

aan DB  
van Erik Bruinsma

onderwerp Voortgangsrapportage Q1 Privacyagenda mei 2024

datum 14 mei 2024

## Inleiding

De CPO rapporteert over de voortgang van de Privacyagenda. 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 (extern): de Rijksinspectie Digitale Infrastructuur (RDI, voorheen Agentschap Telecom) heeft op maandag 18 maart het definitieve besluit gepubliceerd omtrent gebruik telefoniedata door Odido (voorheen T-Mobile). Conclusies:**
  - telefoniedata mag onder de telecommunicatiewet niet gebruikt worden voor statistische doeleinden tenzij het volledig geanonimiseerd is wat in dit geval niet zo was.
  - de boete is wel flink verlaagd, van 375 duizend naar 175 duizend. De conclusie was dat de boete lager kon door de volgende verzachtende omstandigheden. De RDI benoemt specifiek de uitgebreide technische en organisatorische maatregelen die Odido had getroffen om veiligheid en privacy te garanderen en het feit dat er geen mogelijkheid was de gegevens te herleiden naar individuen door het CBS. Bovendien concludeert de RDI dat uit het onderzoek niet is gebleken dat de overtreding heeft geleid tot ernstige gevolgen of geëffectueerde risico's.
- **2 (extern): Autoriteit Persoonsgegevens (AP) heeft aangegeven dat ze komend jaar strenger gaan controleren op cookiebanners, met name van overheden.**
  - De FG heeft hier eerder naar gekeken en het CBS plaatst geen trackingcookies maar wel functionele cookies en cookies voor analyse en onderzoek. CCN zal de cookiepagina updaten met duidelijke informatie voor de gebruiker.
  - Alle CBS websites horen een cookieverklaring te hebben. Eigenaarschap is verspreid. CCN heeft aangeboden een coördinerende rol te spelen in het laten updaten van alle CBS websites. Aan het lijnmanagement wordt gevraagd hier medewerking aan te verlenen.
- **3 (extern): Autoriteit Persoonsgegevens (AP) heeft een advies aan BZK gegeven over het gebruik van Facebook door de overheid.**
  - Het advies van de AP aan BZK is dat overheidsorganisaties Facebook maar beter niet kunnen gebruiken als onduidelijk is wat er met de persoonsgegevens van bezoekers van hun Facebookpagina gebeurt.
  - Vanuit EZK is er een heel duidelijk advies om te wachten met actie totdat BZK en Meta klaar zijn met de onderhandelingen.



➤ **4 (intern): eerste pilot CBS brede opruimweek**

Van 29 januari tot en met 2 februari vond een eerste pilot CBS brede opruimweek plaats. Deze wordt momenteel geëvalueerd en voor de zomer zal gestart worden met een plan van aanpak voor een structureel jaarlijks digitaal opruimmoment. Naar aanleiding van de wereldwijde 'Digital Cleanup Day' heeft CCN een [terugblik](#) op intranet geplaatst.

## **B. Strategisch**

### **1. Opvolging Privacy audit**

Op donderdag 22 februari is het Corrective Action Plan (CAP) voor opvolging van de verbeterpunten uit de privacyaudit goedgekeurd door Duijnborgh. De bewijsstukken dienen vóór 1 augustus aangeleverd te worden aan de interne auditdienst ter beoordeling, voordat het naar Duijnborgh gestuurd wordt voor de volgende externe auditbeoordeling. De acties komend jaar zijn verdeeld over 4 onderwerpen.

#### **Ad.1. Opvolging en verantwoording verbeteracties door DT's.**

- In 2023 is via de Privacyagenda verantwoording afgelegd over de voortgang van de verbeteracties. Inmiddels is er een centraal verbeterregister voor alle verbeteracties uit interne en externe audits voor zowel Kwaliteit, Informatiebeveiliging en Privacy.
- In 2024 is er een nieuw format Q-rapportage aangeboden aan het DB. Hierin is ruimte voor directie-specifieke terugkoppeling audit punten en directiebeoordelingen.
- Vanuit privacy willen we zoveel mogelijk aansluiten bij bestaande processen en dubbele rapportages voorkomen. Daarom stellen we voor om middels de Q-rapportages de voortgang van verbeteracties te rapporteren aan het DB in plaats van via de Privacyagenda.

