Procedure melden van datalekken

Versie 2025

Opstellers	College Noordelijke Rekenkamer
Datum	26 maart 2025

Inhoud

Procedure melden van datalekken

Deze procedure voorziet in een gestructureerde wijze voor het melden van datalekken.

1. Definities en omschrijving

- Datalek: een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
- Melding: kennisgeving van een datalek aan de Autoriteit Persoonsgegevens (AP) en/of aan de betrokkene (= de persoon die de persoonsgegevens betreffen).

De Noordelijke Rekenkamer (hierna: NRK) verwerkt in haar dienstverlenings- en bedrijfsvoeringsprocessen persoonsgegevens van zowel deelnemers aan onderzoeken als haar eigen medewerkers. Op deze verwerkingen van persoonsgegevens is de Algemene verordening gegevensbescherming (hierna: Avg) van toepassing; artikel 32 van de Avg bepaalt dat de verantwoordelijke voor de verwerking van persoonsgegevens (het bestuur van de NRK) beveiligingsmaatregelen treft die verlies of enige vorm van onrechtmatige verwerking moeten voorkomen.

Voor de NRK is de Baseline informatieveiligheid overheid (BIO) het uitgangspunt voor de te treffen maatregelen. De getroffen maatregelen bieden helaas geen honderd procent garantie dat de beveiliging niet kan worden doorbroken. Er kunnen zich twee situaties voordoen:

1. Inbreuk. Dit betreft alle beveiligingsincidenten die de bescherming van persoonsgegevens op enig moment doorbreken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende beveiligingsmaatregelen had getroffen of niet.
2. Datalek. De doorbreking van de bescherming leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Voorbeelden van beveiligingsincidenten zijn:

- kwijtgeraakte USB-stick;
- gestolen laptop;
- inbraak door een hacker;
- malware-besmetting;
- calamiteit zoals een brand in een datacentrum.

Melding bij de AP

Voor een melding geldt dat er sprake moet zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft. Het is dus niet zo dat een enkele tekortkoming of kwetsbaarheid in de beveiliging een melding aan de AP tot gevolg moet hebben. Als de gegevens op de verloren USB-stick of op de gestolen laptop zijn versleuteld, is in principe geen onrechtmatige toegang mogelijk. Dat is wel het geval als een onderzoeksmedewerker een laptop verliest met daarop onversleutelde gegevens van iemand met wie een interview is gehouden in het kader van een onderzoek.

Tenzij het onwaarschijnlijk is dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid of mogelijk kan leiden, moet de verwerkingsverantwoordelijke het datalek zo snel als mogelijk is doch uiterlijk 72 uur na ontdekking melden aan de AP.

Melding aan de betrokkene

Volgens de Avg stelt de verantwoordelijke de betrokkene onverwijld in kennis van de inbreuk op de beveiliging als die inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De verantwoordelijke moet daar een inschatting van maken. Ongunstige gevolgen zijn er al snel als een onbevoegde kennis heeft kunnen nemen van de zogenaamde *bijzondere* pesoonsgegevens. Dit betreft onder meer medische gegevens, strafrechtgegevens, seksuele leven, godsdienst en levensovertuiging. Deze gegevens zijn privacygevoeliger dan gegevens als naam en geboortedatum en kunnen bij verlies of misbruik ernstige gevolgen hebben voor de betrokkene. In dergelijke gevallen dient de verantwoordelijke de betrokkene in kennis te stellen van het datalek.

2. Taken, verantwoordelijkheden en bevoegdheden

- De beveiligingsfunctionaris (de medewerker die belast is met taken op het gebied van informatiebeveiliging) is verantwoordelijk voor de actualiteit van deze procedure, de bekendmaking en het in kennis stellen c.q. instrueren van de medewerkers.
- Iedere medewerker die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden aan de secretaris-directeur.
- De beveiligingsfunctionaris is verantwoordelijk voor onderzoek en rapportage naar aanleiding van een beveiligingsincident.
- De privacy officer (of medewerker die belast is met privacytaken) is verantwoordelijk voor de advisering van de secretaris-directeur en het bestuur over de mogelijk gevolgen van een datalek voor de privacy van betrokkenen.
- De secretaris-directeur verleent alle medewerking aan het onderzoek en is verantwoordelijk voor:

- het ondernemen van preventieve en repressieve beveiligingsacties;
- de melding aan de AP en aan betrokkene;
- de communicatie met de AP en betrokkenen naar aanleiding van de meldingen.

