Procedure datalek

de Zorgnijverij

met hart en handen

Versie 3.2 - 10 april 2024 - Jostijn der Weduwe

Inhoudsopgave

Inleiding

Deze procedure beschrijft de verschillende stappen die binnen de Zorgnijverij genomen worden bij een datalek, die valt onder de registratie en mogelijke meldplicht datalekken van de Algemene Verordening Gegevensbescherming (AVG). Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 33 en 34 AVG). De persoonsgegevens zijn dan (mogelijk) blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen onder meer ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, virus/malware besmetting);
- technisch falen (ICT-storing);
- menselijk falen (te eenvoudige wachtwoorden, het verstrekken van inlognaam/wachtwoord aan derden, incorrecte autorisaties);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van e-mail naar onjuiste geadresseerden;
- maar ook het onrechtmatig verwerken van gegevens.

Een datalek dient intern gemeld, geregistreerd en beoordeeld te worden. Afhankelijk van de beoordeling worden maatregelen geadviseerd. Deze maatregelen dienen te worden gemonitord. Uit de beoordeling volgt ook of het datalek dient te worden gemeld bij de Autoriteit Persoonsgegevens (AP) en of de betrokkenen moeten worden geïnformeerd. Bij de beoordeling van een datalek wordt onder meer het AP Stappenplan gevolgd (zie Bijlage 2).

Wat te doen bij een datalek

1 Datalek?

Een incident is een datalek indien persoonsgegevens:

- verloren zijn;
- onbereikbaar zijn;
- gewijzigd zijn; of
- voor onbevoegden ontoegankelijk zijn.

2 Actie + Beoordeling

- We onderzoeken wat er precies gebeurd is;
- nemen maatregelen om verdere schade te voorkomen; en
- beoordelen of het een datalek is.

3 Melden bij de AP?

Binnen 72 uur na de datalek melden wij dit bij de Autoriteit Persoonsgegevens, tenzij er geen risico voor de betrokkenen bestaat.

4 Informeren

We informeren de betrokkenen bij een hoog risico. Hiervan is sprake indien de datalek kan leiden tot:

- lichamelijk; of
- materiële/immateriële schade

5 Registreren

We nemen het volgende op in een register:

- omschrijving van alle datalekken
- gemeld ja/nee
- geïnformeerd ja/nee
- motivering van beslissing

Rollen

Responseteam Datalek

- Kwaliteitsmedewerker en Jurist
- Operationeel manager
- Functionaris Gegevensbescherming (FG)

Behandelaar

De volgorde van het Responseteam Datalek bepaalt wie de melding initieel aanneemt. Bij afwezigheid dient de opvolgende uit het Responseteam Datalek de melding aan te nemen. De Kwaliteitsmedewerker en Jurist en de Operationeel manager schakelen zo nodig de Functionaris Gegevensbescherming (FG) in.

(Verwerkings-) verantwoordelijke

Degene die formeel, juridisch en feitelijk zeggenschap heeft over het doel en de middelen voor de verwerking van persoonsgegevens en daarmee ook de verantwoordelijke voor het proces waarbinnen het datalek plaatsvindt. In de regel is dit de Zorgnijverij. De Raad van Bestuur is eindverantwoordelijk.

Verwerker

Degene die in opdracht van de Zorgnijverij persoonsgegevens verwerkt (zoals softwareleveranciers, website hosts, clouddiensten, externe kwaliteitsauditor).

1 Melding aan Responseteam Datalek

Elk (mogelijk) datalek dient direct aan het Responseteam Datalek gemeld te worden om de ongewenste situatie te beoordelen en maatregelen te treffen dan wel voor te stellen om deze te herstellen of risico's te beperken. De verplichting tot melding voor medewerkers is vastgelegd en gecommuniceerd via deze procedure. Voor verwerkers en samenwerkende partijen is de verplichting opgenomen in de verwerkersovereenkomst c.q. samenwerkingsovereenkomst.

