 18 april, de inventarisatie was toen nog niet afgerond. Inmiddels is bekend dat het CBS geen samenwerkingen had met Nebu of één van de marktonderzoeksbureaus die met Nebu samenwerkte. Deze inventarisatie kostte relatief veel tijd. Gekeken wordt of met het verbetertraject inkoop deze inventarisatie geautomatiseerd zou kunnen in de toekomst.
 - Leerpunt vanuit TNO: ze hebben gezien hoe belangrijk het goed regelen van bewaartermijnen is. Bij de ene verwerker was dat bij hen wel goed geregeld waardoor er veel minder data gelekt was (laatste 3 maanden) dan bij een ander onderzoek waar data tot 2021 gelekt was.
- **3 (extern): regulier jaaroverleg DG-AP**
 - Op 22 juni heeft Angelique gesproken met Monique Verdier (vicevoorzitter AP). Het was een open en constructief gesprek over gemeenschappelijke zorgen.
 - Belangrijk punt is de implementatie 'open data richtlijn'. De AP heeft zorgen om het conceptvoorstel waarin overheidsinstanties zoveel mogelijk datasets moeten publiceren en zelf moet zorgen voor anonimisering. Zij zien het CBS graag betrokken in deze discussie omdat wij hierin experts zijn.
 - De AP maakt zich zorgen om gebruik algoritmes voor besluitvoering en vraagt het CBS hoe wij kunnen bijdragen aan verantwoord gebruik van onze openbare datasets bij algoritmes.
- **3 (extern): AP vraagt om inventarisatie openbare registers.**
 - Op 28 maart stuurde de voorzitter van de AP een brief aan de Staatssecretaris Koninkrijksrelaties en Digitalisering met het verzoek een inventarisatie te maken van alle openbare registers. Achtergrond van dit verzoek is dat het Hof van Justitie van de Europese Unie een uitspraak heeft gepubliceerd ten aanzien van het UBO-register. Hierin staat dat de openbaarmaking aan het algemene publiek van de persoonsgegevens uit het UBO-



register onrechtmatig is. De AP geeft aan dat deze uitspraak zou moeten leiden tot een herbeoordeling op wetgeving en praktijk bij alle "openbare registers" die in Nederland door de wetgever zijn ingesteld en die persoonsgegevens bevatten.

- Het CBS heeft EZK laten weten dat het CBS geen, voor het publiek toegankelijke, bij wet in het leven geroepen, registers/archieven die persoonsgegevens bevatten beheert.

B. Strategisch

1. Privacybeleid CBS

In de auditbevindingen 2022 is geconstateerd dat het (gedocumenteerde) privacybeleid niet jaarlijks door het management wordt geëvalueerd en goedgekeurd. Als actiepunten was vastgesteld dat er een integraal Privacybeleid geschreven wordt voor het CBS.

- Er is een concept Privacybeleid geschreven waarin ook Privacy by Design en risicomanagement in meegenomen is. Ook het beleidsstuk Privacygovernance wordt hierin geïntegreerd. De komende maanden wordt dit beleidsstuk afgerond in samenspraak met de divisies.
- Er is een concept Privacy by Design beleidsstuk geschreven dat geïntegreerd wordt in het privacybeleid. Ook is hiervoor door CCN een praatplaat ontworpen. Deze is als bijlage 1 ter bespreking toegevoegd en wordt momenteel op verzoek al gedeeld binnen het CBS.

2. Awareness

Privacy is toegevoegd aan de CBS brede awareness enquête Informatiebeveiliging en Privacybescherming dat 25 mei is uitgezet. Deze enquête werd al jaarlijks gehouden voor Informatiebeveiliging. Vanaf dit jaar loopt Privacy als thema hierin mee. Voor het eerst zijn er 2 vragenlijstexperts van DVZ aangeschoven die meegekeken hebben met de vragenlijst. Zij zullen volgend jaar een grotere rol spelen in de ontwikkeling van de vragenlijst met als uiteindelijk doel om de gehele vragenlijst jaarlijks door het CBS te laten verzorgen.

Verder is op 25 mei (5 jaar AVG) een CBS brede awareness actie gehouden waarbij iedere medewerker een datablocker kreeg. Ook zijn er eind mei en begin juni privacy/IB awareness-bijeenkomsten gehouden voor de managementassistenten. Deze sessies waren CBS-breed en de CPO en privacy coördinatoren van alle hoofddivisies waren hierbij betrokken.

