Stichting Nollestee
Nolleweg 1b
3248 LE Melissant
0187-603953
www.nollestee.nl
info@nollestee.nl

KvK: 73872016
AGB code: 98105145
BTW nr: NL8596.94.008.B01
Bank Zorgdiensten: NL88 RABO 03006 70826
Bank Kwekerij: NL47 RABO 01349 70926
Bank Giften: NL97 RABO 03502 38634

Procedure datalekken

Stichting Nollestee
Nolleweg 1b
3248 LE Melissant
0187-603953
www.nollestee.nl
info@nollestee.nl

KvK: 73872016
AGB code: 98105145
BTW nr: NL8596.94.008.B01
Bank Zorgdiensten: NL88 RABO 03006 70826
Bank Kwekerij: NL47 RABO 01349 70926
Bank Giften: NL97 RABO 03502 38634

Inhoud

Stichting Nollestee
Nolleweg 1b
3248 LE Melissant
0187-603953
www.nollestee.nl
info@nollestee.nl

KvK: 73872016
AGB code: 98105145
BTW nr: NL8596.94.008.B01
Bank Zorgdiensten: NL88 RABO 03006 70826
Bank Kwekerij: NL47 RABO 01349 70926
Bank Giften: NL97 RABO 03502 38634

1. STREKKING/DOEL

Sinds 1 januari 2016 geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onverwijld moeten melden aan de Autoriteit Persoonsgegevens (hierna: 'AP'), en in bepaalde gevallen ook aan de betrokken personen van wie de gegevens zijn gelekt.

De bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt, moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen onder andere ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting)
- technisch falen (ICT-storingen)
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen
- calamiteit (brand datacentrum, wateroverlast)
- het verliezen van bijvoorbeeld een USB stick, telefoon, iPad, uitgeprinte planningen of laptop
- verzenden van email met emailadressen van alle geadresseerden in de cc terwijl dit in de BCC had gemoeten etc.
- het onrechtmatig delen van cliëntgegevens (al dan niet bewust), zonder toestemming van de cliënt/vertegenwoordiger.

2. BETROKKEN FUNCTIES

Medewerker SZZ
Functionaris Gegevensbescherming (hierna: FG)
Directeur

3. WERKINSTRUCTIE

3.1 Inleiding

Een datalek moet onverwijld, zo mogelijk niet later dan 72 uur na de ontdekking, worden gemeld bij de AP. Indien het datalek waarschijnlijk ongunstige gevolgen heeft voor het privéleven van de personen van wie gegevens zijn gelekt, dient het datalek eveneens onverwijld gemeld te worden aan die betreffende personen.

3.2 Identificeren van een datalek

- De medewerker die een (mogelijk) datalek constateert, meldt dit incident per omgaande aan de FG door middel van het Meldingsformulier Datalek.
- Ook (de medewerker van) een verwerker kan een datalek constateren. Hij/zij kan dit melden bij de FG.
- De FG informeert bij een (mogelijk) meldingsplichtig datalek per ommegaande de directeur en, indien van toepassing, de verantwoordelijk manager hierover.

3.3 Beoordeling aard/ernst mogelijk datalek

De FG beoordeelt zo spoedig mogelijk, doch uiterlijk de werkdag na de melding, op basis van de verkregen informatie of het datalek gemeld dient te worden.

- Indien het datalek inderdaad meldingsplichtig is, dan worden de volgende acties ondernomen:
    - De FG beoordeelt samen met de directeur en betrokken medewerkers of er directe maatregelen getroffen moeten worden om schade te beperken, waaronder het doen van (een voorlopige) melding aan betrokkenen;
    - De FG beoordeelt of voor het datalek aangifte dient plaats te vinden bij de politie in geval van een mogelijk strafbaar feit (zie ook hierna onder artikel 3.4. lid 5);
    - De FG stelt in samenspraak met de directeur een communicatietraject vast richting betrokkenen en indien van toepassing verwerker.
- In geval dat het incident niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek maar van een beveiligingslek. Melding aan de AP is dan niet aan de orde. Wel kan in het overleg besloten worden, dat het zinvol is om het beveiligingslek te onderzoeken om herhaling te voorkomen.

