

aan DG

cc Directeur CSB, hoofd CAD, hoofd SSC, CPO, CISO

van FG en plvFG

onderwerp Omgang met inbreuken AVG bij het CBS

datum 26 april 2024

### Managementsamenvatting

Wij adviseren de registratie en opvolging van incidenten (datalekken) in de eerste lijn te beleggen zodat de FGs hun wettelijk geborgde advies- en toezichtsrollen kunnen uitvoeren. In de bijlage bij het advies geven we concretere adviezen over de opvolging van vier typen inbreuken. *Nota bene:* vanwege de vertrouwelijkheid van de geconstateerde inbreuken bij het CBS zal dit advies op intranet bij hoge uitzondering zonder de bijlage gepubliceerd worden, tenzij de DG anders besluit.

Dit FG-advies betreft de omgang met inbreuken in verband met persoonsgegevens in de zin van de AVG. Eerst bespreken we het wettelijk kader, daarna gaan we in op de huidige inrichting en waarom deze minder wenselijk is, en vervolgens vatten we samen welke grote lijnen we zien in de bij het CBS gemelde inbreuken en adviseren hoe hiermee om te gaan in termen van wel/niet melden bij de Autoriteit Persoonsgegevens.

### Wettelijk kader

Het wettelijk kader voor de melding van inbreuken in verband met persoonsgegevens wordt gevormd door de AVG, meer specifiek de artikelen 33 en 34. De definitie van een inbreuk in verband met persoonsgegevens is te vinden in art. 4 onder 12: “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens”. Conform art. 33 lid 1 AVG dient zo’n inbreuk bij de toezichthouder gemeld te worden, indien mogelijk binnen 72 uur na kennisneming.

Op deze meldplicht bestaat een uitzondering: “tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen”. Wel moeten alle inbreuken conform art. 33 lid 5 AVG gedocumenteerd worden, inclusief feiten, gevolgen en corrigerende maatregelen. Dit register moet door de toezichthouder ingezien

### De Babylonische spraakverwarring: incidenten, datalekken, inbreuken

De veelgebruikte term ‘datalek’ komt niet voor in de AVG. In de artikelen 33 en 34 wordt gesproken over ‘inbreuken in verband met persoonsgegevens’. Het gaat hierbij niet alleen maar om gevallen waarbij, populair gezegd, persoonsgegevens op straat komen te liggen, maar ook om bijvoorbeeld lange periodes van niet-beschikbaarheid. Daarom vermijden we in dit advies de term ‘datalek’ zo veel mogelijk. We gebruiken ‘incident’ als een nog niet in AVG-termen geclassificeerde gebeurtenis.



kunnen worden om de naleving van art. 33 AVG te kunnen controleren. Art. 34 AVG bepaalt de omstandigheden waaronder een inbreuk moet worden gemeld aan betrokkenen. Dit advies gaat verder niet op deze materie in. In voorkomende gevallen kan de FG adviseren over deze informatieplicht.

Gezien de inhoud van de CBS-wet worden naast alle inbreuken in verband met persoonsgegevens ook alle vergelijkbare inbreuken in verband met bedrijfsgegevens vastgelegd. Deze verplichting geldt sowieso vanuit de AVG wanneer de bedrijfsgegevens ook kwalificeren als persoonsgegevens, en naar analogie en vanuit art. 38 CBS-wet ook voor bedrijfsgegevens die niet kwalificeren als persoonsgegevens.

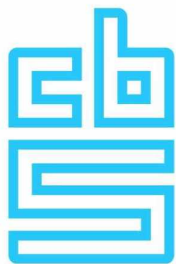
#### **Situatie bij het CBS**

De Procedure datalekken van 20 juni 2022 beschrijft de huidige omgang van het CBS met inbreuken in verband met persoonsgegevens. Bij het CBS bestaat al jaren een situatie waarin de registratie van inbreuken de facto grotendeels is belegd bij de FG. Deze situatie zal op afzienbare termijn veranderen, waardoor de FGs hun adviesfunctie op zuivere wijze kunnen invullen. De FGs adviseren dan aan de verwerkingsverantwoordelijke over de AVG-aspecten van de inbreuk, en kunnen toezicht houden op de wijze waarop de verwerkingsverantwoordelijke met inbreuken omgaat (inclusief de melding aan toezichthouder en betrokkenen, en de opvolging van inbreuken). De verwerkingsverantwoordelijke registreert de inbreuk, volgt deze intern (en waar nodig extern) op, en maakt na een integrale afweging al dan niet melding van de inbreuk bij de toezichthouder, en eventueel de betrokkene.

#### **Inzichten in gemelde inbreuken**

Intussen hebben de registratie en opvolging van inbreuken gedurende zo'n twee jaar wel inzichten opgeleverd, die wij bij dezen met de organisatie delen. Wij verwachten dat deze inzichten, samen met onze adviezen, gebruikt zullen worden voor het inbedden van registratie en opvolging in de eerste lijn. In de onderstaande tabel is het aantal gemelde inbreuken over de jaren 2019 tot en met 2023 gegeven. In de bijlage geven we in meer detail weer hoe ons advies luidt over de opvolging van deze inbreuken in verband met persoonsgegevens.

<i>Jaar</i>	<i>Gemelde inbreuken</i>
2019	7
2020	3
2021	14
2022	53
2023	109



### **Adviezen**

Wij adviseren als volgt:

- Beleg de registratie en opvolging van inbreuken in de eerste lijn.
- Zorg voor een robuuste inbedding van de registratie van inbreuken in bestaande incidentgerelateerde processen.
- Zorg dat de registratie en opvolging van inbreuken in lijn zijn met de meldplicht binnen 72 uur na kennisneming van de inbreuk.
- Richt de incidentgerelateerde processen zodanig in dat – waar toepasselijk – de adviesfuncties van bijv. de FG aangehaakt kunnen worden.
- Zorg ervoor dat interne stakeholders inzage krijgen in de actuele inbreukinformatie op detail- of geaggregeerd niveau, afhankelijk van de noodzaak daartoe.
- Wees terughoudend met de verstrekking van incidentinformatie aan externe partijen, uitgezonderd de Autoriteit Persoonsgegevens, de externe auditoren en de accountant. Bij laatstgenoemde partijen kan de verstrekte informatie gepseudonimiseerd worden.
- Neem in de inbreukregistratie ook inbreuken met betrekking tot bedrijfsgegevens en inbreuken van andere verwerkingsverantwoordelijken mee (met name van bronhouders).
- Onderneem proactieve stappen naar aanleiding van (patronen in) inbreuken binnen en buiten het CBS.