Protocol meldplicht datalekken

Dehlia Kracht B.V.

Protocol meldplicht datalekken aan de Functionaris voor de Gegevensbescherming

Groenestraat 294, 6531 JC Nijmegen

Inhoudsopgave

Protocol meldplicht datalekken aan Functionaris Gegevensbescherming

Inleiding

Als persoonsgegevens in verkeerde handen zijn gekomen, of zijn kwijtgeraakt, moet dat worden gemeld bij de Autoriteit Persoonsgegevens. Die melding hoef je niet zelf te doen, dat doet de Functionaris voor de Gegevensbescherming (FG). Maar wat is een datalek? Wanneer moet je het datalek melden bij de Functionaris voor de Gegevensbescherming?

Hoe te melden?

In de bijlage van dit protocol tref je het formulier aan, waarmee je een datalek kunt melden. Vul dit formulier zo goed mogelijk in en mail dat naar de Functionaris voor de Gegevensbescherming.
Is het formulier helemaal ingevuld? Mail het dan naar privacy@dahliakracht.nl.

Wat is een Functionaris voor de Gegevensbescherming?

De Functionaris voor de Gegevensbescherming is de interne toezichthouder op de gegevensverwerking binnen de organisatie. De Functionaris voor de Gegevensbescherming draagt er zorg voor dat een datalek wordt gemeld bij de Autoriteit Persoonsgegevens en geeft achteraf ook advies over hoe het proces is verlopen. De Functionaris voor de Gegevensbescherming heeft daarnaast als taak gevraagd en ongevraagd advies te geven aan de directie ten aanzien van de naleving van de privacy regels.

Wat is een datalek?

In de Algemene Verordening Gegevensbescherming is datalekken gedefinieerd als: 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.
Een datalek is op de eerste plaats een beveiligingsincident. Daarnaast moet er dus sprake zijn van verlies van persoonsgegevens of dat een onrechtmatige verwerking daarvan niet kan worden uitgesloten. De verloren persoonsgegevens moeten impact hebben op de levenssfeer van de betrokkene.

Voorbeelden van datalekken

- Een USB stick dat raakt zoek, of een laptop wordt gestolen. Er staan bestanden op met persoonsgegevens;
- Je werkt thuis, bent ingelogd op het netwerk, en de laptop waarop je werkt wordt gehackt, er is malware of ransomware geïnstalleerd. Omdat dit soort kwaadaardige programma's meestal op zoek zijn naar persoonsgegevens, wordt er verondersteld dat er een datalek is;
- Bestanden met persoonsgegevens worden per abuis gewist, en er is geen back-up. Ook dan is er een datalek;
- E-mails waarin zichtbaar is aan wie de e-mail allemaal nog meer is gezonden (het gaat uiteraard niet om e-mails aan collega's binnen de organisatie, maar e-mails aan derden buiten de organisatie);
- Het bedrijfstelefoon raakt zoek. Hierop staan ook persoonsgegevens;

- Laptops worden afgedankt door de organisatie maar de gegevens erin zijn niet gewist;
- Een e-mail met persoonsgegevens wordt per ongeluk naar een verkeerde ontvanger verzonden.

Wat is geen datalek?

- De privételefoon raakt zoek. Hierop staan ook persoonsgegevens, maar dat is uitsluitend voor huishoudelijke doeleinden.
- Een USB stick raakt kwijt. Er zijn geen persoonsgegevens hierin opgeslagen.

Kortom: datalekken hebben betrekking op persoonsgegevens.

Wat is een persoonsgegeven?

Elk gegeven dat naar een natuurlijke persoon herleidbaar is, is persoonsgegeven.
Een paar voorbeelden van persoonsgegevens:

- Naam, adres, woonplaats;
- Postcode met huisnummers;
- E-mailadressen;
- Burger servicenummers;
- Locatiegegevens;
- IP adressen;
- Gebruikersgegevens, zoals inlognamen en wachtwoorden.

Een persoonsgegeven dat op zich geen persoonsgegeven is, maar in combinatie met andere gegeven er toe leidt, dat een persoon te identificeren is, wordt aangemerkt als persoonsgegeven. Een kenteken, chassisnummer van een auto, locatiegegevens in een navigatiesysteem zijn op zich geen persoonsgegeven, maar in combinatie met persoonsgegevens worden zij wel persoonsgegevens.

Er zijn ook nog bijzondere categorieën van persoonsgegevens. Op de verwerkingsverantwoordelijke rust aanvullende plicht om deze persoonsgegevens te beschermen tegen onbevoegden. Hat gaat om persoonsgegevens over geloofsrichting, medische gegevens, afkomst en/of huidskleur, politieke voorkeur, seksuele voorkeur of seksueel gedrag, lidmaatschap van de vakbond, biometrische gegevens en strafrechtelijke gegevens. Als er mogelijk sprake is van een datalek, is het voor de Functionaris voor de Gegevensbescherming van belang om te weten of het gaat om bijzondere persoonsgegevens.

Datalekken en Functionaris voor de Gegevensbescherming

Een datalek dient altijd te worden gemeld. Ook bij twijfel moet altijd de Functionaris voor de Gegevensbescherming worden geïnformeerd over het datalek. De Functionaris voor de Gegevensbescherming zal vervolgens een afweging moeten maken of het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens. Als er twijfel is of een beveiligingsincident een datalek is, is het verstandig om zo snel mogelijk contact op te nemen met de Functionaris voor de Gegevensbescherming om de noodzaak van het melden van een datalek te onderzoeken.