3. Uitvoering

1. De medewerker die direct of indirect kennis draagt of krijgt van een datalek, meldt dit direct aan de beveiligingsfunctionaris.
2. De beveiligingsfunctionaris laat het beveiligingsincident onderzoeken; hierbij is aandacht voor de volgende aspecten:
   - de aard van het datalek;
   - de oorzaak dat dit datalek heeft plaatsgevonden;
   - is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
   - is er sprake van verwijtbaar handelen en door wie?
3. De beveiligingsfunctionaris maakt van het datalek een verslag; het verslag bevat in ieder geval de volgende informatie:
   - plaats in de organisatie waar het datalek zich heeft voorgedaan, en het informatiesysteem of persoonsgegevensverwerkend proces waar het datalek betrekking op heeft;
   - beschrijving van het datalek;
   - opgave van de categorieën van personen waarvan de (bijzondere) persoonsgegevens betrokken zijn in het datalek;
   - inzicht in de getroffen maatregelen die genomen zijn om eventuele gevolgen te beperken;
   - inzicht in de getroffen maatregelen om dergelijke datalekken in de toekomst te voorkomen .
4. De privacy officer beoordeelt of het datalek ernstige nadelige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n) en adviseert secretaris-directeur en bestuur over het doen van de meldingen aan de AP en aan de betrokkenen.
5. De secretaris-directeur besluit over het al dan niet doen van een melding.
6. De secretaris-directeur doet de melding aan de AP en aan de betrokkene(n).
7. De secretaris-directeur en de beveiligingsfunctionaris zijn aanspreekpunt voor de AP en voorzien de AP voor zover noodzakelijk van nadere toelichting.
8. De NRK legt eventuele aanwijzingen van de AP vast en volgt die op.
9. De beveiligingsfunctionaris legt een dossier aan van het datalek en registreert dit in de incidentenregistratie.
10. De beveiligingsfunctionaris informeert de Informatiebeveiligingsdienst van de provincies over incidenten die gevolgen kunnen hebben voor andere verantwoordelijken.

4. Interne controle

- De beveiligingsfunctionaris analyseert de gedurende een jaar ontvangen meldingen en stelt een verbeterplan of -advies op. Dat plan of advies wordt opgenomen in de jaarlijks uit te brengen managementrapportage.
- Minimaal jaarlijks beoordeelt de beveiligingsfunctionaris of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien dat niet het geval is, beoordeelt de NRK of zij de procedure moet actualiseren en/of medewerkers moet instrueren op een juiste toepassing van de procedure.

5. Verwerkers

Een verwerker is een persoon of organisatie die niet onder het gezag valt van de verantwoordelijke en die namens de verantwoordelijke werkzaamheden verricht die gericht zijn op de verwerking van persoonsgegevens. Voorbeelden van dat soort werkzaamheden zijn de uitbesteding van de ICT-infrastructuur en het gebruik van Exact On-Line. Verantwoordelijke en verwerker leggen in een verwerkersovereenkomst vast aan welke beveiligingseisen de verwerker moet voldoen. De verwerker dient de verantwoordelijke in staat te stellen om te kunnen voldoen aan diens verplichtingen in het kader van het melden van datalekken. Verantwoordelijke en verwerker kunnen overeenkomen dat de verwerker namens de verantwoordelijke op een vergelijkbare wijze als beschreven in deze procedure, invulling geeft aan de meldplicht. De verantwoordelijke is verplicht de nakoming van de afspraken te controleren.