**Vraag aan DB:** gaat het DB akkoord met het voorstel om verantwoording van de verbeteracties uit de Privacyagenda te halen en bij te houden in het verbeterregister met een terugkoppeling via de Q-rapportages?

#### **Ad.2. Opvolging en verantwoording privacyrisico's**

- In 2023 is door IB een risicoregister opgezet met daarbij ook een procedure. Hierin is Privacy niet meegenomen. De externe auditoren adviseren hierin de privacyrisico's ook te borgen.
- De privacyrisico's zijn apart in DPIA's behandeld en brede CBS risico's worden in de privacyagenda terug gekoppeld. Wel geldt voor alle niveaus dat IB en Privacy vaak als twee aparte trajecten worden beschouwd en dat is op zichzelf een risico. In DPIA's is wel standaard aandacht voor IB risico's. In het risicoregister van IB nog niet voor Privacy.
- Het huidige IB risicoregister is niet direct toepasbaar voor privacyrisico's.
- Er wordt voor privacyrisico's een apart register opgezet met een duidelijke procedure. Deze procedure bestaat uit een risicoprocedure en een DPIA procedure. Het register zal zoveel mogelijk aansluiten bij het risicoregister.
- Vanuit privacy willen we zoveel mogelijk aansluiten bij bestaande processen en dubbele rapportages voorkomen. Daarom stellen we voor om middels de Q-rapportages de voortgang van privacyrisico's te rapporteren aan het DB in plaats van via de Privacyagenda.

**Vraag aan DB:** gaat het DB akkoord met het voorstel om verantwoording opvolging privacyrisico's uit de Privacyagenda te halen en bij te houden in het risicoregister met een terugkoppeling via de Q-rapportages?

#### **Ad.3. Formaliseren procedure rondom de uitvoering, toetsing en goedkeuring van DPIA's.**

- In 2023 is een start gemaakt met het DPIA proces. De CPO zal de procedure en de sjablonen in juni ter vaststelling aanbieden aan het DB.



#### **Ad.4. E-learning voor nieuwe medewerkers**

- Privacybescherming vormt nu een onderdeel van de onboarding.
- CCN heeft een introductiefilmpje gemaakt voor nieuwe CBS medewerkers.
- In 2024 zal er een E-learning Privacybescherming opgezet worden.

## **2. FG Adviezen**

De FG adviezen zijn onderverdeeld in 4 categorieën. Opvolging en verantwoording gebeurde in 2023 via de Privacyagenda. Zoals eerder genoemd willen we vanuit privacy zoveel mogelijk aansluiten bij bestaande processen en dubbele rapportages voorkomen. Per categorie wordt aan het DB gevraagd akkoord te gaan met het voorstel voor de opvolging en verantwoording aan het DB.

- Adviezen aan de DG: deze worden aan het DB ter bespreking aangeboden. De acties die hieruit voortkomen worden opgenomen in het privacy risicoregister. Terugkoppeling gebeurt via de Q-rapportages in plaats van via de privacyagenda.
- Adviezen in FG paragrafen: in het DB van 20 februari is vastgesteld dat voor FG adviezen in de FG paragraaf bespreking in het DB en het vastleggen van opvolging in het DB verslag voldoende borging is.
- Adviezen op DPIA's: deze adviezen worden lokaal opgeslagen bij de procesdocumentatie. DPIA's zelf worden indien nodig opgenomen in het risicoregister. In juni volgt een uitgebreide procedure ter vaststelling.
- Decentrale adviezen (gegeven aan een lijnmanager op een niveau onder de DG): deze adviezen worden door de directies zelf geborgd. Terugkoppeling vindt alleen plaats wanneer het CBS breed relevant is via de Q-rapportages.

