PROCEDURE MELDPLICHT DATALEKKEN

1. Dr. L. van Londen, psychiater (verantwoordelijke) en de meldplicht datalekken

De meldplicht houdt -kort gezegd- in dat de verantwoordelijke datalekken onverwijld moet melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de natuurlijke persoon van wie persoonsgegevens zijn gelekt (de betrokkene). De meldplicht is eveneens van toepassing op de verantwoordelijke, als het datalek bij een derde is ontstaan, bijvoorbeeld een verwerker waarmee de verantwoordelijke afspraken heeft gemaakt over de verwerking van persoonsgegevens.

Het doel van deze procedure is vast te leggen welke stappen genomen moeten worden bij het vermoeden van of kennisnemen van een incident dat (mogelijk) aangemerkt kan worden als een datalek. Nagestreefd wordt het steeds volgen van een eenduidige procedure, het vaststellen van onvolkomenheden in de beveiligingsmaatregelen en het bevorderen van verbetermaatregelen.

2. Begrippen

Verantwoordelijke
De verantwoordelijke voor de gegevensverwerking en voor een juiste uitvoering van de procedure meldplicht datalekken.

Betrokkene
De natuurlijke persoon van wie persoonsgegevens worden verwerkt, en die zijn gelekt.

Datalek
Een inbreuk in verband met persoonsgegevens. Oftewel een inbreuk op de beveiliging van persoonsgegevens 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 persoonsgegevens (artikel 4 sub 12 AVG).

Het is voor de kwalificatie als 'inbreuk in verband met op de beveiliging van persoonsgegevens' niet relevant dat er boos opzet in het spel is. Hoewel een hack van systemen waarbij persoonsgegevens worden buitgemaakt een schoolvoorbeeld is van een datalek, kunnen ook gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk openstaat ook kwalificeren als een datalek. Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging geweest, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, en de preventieve maatregelen die eventueel zijn getroffen waren niet toereikend om dit te voorkomen[1].

3. Melding

3.1 Melder
3.1.1 Degene die een (mogelijk) datalek[2] constateert meldt dit per omgaande in persoon dan wel telefonisch aan de verantwoordelijke en bevestigt de melding vervolgens via mail aan de

[1] Uitleg uit: Ministerie Justitie en Veiligheid, januari 2018, Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet, p.64
[2] Bijvoorbeeld: gestolen telefoon, inbraak in computer, post is aan verkeerde personen gestuurd, verkeerde emailadressen gebruikt, gecrashte pc, gestolen laptop

verantwoordelijke. Indien de verantwoordelijke zelf het datalek constateert onderneemt deze meteen actie.
3.1.2 De melder dient in de mail nadere informatie te verstrekken omtrent het datalek. Daarbij dient de melder zo volledig mogelijk te zijn. Denk aan:
- wat is geconstateerd/gebeurd,
- om welke gegevens gaat het,
- om hoeveel gegevens gaat het,
- welke actie heeft melder eventueel zelf al genomen.

Indien de verantwoordelijke zelf het datalek heeft geconstateerd beschrijft deze zelf deze informatie over het datalek.
3.1.3 Desgevraagd dient de melder in het verdere verloop van de procedure nadere vragen te beantwoorden.

3.2 Derde
Ook (de medewerker van) een verwerker kan een (mogelijk) datalek constateren. In dat geval dient door deze derde melding te worden gedaan aan de verantwoordelijke. De stappen als genoemd in 3.1 worden vervolgens doorlopen.

4. Beoordeling, melding, bijeenkomst, onderzoek

4.1 Beoordeling aard/ernst incident
4.1.1 De verantwoordelijke zal op basis van de verkregen informatie onderzoeken of er inderdaad sprake is van een (mogelijk) datalek. Zo nodig wordt een extern deskundige ingeschakeld.
4.1.2 Daarbij hoort ook de beoordeling of er per direct maatregelen genomen moeten worden[3] om de schade te beperken, waaronder het doen van een (voorlopige) melding aan betrokkene(n) (zie hierna onder [4.2]), of dat het datalek gemeld dient te worden aan de politie (bij een vermoeden van een strafbaar feit).