Het is mogelijk dat persoonsgegevens van een cliënt door derden buiten de zorginstelling worden verwerkt. Als een database bij een andere organisatie is ondergebracht, is de zorginstelling verwerkingsverantwoordelijke in de zin van de Algemene Verordening Gegevensbescherming. De zorginstelling is de verwerkingsverantwoordelijke, omdat zij bepaalt welke persoonsgegevens moeten worden opgeslagen, bewerkt, verwijderd etc. Ook als er datalek is bij de externe verwerker van persoonsgegevens, moet zo'n datalek bij de Functionaris voor de Gegevensbescherming gemeld worden. De Functionaris voor de

Gegevensbescherming beoordeelt of er contractueel andere afspraken zijn gemaakt over het melden van datalekken.

Als er sprake is van een datalek, moet dit altijd bij de Functionaris voor de Gegevensbescherming te worden gemeld. In dit protocol wordt niet ingegaan op de vraag welke afwegingen de Functionaris voor de Gegevensbescherming dient te maken.
Als de Functionaris voor de Gegevensbescherming om medewerking vraagt, bijvoorbeeld om te kunnen beoordelen of de betrokkenen moeten worden geïnformeerd over het datalek, dan moet hier prioriteit aan worden gegeven. Er moet namelijk snel en adequaat gehandeld worden. Ingeval van een datalek speelt tijdsdruk altijd een belangrijke rol.

Termijn melding datalekken

Na het ontdekking van het datalek, dient de Functionaris voor de Gegevensbescherming het datalek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens, dit op grond van de privacywetgeving. Het is voor iedereen van belang dat een datalek zo spoedig mogelijk, het liefst al binnen 24 na de ontdekking van het datalek, wordt gemeld.
Als een organisatie deze verplichting niet (of niet op tijd) nakomt, kunnen er enorme boetes worden volgen.
In geval van twijfel, neem contact op met de Functionaris voor de Gegevensbescherming zodat er snel schadebeperkende maatregelen kunnen worden getroffen.
Een schade beperkende maatregel kan zijn, dat degenen waarvan de persoonsgegevens zijn gelekt, worden geïnformeerd over het datalek en dat aan hen suggesties worden gedaan hoe verder schade kan worden voorkomen. De Functionaris voor de Gegevensbescherming beoordeelt of dit nodig is. Daarvoor heeft hij de gegevens uit het bijgevoegde formulier nodig.
Bij de melding moet ook worden aangegeven wat er al is gebeurd, en welke maatregelen er genomen zijn om de nadelige gevolgen van datalekken zoveel mogelijk te beperken.

Melden datalek aan de toezichthouder achterwege laten?

Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met het lidmaatschap van de patiënten of cliëntenorganisatie zijn gelekt. Het lidmaatschap van de organisatie kan gezien worden als een gevoelig gegeven en de leden van de organisatie kunnen wellicht behoren tot een kwetsbare groep, die extra bescherming nodig heeft. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Melden datalek aan betrokkene achterwege laten?

Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Formulier melding datalekken
Op de volgende bladzijde is het formulier voor het melden van datalekken bijgevoegd.

FORMULIER MELDEN DATALEKKEN

Algemene gegevens	
Gaat het om een nieuwe melding of bestaande melding?	Nieuwe melding al bestaande melding
Naam van degene die melding doet bij de Functionaris voor de Gegevensbescherming	
Telefoonnummer melder	
E-mailadres melder	
Functie melder	
Gegevens over het datalek	
Gaat het om een verwerking die is uitbesteed aan een andere organisatie? Zo ja, welke organisatie?	
Van minimaal en maximaal hoeveel personen zijn persoonsgegevens betrokken bij het datalek?	Minimaal: Maximaal:
Is het bekend wanneer het datalek was?	Ja / Nee
Zo ja, wanneer?	
Aard van de inbreuk	
Lezen (vertrouwelijk)	Ja / Nee / weet niet
Kopiëren	Ja / Nee / weet niet
Veranderen (integriteit)	Ja / Nee / weet niet
Verwijderen of vernietigen (beschikbaarheid)	Ja / Nee / weet niet
Nog niet bekend	Ja / Nee / weet niet
Soort persoonsgegevens	
Over iemands godsdienst of levensovertuiging	Ja / Nee / weet niet
Iemands ras / afkomst / huiskleur	Ja / Nee / weet niet
Iemands politieke gezindheid	Ja / Nee / weet niet
Iemands gezondheid / medische gegevens	Ja / Nee / weet niet
Seksuele leven / voorkeur	Ja / Nee / weet niet
Biometrische gegevens, DNA en dergelijke	Ja / Nee / weet niet
Lidmaatscha vakvereniging	Ja / Nee / weet niet
Strafrechtelijke gegevens	Ja / Nee / weet niet
Mogelijke gevolgen van het datalek	

Stigmatisering of uitsluiting	Ja / Nee / weet niet
Schade aan gezondheid	Ja / Nee / weet niet
Blootstelling aan identiteitsfraude	Ja / Nee / weet niet
Blootstelling aan spam of phishing	Ja / Nee / weet niet
Andere gevolgen:	