## **3. Jaarplanning**

De volgende acties staan op de agenda voor 2024:

- digitale opruimweek evaluatie en planning 2025;
- herziening Privacyagenda: reguliere opvolging en verantwoording verbeteracties en risico's gebeurt vanaf nu via de Q-rapportages;
- ontwikkeling E-learning privacybescherming;
- jaarlijkse awareness enquête IB+P (medio mei);
- opstellen procedure privacyrisico's en het Risicoregister in navolging van IB;
- DPIA procedure en sjablonen;
- CBS brede DPIA herziening.

## **4. Rapportage voortgang BSN-reductie (bijlage 1)**

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. Deze jaarlijkse rapportage wordt in de Privacyagenda van Q1 aan het DB aangeboden.

**Vraag aan DB:** gaat het DB akkoord om voor 2025 een laatste rapportage uit te vragen?

Momenteel is zichtbaar dat de meeste verbetertrajecten in 2025 afgerond zijn en de lopende trajecten geen impuls meer nodig hebben vanuit het DB en opgenomen kunnen worden in het risicoregister.

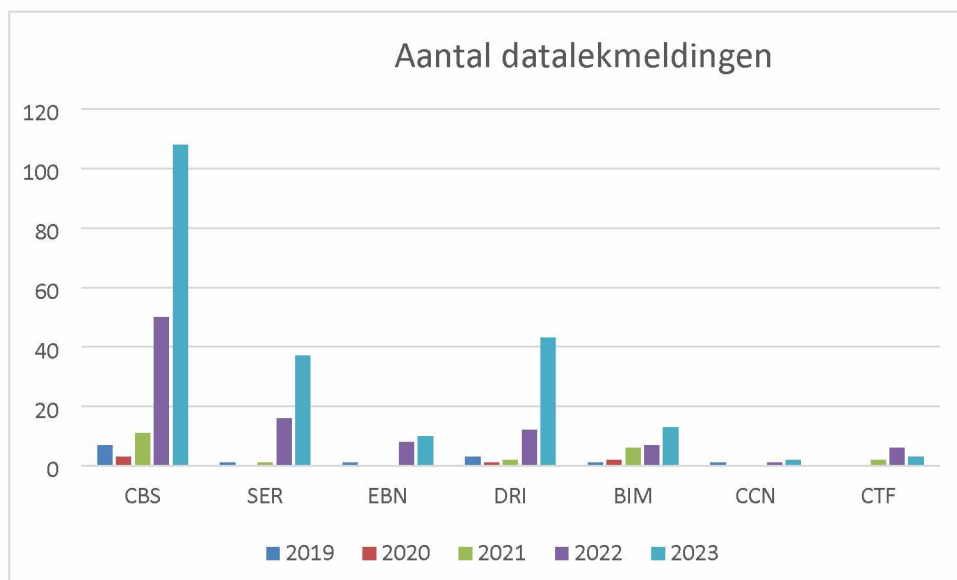
## **5. Korte terugkoppeling Datalekken 2023**

Sinds 2021 is de procedure melden datalekken sterk vereenvoudigd. Tevens is er bij webinars



en tijdens de awareness acties binnen de directies veel aandacht besteed aan het melden van een datalek. Door CBS medewerkers de gelegenheid te bieden op een sociaal veilige manier datalekken te melden kunnen we met elkaar het CBS zo veilig mogelijk houden. We hebben vanuit het privacyteam dan ook iedereen gestimuleerd alles te melden, ook al is het geen datalek dat door het CBS is veroorzaakt. Mede hierdoor is het aantal datalekken flink gestegen afgelopen jaar. Dit zien we als positief.

