



aan DB
van Erik Bruinsma

onderwerp Evaluatie Datalekken 2022

datum 7 maart 2023

Achtergrond datalekregister

Het CBS is verplicht als verwerkingsverantwoordelijke een datalekregister bij te houden met daarin alle datalekmeldingen van de organisatie, ongeacht de ernst van het datalek (AVG art. 33). Met dit datalekregister kan het CBS aantonen dat we ons houden aan de meldplicht datalekken. Datalekken moeten bovendien binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen. Daarnaast is een belangrijk doel van het datalekregister dat een organisatie leert van eerdere datalekken en maatregelen neemt om de kans op nieuwe datalekken te verminderen.

Een datalek is: *‘toegang tot, of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie’*. Een datalek zit dus in een klein hoekje, maar door snel te handelen kan je de gevolgen beperken.

Aantal datalekken flink gestegen – en dat is niet altijd erg

Het melden van datalekken helpt de organisatie om veiliger te worden, de risico's te beheersen en de gevolgen te beperken. De afgelopen jaren kende het CBS zeer weinig datalekmeldingen. Zowel de Functionaris Gegevensbescherming als de externe auditors hebben hier zorgen over geuit aangezien de beperkte hoeveelheid meldingen kan wijzen op niet zichtbare risico's.

Om deze reden is in 2022 de procedure datalekken (zowel de front-als backoffice) hernieuwd en vereenvoudigd via TOPdesk. Daarnaast is er door de CPO en PC's in de awareness sessies veel aandacht besteed aan het belang van het melden van een datalek. Daarbij ligt altijd de nadruk op het veilig houden van de organisatie en het lerend vermogen van de organisatie door alles te melden. Dit heeft ertoe geleid dat er meer datalekken zijn gemeld dan eerdere jaren.

1. Totaal aantal datalekken

	Totaal	SER	EBN	DRI	BIM	CCN	CTF	Melding AP
2019	7	1	1	3	1	1	0	3
2020	3	0	0	1	2	0	0	0
2021	11	1	0	2	6	0	2	1
2022	50	16	8	7	7	1	6	1

Evaluatie datalekken

Van de 50 datalekmeldingen waren 19 meldingen intern.

- 10 keer betrof het verlies/diefstal van een laptop/telefoon. Deze meldingen worden voortaan niet meer opgenomen in het datalekregister, hier is een goede standaardprocedure voor;
- 9 keer kon mogelijk vertrouwelijke informatie worden ingezien door collega's binnen het CBS. Denk hierbij aan persoonlijke documenten in werkruimtes of door onterechte toegang op Varonis mappen.



Bij 31 van de 50 datalekmeldingen was er een externe instantie betrokken of externe contacten/respondenten. In 27 gevallen betrof het een datalek met beperkte impact:

- In 11 gevallen betrof het een externe fout, meestal microdata van berichtgevers die via de mail naar een CBS'ers werd gestuurd in plaats van via de uploadportal. Dit betreft geen datalek van het CBS maar is voor de evaluatie en communicatie richting berichtgevers goed om te weten;
- In 15 gevallen ging het om gegevens naar een verkeerde ontvanger (een CC in plaats van een BCC of om verkeerd bezorgde responsbrieven. Het CBS heeft 1 keer gegevens in een verkeerde uploadportal gezet en 1 keer heeft een externe partij verkeerde documenten van een zienswijze ontvangen. Daarnaast is er 1 keer een interne mail naar buiten verzonden waarin gegevens stonden over een rechtszaak;
- Er is 1 keer bij een brief naar een huisarts de naam van de overleden patiënt gebruikt in plaats van de arts.

De volgende 4 incidenten verdienen meer aandacht:

1. 2 datalekmeldingen bij dataservices:

- Eén incident betrof een outputbestand dat niet vrijgegeven had mogen worden, maar wel is vrijgegeven, maar wel aan de juiste ontvanger. Dit ging over het gepseudonimiseerd microdatabestand.
 - Verbeteractie: er is een extra handeling toegevoegd in de procedure om het risico dat de verkeerde output vrijgegeven wordt te verkleinen.
- Het andere incident betrof een output die wel vrijgegeven mocht worden, maar bij de verkeerde ontvanger terecht is gekomen.
 - Verbeteractie: vòòr het versturen van de output aan de onderzoeker wordt extra gecheckt of de naam en het projectnummer klopt.

Dataservices gaat dit jaar hun processen aanpassen naar o.a. een selfservice portaal in het project MUZIEK. Hierdoor komt er meer automatisering waardoor de kans op fouten kleiner worden.

2. Er is 1 keer een bestand naar een universiteit gemaïld door een stagiair (die dit overigens zelf heeft gemeld). Onthullingsrisico was hierbij zeer klein (volgens deskundige en FG).

Aanbevelingen:

- informatiebeveiliging en privacy standaard als onderwerpen bespreken bij de start van een stage of traineeship. Dit kan ook meegenomen worden in een breder advies over mailgebruik en beveiliging.
- 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.

3. 416 dozen met doodsoorzakenformulieren leken te zijn zoekgeraakt bij de oude archiefbewaarder. Door de overname van het archief door een andere partij is het CBS-archief zonder toestemming verplaatst. Door onduidelijkheid en ontbrekende depotlijsten zijn deze dozen enige tijd 'zoekgeraakt'. Uiteindelijk bleken de dozen bij de afdeling doodsoorzaken van het CBS aanwezig. Er wordt gekeken naar maatregelen om de procedures rond archivering en opvraging aan te scherpen of aangescherpt uit te laten voeren.

Aanbeveling: onderzoek doen of het daadwerkelijk nodig is het papieren archief in stand te houden. CPO zal in samenwerking met het inhoudelijk team archivering dit oppakken.

Veel datalekmeldingen met externe contacten/respondenten betreft ook mailverkeer. Een algemene aanbeveling is om samen met IB te kijken naar mogelijkheden hier technische oplossingen voor te bieden.