3.4 Melden aan de Autoriteit Persoonsgegevens

- De FG verzorgt de tijdige elektronische melding bij de AP volgens het online meldingsformulier van de AP. De FG fungeert als contactpersoon inzake de communicatie naar de AP. (zie 3.1) Dit geldt ook in het geval dat nog niet duidelijk is of er sprake is van een datalek. Dan is de mogelijkheid aanwezig om na vaststelling van de aard van het incident de melding aan te vullen dan wel in te trekken.
- De directeur is eindverantwoordelijk, de FG is gedelegeerd regievoerder over de interne afhandeling van het (mogelijke) datalek.
- De AP zal na het melden van een datalek een ontvangstbevestiging sturen. Alleen indien de melding daartoe aanleiding geeft, zal de AP contact opnemen.

- De FG is verantwoordelijk voor de interne vastlegging van de melding en het administratief beheren van de ontvangstbevestiging van de AP.
- Bij een datalek als gevolg van een hack (art. 138ab van het 8 Wetboek van Strafrecht), is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico's van misbruik voor de betrokkene(n) zijn. Bij een hack ligt naast melding bij de AP, ook aangifte bij de politie in de rede in verband met de opsporing van de daders. Aangifte loopt via de directeur richting politie.

3.5 Beoordeling of datalek gemeld dient te worden aan betrokkene(n)

- Indien een datalek is gemeld aan de AP dient tevens vastgesteld te worden of het datalek ook moet worden gemeld aan degenen om wiens gegevens het gaat. Dit is ter beoordeling van en advisering door de FG aan de Directeur Bestuurder.
- De beoordeling of er sprake is van een incident dat gemeld moet worden aan de betrokkenen kan tot stand komen met behulp van pdf meldplicht datalekken AP
- Bij de beoordeling speelt onder meer een rol:

Indien SZZ passende technische beschermingsmaatregelen heeft genomen, waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, dan kan de melding aan de betrokkene(n) achterwege blijven. Bij twijfel hierover dient het datalek gemeld te worden aan de betrokkene(n).

Het datalek moet aan de betrokkene(n) worden gemeld, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. De schade kan van materiële of van immateriële aard zijn. Bij dit laatste moet bijvoorbeeld gedacht worden aan onrechtmatige publicatie, aantasting in eer en goede naam, identiteitsfraude of discriminatie. Identiteitsfraude kan overigens niet alleen leiden tot immateriële gevolgen, maar ook tot materiële gevolgen.

- De melding aan de betrokkene(n) mag achterwege blijven, als daarvoor zwaarwegende redenen aanwezig zijn. Daarbij geldt wel dat de melding aan de betrokkene alleen achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die worden genoemd in de wet. Er mag van de melding aan de betrokkene worden afgezien voor zover dit noodzakelijk is in het belang van de bescherming van de betrokkene.
- Het direct betrokken management draagt ervoor zorg dat de bij het incident betrokkenen worden geïnformeerd. De melding aan de betrokkenen bevat in ieder geval de volgende gegevens in duidelijke en eenvoudige taal:
    - De aard van de inbreuk
    - De naam en contactgegevens van de FG
    - De waarschijnlijke gevolgen van het datalek
    - De maatregelen die worden voorgesteld of genomen.

3.6 Verbetermaatregelen

- De directeur geeft opdracht tot onderzoek door de FG naar de feitelijke toedracht van het (mogelijke) datalek. Er wordt onder andere onderzocht of en zo ja hoe dergelijke incidenten

in de toekomst kunnen worden voorkomen en welke verbetermaatregelen genomen kunnen worden.

- De FG is verantwoordelijk dat de vastgestelde verbetermaatregelen worden geïmplementeerd, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering en rapporteert over de voortgang aan de directeur.
- Indien bij een verwerker verbetermaatregelen nodig zijn, dan zal de directeur daartoe opdracht geven.

3.7 Sluiten melding en vastlegging

- De FG informeert de directeur op het moment dat het datalek definitief afgehandeld is en de melding is gesloten.
- Het datalek dossier wordt digitaal door de FG gearchiveerd voor de duur van minimaal 1 jaar.
- De FG houdt een register bij van de datalekken. Alle meldingen van (potentiële) datalekken worden geregistreerd in het datalekregister, waarbij onder meer aandacht is voor de gevolgen van
- datalekken, de eventuele melding aan AP en de betrokkenen, en de reactie en preventie herstelmaatregelen die zijn genomen. De FG informeert de directeur over de voortgang van deze herstelmaatregelen.

4. BELANGRIJKE ACHTERGROND INFORMATIE

Indien niet wordt voldaan aan de meldplicht datalekken, kan een hoge boete worden opgelegd. De boetes kunnen onder meer opgelegd worden voor:

- Het niet melden van een datalek terwijl dat wel moet;
- Het niet op orde hebben van de beveiliging;
- Het verwerken van persoonsgegevens zonder toestemming.