Verder zijn de volgende acties per divisie uitgevoerd:

- **SER:** vervolg gegeven aan de privacy- en IB-awareness bijeenkomsten. De SER-privacycoördinatoren hebben na afloop van Q2 2023 alle teams bezocht, inclusief een virtuele meeting met de collega's in Caribisch Nederland. De bijeenkomsten zijn goed bezocht en leiden daadwerkelijk tot meer awareness (toename aantal vragen en aantal meldingen van (potentiële) datalekken/incidenten). Nadat alle teams van een sector bezocht zijn, vindt met het MT van de sector MT een reflectie plaats op de bijeenkomst waarbij wordt teruggeblikt en de voornaamste uitkomsten/vervolgacties besproken worden.
Maandelijks is er een overleg tussen de hoofddirecteur en de privacy coördinatoren. Elk kwartaal bezoeken de SER privacy coördinatoren het DT SER om daar in gesprek te gaan over de actuele stand van zaken.
- **DRI:** er zijn awareness sessies binnen DRI met teamhoofden. Focus ligt op continu aandacht (effect op veel aspecten) en de toepassing van procedures (privacy by design, datalekken, contracten). Ook is er veel aandacht voor de vraag wanneer je als teamhoofd in control bent. Hiervoor wordt de checklist (zie punt 4) van de CPO ter ondersteuning gebruikt. Het lijnmanagement draagt awareness uit aan de medewerkers via het werkoverleg.
- **CCN:** er wordt bijgedragen aan awareness door regelmatig communicatieve uitingen op het interne Slack kanaal van CCN te plaatsen.



- **BIM:** er zijn awareness sessies ingepland voor de teams binnen BIM. Separaat is een aparte awareness sessie ingepland voor directeuren/managers.
- **EBN:** awareness sessies hebben een vervolg gekregen binnen EBN. De sectoren EBD en ERB zijn allemaal bezocht. Met de overige sectoren is ook gestart. Eind 2023 zijn alle sectoren bezocht.

Binnen EBN gaat de privacy coördinator verder in gesprek over de actuele stand van zaken op het gebied van privacy in een maandelijks overleg met de werkgroep privacy EBN. Daarin hebben alle sectoren een afgevaardigde. Ook maandelijks is er overleg tussen de privacycoördinator en de directeur ERB als betrokken DT-lid voor privacy.

3. Privacygovernance

De privacygovernance wordt steeds meer volwassen. De privacy coördinatoren zijn goed zichtbaar in de organisatie, mede dankzij de awareness bijeenkomsten. Tweewekelijks vindt overleg plaats tussen de PC en de CPO, maandelijks tevens met de FG. De lijntjes zijn kort. De privacygovernance is voor alle divisies ook uitgewerkt en vastgesteld in DT's. Alleen voor BIM moet dit nog gebeuren, planning is in de zomer.

Opvolging Privacy audit

4. Checklist 'manager in control'

Tijdens de bespreking van de Privacyagenda van Q1 2023 heeft het DB aangegeven dat de rapportage van de externe Privacy audit lastig leesbaar is. Er is gevraagd of dat niet op een andere wijze gerapporteerd kan worden. Vanuit de organisatie is ook feedback ontvangen via de PC en de CPO over de voorbereiding op de audits.

De rapportage van de externe auditor gaat volgens het Privacy Control Framework van NOREA. De rapportagevorm is hierbij aan strikte eisen gehouden en kan daarom niet aangepast worden. Om managers te ondersteunen in de privacycompliance heeft de CPO een korte checklist opgesteld, gebaseerd op hetzelfde framework en dezelfde terminologie als het Privacy Control Framework van NOREA. Deze checklist kan gebruikt worden bij directiebeoordelingen, Q-rapportages en voorbereidingen op externe audits. Managers kunnen de checklist gebruiken als hulpmiddel om te zien met welke aspecten hun team/sector/divisie te maken heeft en of dat aantoonbaar nageleefd wordt. De checklist is via de PC op te vragen en wordt momenteel experimenteel getest. Ook is er een vergelijkbare checklist voor medewerkers gemaakt (zie bijlage 2 en 3).

5. 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.

- **SER:** Momenteel wordt binnen SER gezien of de in 2022 vastgestelde SER-brede notitie rondom bewaartermijnen aangepast dient te worden. De notitie is vorig jaar vastgesteld en divisiebreed verspreid. Ook is deze nadrukkelijk onder de aandacht gebracht tijdens een divisiebrede digitale opruimweek die in het vroege voorjaar plaatsvond. Met verwijzing naar deze notitie konden veel vragen rondom bewaren en vernietigen op uniforme wijze beantwoord worden.
- **DRI:** bewaar- en vernietigingstermijnen zijn binnen DRI ingeregeld per waarde stroom, met periodieke toets vanuit procescoördinatie en audits en bijsturing indien bevindingen hierom vragen.



