

aan DB
van Erik Bruinsma

onderwerp Voortgangsrapportage Q1 Agenda Privacy mrt 2023

datum 7 maart 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

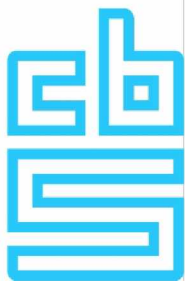
Dit gedeelte geeft een vooruitblik over komende wetgeving, maatschappelijk ontwikkelingen of interne vragen die mogelijk impact kunnen hebben op het Privacybeleid van het CBS. Het DB kan proactief acties verbinden aan deze ontwikkelingen indien zij dit nodig achten.

- **1 (intern): Het CBS maakt gebruik van tracking cookies (reCAPTCHA) en is daarmee niet compliant.**
 - Het gebruik van reCAPTCHA is in 2018 na een aanval via webformulieren snel ingevoerd om de informatiebeveiliging te waarborgen.
 - reCaptcha is een dienst aangeboden door Google, waarbij communicatie naar de servers van google.com nodig is, waarbij een gebruiker een vinkje zet op een pagina om aan te tonen dat hij een echte gebruiker is, en geen script.
 - Momenteel worden privacy vriendelijkere tools onderzocht, wordt de verklaring op de site aangepast en gekeken welke acties er nog meer moeten komen om te voldoen aan alle wet-en regelgeving.
- **2 (extern): De Portugese Autoriteit Persoonsgegevens heeft het Portugese nationale statistiekbureau een boete opgelegd van 4,3 miljoen euro voor gebruik cloud.**
 - Voor de volkstelling werd gebruik gemaakt van de CDN service (Content Delivery Network) van een Amerikaanse clouddienst (cloudflare). De 5 bevindingen die tot deze boete leidden waren: 1) respondenten werden niet geïnformeerd dat bijzondere gegevens optioneel beantwoord mochten worden; 2) ontbreken transparantie in gebruik van deze clouddienst; 3) een DPIA die niet het gehele proces omvatte; 4) onzorgvuldig proces in de keuze voor een verwerker; 5) een data transfer naar de Verenigde Staten zonder aanvullende maatregelen, bijvoorbeeld omtrent subverwerkers.
- **3 (extern): de EC zal in het 2^e kwartaal een wetsvoorstel indienen om de samenwerking tussen nationale gegevensbeschermingsautoriteiten te stroomlijnen bij handhaving van de AVG bij grensoverschrijdende gevallen.**
 - Denk hierbij aan Big Tech bedrijven zoals Meta, Google, Apple (Ierland) en Amazon (Luxemburg). Dit heeft niet direct een gevolg voor Nederland of voor het CBS.
- **3 (extern): Het kabinet gaat de keuze om commerciële cloudaanbieders bij de rijksoverheid toe te staan heroverwegen en een Europees cloudalternatief kiezen.**

B. Strategisch

1. Opvolging Privacy audit (CSB)

De privacy audit 2022 is afgerond. In de memo (bijlage 1) staan de bevindingen, de planning en de acties en actiehouders. Risicomanagement werd vorig jaar ook als verbeterpunt genoemd.



Vanuit privacy zal aangesloten worden op wat er vanuit IB momenteel wordt ontwikkeld. Ook het onderwerp bewaartermijnen kwam vorig jaar aan bod, destijds nadruk op eenduidigheid van het beleid, dit jaar op de implementatie en naleving van dit beleid.

2. BSN reductie: monitoring en verantwoording (CSB)

In Q4 van 2022 is de eerste structurele uitvraag onder alle divisies gedaan (m.u.v. CCN) naar de hoeveelheid BSN-toegangen. De uitvraag is op een eenduidige manier vormgegeven waarbij alle divisies ook een verantwoording hebben gegeven over de voortgang van de verbetertrajecten die in het voorjaar van 2022 aan het DB zijn aangeleverd. Zie hiervoor Bijlage 2. Door harmonisatie van de uitvraag (toegangen tellen in plaats van personen) en de uitgebreide verbetertrajecten zijn er begin 2022 nog meer BSN-toegangen aan het licht gekomen. Deze verantwoording zal op dezelfde wijze jaarlijks aan het DB worden aangeboden.

3. Werkprogramma 2023

Het werkprogramma van 2022 is geëvalueerd. Waar de focus vorig jaar lag op de governance en awareness heeft het privacyteam dit jaar een uitgebreider werkprogramma met planning opgesteld (zie bijlage 3). De focus dit jaar ligt op de verdere uitwerking van beleidsstukken, adviezen en informatie om de organisatie te ondersteunen in de verantwoording van het privacybeleid.

4. Evaluatie datalekregister 2022

De procedure datalekken is in 2022 vereenvoudigd en in awareness sessies is aandacht besteedt aan het belang van het melden van een datalek. Hierdoor zijn er in 2022 fors meer datalekken gemeld. Een belangrijk doel van het datalekregister is dat een organisatie leert van eerdere datalekken en maatregelen neemt om de kans op nieuwe datalekken te verminderen. In deze evaluatie zijn aanbevelingen gedaan (zie bijlage 4).

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	Privacy governance en awareness (PDCA) - Nieuw werkprogramma gemaakt.	Afgerond	CSB
2	Evaluatie datalekken 2022 De evaluatie is afgerond, de voorgestelde acties uit de evaluatie worden na vaststelling DB aan deze actielijst toegevoegd.	Afgerond	CSB
3	VerPRINnen Advies stuurgroep is 31 januari in het DB geweest. Traject verPRINnen gaat de volgende fase in. Deze actie wordt afgevoerd van de lijst.	Afgerond	CTB
4	Wachtwoordbeleid respondenten niet compliant Advies beleidswerkgroep is in DB goedgekeurd. Traject gebruik DigiD voor het authenticatieproces rondom inloggen voor CBS enquêtes is gestart.	Afgerond	DRI
5	Actualiseren crisismanagementplan en organiseren van een crisisoefening.	Afgerond	CSB



	Nota van de Werkgroep Business Continuity Management is in december door het DB vastgesteld. Er wordt geworven voor een crisis coördinator.		
6	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.	Q2	BIM voor E-learning CSB voor privacy sessie
	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
	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.	Q2	BIM
8	CBS-breed pseudonimiseerbeleid (middellange termijn) Om het veiligheidsniveau op de middellange termijn te verhogen worden verschillende actielijnen uitgezet om verPRINnen nader te onderzoeken. Een andere actielijn is het formuleren van een CBS-breed pseudonimiseerbeleid.	2 ^e helft 2023	CSB
9	Proces beschrijven FG adviezen en opvolging	Q2-Q3	CSB
10	CBS- breed beleid opstellen ten aanzien van 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.	2 ^e helft 2023	CSB
11	Beleid omtrent productiedata op niet productie omgeving		

Vervolg

De volgende rapportage is dinsdag 30 mei 2023.