4.2 Melding aan betrokkene(n)
4.2.1 Indien het datalek een hoog risico voor betrokkene(n) inhoudt dient melding aan betrokkene(n) plaats te vinden, tenzij:
a. Reeds passende organisatorische en technische beschermingsmaatregelen zijn getroffen, waardoor persoonsgegevens onbegrijpelijk zijn voor onbevoegden, zoals versleuteling,
b. Achteraf maatregelen zijn genomen om er voor te zorgen dat het bedoelde risico zich waarschijnlijk niet meer zal voordoen;
c. De mededeling aan betrokkenen onevenredig veel inspanning kost. In dat geval kan worden volstaan met een openbare mededeling op de website.
4.2.2 Indien melding aan betrokkene(n) plaats dient te vinden, dan bevat de melding in ieder geval het volgende:
a. een omschrijving van de aard van de inbreuk, en
b. contactgegevens van de verantwoordelijke waar meer informatie ingewonnen kan worden, en
c. waarschijnlijke gevolgen van de inbreuk voor betrokkene, en
d. de (voorgestelde) maatregelen die genomen zijn.

4.3 Melden aan de Autoriteit Persoonsgegevens (AP)
4.3.1 De verantwoordelijke is verantwoordelijk voor de melding aan de AP.
4.3.2 De verantwoordelijke doet melding, zo mogelijk niet later dan 72 uur na de ontdekking van het datalek, bij de AP volgens het online meldingsformulier van de AP.

[3] Kijken naar aard gegevens; bijvoorbeeld gegevens over de financiële situatie van de betrokkene, gebruikersnamen, wachtwoorden en andere inloggegevens, salaris, ziekteverzuim etc.

4.3.3 Melden aan de AP is niet vereist indien het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

4.4 Onderzoek
4.4.1 De verantwoordelijke stelt zo nodig een (intern) onderzoek in naar de feitelijke toedracht van het (mogelijke) datalek. De verantwoordelijke kan daartoe een extern deskundige inschakelen.
4.4.2 De verantwoordelijke onderzoekt verder of en zo ja hoe dergelijke incidenten in de toekomst kunnen worden voorkomen.
4.4.3 Schakelt de verantwoordelijke een extern deskundige in dan zijn diens bevoegdheden:
a. de mogelijkheid met iedereen te spreken;
b. alle relevante documenten in te zien;
c. toegang te hebben tot alle plaatsen.
Dit alles in het kader van wat de extern deskundige nodig acht ten behoeve van een zorgvuldige analyse.
4.4.4 Indien de melding is gedaan door een medewerker van een verwerker dan is tevens datgeen van toepassing wat dienaangaande in de verwerkersovereenkomst is opgenomen.
4.4.5 De verantwoordelijke streeft er naar binnen vier weken het onderzoek te hebben afgerond en het conceptrapport te hebben opgemaakt.
4.4.6 Indien een onderzoek achterwege blijft, dient de verantwoordelijke dit gemotiveerd en schriftelijk te besluiten[4].

4.5 Vaststellen verbetermaatregelen, sluiten melding, bewaren en vastlegging
4.5.1 De verantwoordelijke stelt zo nodig voorgestelde SMART geformuleerde verbetermaatregelen vast.
4.5.2 De verantwoordelijke informeert voor zover nodig en vereist betrokkene(n) over de maatregelen die zijn genomen om de inbreuk op persoonsgegevens aan te pakken.
4.5.3 Het rapport wordt digitaal gearchiveerd voor de duur van minimaal één jaar. Er kunnen redenen zijn om het rapport gedurende langere tijd te archiveren.

5. Algemene Bepalingen

5.1 Implementeren verbetermaatregelen
De verantwoordelijke is verantwoordelijk dat de vastgestelde verbetermaatregelen worden geïmplementeerd, ziet toe op de communicatie rondom en de uitvoering van de verbetermaatregelen, en zorgt dat de genomen maatregelen worden geëvalueerd op bruikbaarheid en procesverbetering.

5.2 Documenteren
Alle datalekken, alsmede de feiten en gevolgen van de inbreuk, als ook de genomen maatregelen, dienen schriftelijk vastgelegd te worden in een overzicht. De verantwoordelijke houdt dit overzicht bij.

Deze Interne Procedure Meldplicht Datalekken is vastgesteld op 14 mei 2018.

[4] Bijvoorbeeld als het datalek niet ernstig van aard is, dan wel indien melding aan de AP achterwege is gebleven.