Melding van een datalek kan worden gedaan door het invullen van het formulier Melding Datalek in Forms (Bijlage 1), de melding komt dan terecht bij het Responseteam Datalek.

De melding kan ook door een externe persoon worden gedaan bij een medewerker van de Zorgnijverij. De melding moet dan direct door de medewerker worden doorgezet via formulier Melding Datalek in Forms (Bijlage 1), de melding komt dan terecht bij het Responseteam Datalek.

2 Intake

De Behandelaar neemt contact op met de melder voor een verdere intake om te beoordelen of er sprake is van een datalek.

Bij de intake worden de volgende gegevens vastgesteld:

- naam van de melder;
- datum en tijd van de melding;
- aard van de inbreuk (is er een aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- welke persoonsgegevens onder de melding vallen;
- om welk aantal en/of gegevensrecords het gaat;
- welke (groepen) personen betrokken zijn bij de melding;
- welke maatregelen door de melder zijn of worden getroffen;
- welke gevolgen er volgende de melder voor de betrokkenen zijn;
- de contactpersoon voor de melding voor meer informatie.

Bij voorkeur wordt gebruik gemaakt van het Intakeformulier datalek. Dit intakeformulier wordt door de Behandelaar opgenomen in het Datalek Register.

3 Eerste analyse

De Behandelaar beoordeelt of van de inbreuk redelijkerwijs kan worden aangenomen dat deze leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van betrokkenen zijn verbonden.

4 Registratie

Ieder gemeld (mogelijk) datalek dient door de Behandelaar geregistreerd te worden in het totaaloverzicht in het Datalek Register.

5 Informeren van verwerkingsverantwoordelijke

Afhankelijk van het risico van het datalek informeert de Behandelaar de Verwerkingsverantwoordelijke, telefonisch dan wel schriftelijk, voorafgaand aan het advies, dit omdat de tijd tussen melding en advies te lang zou kunnen zijn.

6 Overleg Responseteam Datalek

Bij een hoog risico of niet precies te duiden datalek kan de Behandelaar besluiten het voltallig Responseteam Datalek bijeen te laten komen. De wijze waarop (videoconference, fysiek, e-mail) is afhankelijk van de aard en impact van het potentiële datalek en het tijdstip van de melding.

Tijdens kantooruren: direct bijeenroepen van het Responseteam Datalek
Buiten kantooruren en in het weekend: Als her mogelijk is, wordt een eventueel benodigd overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is, wordt zoveel als mogelijk telefonisch en elektronisch overleg gevoerd.

De bijeenkomst wordt voorgezeten door de Behandelaar. Het responseteam bespreekt en legt vast:

- De gegevens die door de Behandelaar zijn vastgelegd bij de intake;
- De noodzakelijke vervolgacties met betrekking tot het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en/of tegelijkertijd meer informatie vergaren over de indringer). Deze vervolgacties zullen in het advies aan de Verwerkingsverantwoordelijke worden opgenomen. Het Responseteam Datalek kan besluiten bepaalde risico mitigerende maatregelen al direct in gang te zetten;
- Hetgeen gemeld gaat worden bij de AP door de Behandelaar (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records):
- De mogelijke gevolgen voor de betrokkenen;
- De maatregelen die de Zorgnijverij neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
- De maatregelen die betrokkenen kunne nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
- Contactgegevens voor betrokkenen;
- De wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling, leidinggevenden en de Raad van Bestuur;
- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- Hetgeen intern gecommuniceerd wordt en op welk moment;
- Hetgeen extern gecommuniceerd wordt en op welk moment;
- Of naast het AP ook andere stakeholders geïnformeerd dienen te worden.