- **CCN:** is er verder gewerkt aan de optimalisatie van Piwikpro, ook is gekeken hoe de tijdreeks van Google Analytics voor een aantal jaren opgeslagen kan worden voor eventueel tijdreeks onderzoek, daarbij is tevens gekeken en geborgd dat er jaarlijks ook een jaar (oudste) wordt opgeruimd.
- **EBN:** tijdens de awareness sessies wordt nadrukkelijk aandacht besteed aan het naleven van het bewaartermijnenbeleid. Bekeken wordt waar de EBN-brede voorschriften ten aanzien van bewaartermijnen aangepast en verbeterd kunnen worden. Samen met SER wordt verder gekeken waar de monitor bewaartermijnen aanpassing behoeft.
- **BIM:** het opstellen en implementeren van het bewaar-en vernietigingsbeleid binnen BIM is ingepland in de zomer.

6. FG adviezen

Aanbeveling: de bevindingen van de FG dienen procesmatig en procedureel te worden opgevolgd.

- De FG adviezen werden voorheen aan de DG aangeboden en gepubliceerd op de intranetsite van het CBS. Afgesproken is nu dat alle FG adviezen standaard aan het DB worden aangeboden door CSB. DB leden zijn verantwoordelijk voor verdere opvolging van de FG adviezen. In de privacy agenda zal de opvolging gemonitord worden.
- De FG adviezen van Q4 2022 en Q1 2023 zijn op 18 april gebundeld aangeboden aan het DB. De DB leden hebben de behoefte geuit om de adviezen verder te bespreken met de FG.
- Er zijn gesprekken geweest met de hoofddirecteur BIM, SER, EBN en een afspraak met DT DRI is ingepland in juli. De FG heeft met de accountmanagers gesproken over zijn advies over gezamenlijke verwerkingsverantwoordelijkheid.
- DT's moeten zelf de acties voor opvolging verder vormgeven.

7. 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 Q3 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.
- Privacycoördinatoren begeleiden en adviseren in de eerste lijn bij DPIA's. Zij betrekken, indien nodig, de CPO en FG. Op dit moment lopen er DPIA's voor datadonatie en OSSC-ODISSEI (DRI). Ook wordt er een start gemaakt met de DPIA voor het vernieuwde ABR

8. Verbeterregister

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

- 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

9. Directiebeoordeling

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



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

10. CBS-brede risicoanalyses

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

- In overleg met de CISO is besloten aan te sluiten op de risicoanalyse zoals voor de audit ISO 27001 wordt uitgewerkt. Dit is in Q2 afgerond en vastgesteld door het DB. Aanvullend heeft de CPO in het Privacybeleid het risicomanagement voor specifiek privacyrisico's beschreven.
- 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 de zomer uitgewerkt.

C. Overzicht Actiepunten

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

	Actie en status	Planning	Actie houder
1	Jaarlijkse IB en privacy enquête Jaarlijks wordt door SSC een Informatiebeveiligingsenquête opgezet vanuit Secura om kennis en awareness te monitoren. Dit jaar zal Privacy voor het eerst aanhaken. Ook zijn vragenlijstexperts vanuit DRI gevraagd hun expertise hiervoor in te zetten dit jaar om na de evaluatie te kijken in hoeverre deze uitvraag door het CBS zelf georganiseerd zou kunnen worden.	Afgerond, evaluatie ingepland.	BIM
2	Proces beschrijven FG adviezen en opvolging	Proces beschreven, nu van start met de opvolging.	CSB proces, de divisies implementatie
3	E-learning module Awareness IB 2.0. vernieuwen en aansluiten privacybescherming. BPO heeft dit samen met SSC opgepakt, in november ook input van CPO en FG in deze module. Afgesproken is dat privacy in een aparte fysieke sessie voor nieuwe medewerkers wordt aangeboden.	Q3	BIM voor E-learning CSB voor privacysessie
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.	Q3	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.	2 ^e helft 2023	CSB
6	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	2 ^e helft 2023	CSB



	indiensttreding. Dit punt is op verzoek van de DG op de privacy Agenda gezet.		
7	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.	2 ^e helft 2023	CSB
8	Implementatie opvolging FG adviezen per divisie De gesprekken met de FG zijn gevoerd of ingepland. Het is aan de divisies zelf dit op te pakken en hiervan een terugkoppeling te geven in de Privacyagenda.	Q3 2023	CSB proces, divisies implementatie
9	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.	2 ^e helft 2023	CSB
10	VerPRINnen Medio april is 5.1.2.e als projectleider beschikbaar gekomen voor het project verPRINnen. Hij is gestart met het zich verdiepen in het onderwerp van het project. Hiervoor heeft hij inmiddels vele gesprekken gevoerd met diverse CBS medewerkers waaronder de leden van het kernteam van het vorige project. Er is een stuurgroep voor dit project samengesteld met een brede afvaardiging uit de verschillende onderdelen van het CBS die zullen participeren in het project. Deze stuurgroep zal medio juni voor de eerste keer bij elkaar komen. Verder is, met BIT medewerkers in de trekkende rol, gestart met het uitvoeren van een marktverkenning.	Gestart	SER
11	Update CBS DPIA	2 ^e helft 2023	CSB

Vervolg

De volgende rapportage is dinsdag 3 oktober 2023.