In 2023 is er één datalek gemeld bij de Autoriteit Persoonsgegevens. De streefwaarde voor het aantal gemelde datalekken was 0. Het datalek betrof een fout in een extern recruitmentsysteem waarbij sollicitatiegegevens niet automatisch na verloop van de relevante bewaartermijn werden verwijderd. Deze fout is inmiddels opgelost.



Van de 108 gemelde datalekken betrof de lek in 78 gevallen statistische informatie. In 52 gevallen betrof het informatie die door bronhouders of bedrijven via de mail naar het CBS waren gestuurd in plaats van via de beveiligde uploadportals. In 25 gevallen betrof het gegevens met BSN van registratiehouders (met name gemeenten). Omdat we nu inzichtelijk hebben hoe vaak we als CBS via mail gevoelige informatie ontvangen van zowel registratiehouders als bedrijven zijn we samen met CCN aan het onderzoeken hoe we de communicatie hierover kunnen verbeteren. Sommige websites kunnen weg, bij sommigen moeten we explicieter verwijzen naar uploadportals en e-





mailadressen verwijderen. Ook geeft Google nog een verwijzing naar een emailadres voor het aanleveren van gegevens. Deze wijzigingen zijn in een aantal gevallen al doorgevoerd.

**Oorzaken datalek**

Divisie	Totaal	SER	EBN	DRI	BIM	CCN	CTF
Via mail ontvangen gegevens	52	24	3	25	0	0	0
- w.o. BSN	25	17		8			
Gestolen apparatuur	15	3	5	7	0	0	0
personeelsgegevens	8	0	1	0	4	1	2
Verkeerde mail/info gestuurd	20	8	0	6	4	1	1
Overig	13	2	1	5	5	0	0
<b>Totaal</b>	<b>108</b>	<b>37</b>	<b>10</b>	<b>43</b>	<b>13</b>	<b>2</b>	<b>3</b>



## Actiepunten

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

	Actie en status	Planning	Actie houder
1	<b>E-learning privacybescherming en onboarding</b> De E-learning IB wordt momenteel uitgerold in de organisatie. Er is gestart met een aanvullende module privacybescherming. CCN heeft samen met de CPO een introductiefilmpje privacybescherming gemaakt voor nieuwe medewerkers. Ook is gestart met een awareness module in de onboarding, gelijk aan die van IB.	Q2 2024	BIM
2	<b>Proces toegang verlenen mailboxen</b> In bijlage 2 is een proces beschreven voor het verlenen van toegang aan overleden of vertrokken/langdurig afwezige medewerkers. Dit proces is afgestemd met SSC, directeur BIT, de FG en CSB-J. Het DB wordt gevraagd dit proces te verspreiden in de organisatie.	Q1 2024	CSB
3	<b>VerPRINnen</b> In bijlage 3 informeert de stuurgroep verPRINnen over de voortgang van het project.	Lopend	CTB
4	<b>Actualiseren crisismanagementplan en organiseren van een crisisoefening.</b> Vanuit privacy wordt aangehaakt bij de CBS brede crisisoefeningen en het crisisplan.	Start Q4 2023	CSB
5	<b>CBS quickscan en DPIA sjablonen</b>	Q2 2024	CSB
6	<b>Update CBS DPIA</b>	Q2 2024	CSB
7	<b>Risicoprocedure en risicoregister</b>	Q2 2024	CSB
8	<b>CBS-breed pseudonimiseerbeleid (middellange termijn)</b> 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.	Q3	CSB
9	<b>Beleid omtrent productiedata op niet productie omgeving.</b> EZK heeft hiervoor een concept beleidsstuk geschreven. De CPO zal voor het CBS beleid kijken of we hierop kunnen aansluiten.	Start Q4 2023	CSB
10	<b>Beleidsvoorstel IMS voor Privacy, IB en kwaliteit</b>	Q2	CSB

## Vervolg

De volgende rapportage is medio juli 2024