7 Advies aan verwerkingsverantwoordelijke

De Behandelaar adviseert de Verwerkingsverantwoordelijke schriftelijk. Dit advies beschrijft het incident en stelt de te nemen maatregelen voor, waaronder minimaal het advies om het datalek wel of niet te laten melden bij de Autoriteit Persoonsgegevens en het wel of niet informeren van de betrokkenen. De Behandelaar vraagt ten slotte de Verwerkingsverantwoordelijke om binnen 8 uur na het advies te reageren op dit advies, waarbij de Verwerkingsverantwoordelijke in ieder geval laat weten of de geadviseerde maatregelen worden opgevolg, en zo niet waarom hiervan wordt afgeweken. Tevens moet de Verwerkingsverantwoordelijke akkoord geven voor het melden van het datalek bij de Autoriteit Persoonsgegevens, indien is beoordeeld dat een meldingsplichtig datalek betreft.

Dit advies wordt door de Behandelaar opgenomen in het Datalek Register.

8 Herstelmaatregelen

De Behandelaar onderneemt waar nodig actie om de schade te beperken, bijvoorbeeld door:

- een laptop, tablet of smartphone op afstand te wissen of te versleutelen;
- een gepubliceerd bestand offline halen;
- een verkeer ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd;
- het op afstand blokkeren van de toegang tot een medewerkers account of clouddienst

.

De genomen herstelmaatregelen worden opgenomen in het Datalek Register.

9 Melding aan Autoriteit Persoonsgegevens

Wanneer uit de beoordeling blijkt dat er sprake is van een meldingsplichtig datalek, meldt de Behandelaar (na akkoord van de Verwerkingsverantwoordelijke) binnen 72 uur na de ontdekking van het datalek volgens de aangewezen methode4 het datalek bij de Autoriteit Persoonsgegevens. Het beleggen van het daadwerkelijk melden bij de Behandelaar in plaats van de Verwerkingsverantwoordelijke is gedaan omwille van expertise en breder zicht op andere lopende of geplande maatregelen.

In ieder geval zal gemeld worden:

- de aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- een beschrijving van de te verwachten gevolgen;
- de getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- de contactgegevens voor de betrokkene(n).

Is er een melding gedaan, dan dient de Behandelaar de webbased ontvangstbevestiging, inclusief inhoudelijke melding, op te slaan naar een pdf-bestand.5 Deze ontvangstbevestiging wordt door de Behandelaar opgenomen in het Datalek Register.

10 Melding aan betrokkenen

De Behandelaar adviseert de Verwerkingsverantwoordelijke over het informeren van (groepen) betrokkenen. De Verwerkingsverantwoordelijke is verantwoordelijk voor het tijdig informeren van betrokkenen. De Verwerkingsverantwoordelijke kan het informeren van betrokkenen uitbesteden aan de Mentor.

De Verwerkingsverantwoordelijke informeert de Behandelaar betreffende de status van het informeren van de betrokkenen en verschaft de Behandelaar een geanonimiseerd voorbeeld van het daadwerkelijk verstuurde bericht.

Deze voorbeelden worden door de Behandelaar opgenomen in het Datalek Register voor eventueel ander gebruik.

Bijlage I - Formulier melding datalek

Als er zich een situatie heeft voorgedaan waarbij er kans is dat er persoonsgegevens van cliënten of medewerkers van De Zorgnijverij in verkeerde handen zijn gevallen, verloren zijn gegaan of veranderd zijn, dan is de Zorgnijverij verplicht dit te onderzoeken en indien nodig te melden bij de Autoriteit Persoonsgegevens en/of de betrokkenen.

Vul in en verstuur bij (een vermoeden van) een beveiligingsincident/datalek onderstaand formulier. Na ontvangst van de melding nemen wij contact met u op voor nadere informatie om het datalek te kunnen onderzoeken.

1. Naam melder/contactpersoon
2. E-mail melder/contactpersoon
3. Telefoonnummer melder/contactpersoon

1. Wat voor soort datalekmelding wilt u doen?

- Ik wil één inbreuk melden (reguliere melding)
- Ik wil meerdere gelijksoortige inbreuken, als gevolg van een grootschalige postverzending, tegelijk melden (bulkmelding)

2. Afdeling

(meerdere antwoorden mogelijk)

- Kind en Jeugd
- Dagbesteding Houtwerkplaats
- Dagbesteding SMAAK
- KDC

2. Geef een samenvatting van het incident waarbij het vermoeden of de constatering van de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan

3. Wat is de aard van de inbreuk?

(meerdere mogelijkheden aankruisen/beschrijven)

- Lezen (vertrouwelijk)
- Kopiëren
- Veranderen (integriteit)
- Verwijderen of vernietigen (beschikbaarheid)
- Diefstal
- Verloren
- Nog niet bekend
- Anders / Omschrijving van de situatie:

4. Om welk type persoonsgegevens gaat het?

- Naam-, adres- en woonplaatsgegevens
- Telefoonnummers
- E-mailadressen of andere adressen voor elektronische communicatie
- Toegangs- of identificatiegegevens (bv inlognaam / wachtwoord of klantnummer)
- Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
- Burgerservicenummer (BSN)
- Paspoortkopieën of kopieën van andere legitimatiebewijzen
- Geslacht, geboortedatum en/of leeftijd
- Bijzondere Persoonsgegevens; Geef aan om welke bijzondere Persoonsgegevens het gaat (kies één of meerdere opties):
- Godsdienst of levensovertuiging
- Ras
- Politieke voorkeur
- Gezondheid
- Seksuele geaardheid
- Lidmaatschap van een vakbond
- Strafrechtelijke informatie
- Anders, namelijk:

5. Wanneer vond de inbreuk plaats?

(kies een van de volgende opties en vul waar nodig aan)

- Op
- Tussen
- Nog niet bekend

Bijlage 2- Stappenplan AP

AUTORITEIT
PERSOONSGEGEVENS

Stappenplan: kom in actie bij een datalek

Heeft uw organisatie te maken met een datalek? Dan is het belangrijk dat u als privacycontactpersoon snel in actie komt. Met dit stappenplan helpen we u op weg.

Stap 1: zorg voor overzicht

Analyseer onmiddellijk de situatie. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Indien gegevens zijn gelekt, onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Deze informatie heeft u nodig voor de vervolgstappen.

Stap 2: Beperk de schade!

Bepaal op basis van stap 1 of er maatregelen zijn die u meteen kunt nemen om het datalek te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Bijvoorbeeld door een gestolen laptop op afstand te wissen. Maak tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert (stap 3).

Stap 3: Wel/niet melden bij de AP

Bepaal of u het datalek verplicht moet melden bij de Autoriteit Persoonsgegevens (AP). Zo ja, zorg dat u dit ***binnen 72 uur*** nadat u het lek heeft ontdekt doet. U moet een datalek melden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Heeft u bij de eerste melding nog niet alle informatie over het datalek?
Doe dan een eerste melding binnen 72 uur en doe later een vervolgmelding.

Naar het meldloket datalekken
Zie ook: voorbeeldlijst 'datalek wel/niet melden bij AP en betrokkenen'

Stap 4: Wel/niet melden aan de betrokken personen

Bepaal of u het datalek verplicht moet melden aan de betrokken personen. Zo ja, zorg dat u dit zo snel mogelijk doet. U moet een datalek melden aan de betrokken personen wanneer er sprake is van een *hoog* risico voor de rechten en vrijheden van de betrokken personen.

Stap 5: Registreer het datalek

Registreer het datalek in uw verplichte datalekregister. Ook wanneer u het datalek niet meldt aan de AP.

Zie ook: 10 praktische tips voor betere datalekregistratie

Heeft u bovenstaande stappen doorlopen? En alles gedaan om de schade te beperken?
Start dan een evaluatie om een herhaling van het datalek te voorkomen.