Procedure meldplicht datalekken

Samenvatting voor medewerkers

Inhoudsopgave

1 Documentbeheer en goedkeuring 3

Versiebeheer 3

Beoordeeld door 3

Goedgekeurd door 3

2 Inleiding 4

3 Werkinstructie 5

3.1 Fase 1 - Melding en registratie 5

3.2 Fase 2 - Privacy incident / Datalek 5

3.3 Fase 3 - Evaluatie, rapportage en afwikkeling 5

4 Flowchart Meldplicht datalekken 7

5 Taken en verantwoordelijkheden binnen datalek proces 8

5.1 ICT-manager 8

5.2 Functionaris gegevens bescherming 8

1 Documentbeheer en goedkeuring

Versiebeheer

Versie	Auteur	Datum	Revisie
0.1	T. Schopman	April 2018	Samenvatting procedure meldplicht datalekken
0.2	T. Schopman	April 2018	Diverse aanpassingen
1.0	T. Schopman	Mei 2018	Definitieve versie
1.1	J. Petri	Juni 2018	Opmaak TMI stijl

Beoordeeld door

Versie	Beoordelaar	Handtekening	Datum beoordeling
0.1	J. Petri/V. Harbers		24 April 2018
0.2	J. Petri/V. Harbers		3 Mei 2018

Goedgekeurd door

Versie	Naam	Handtekening	Datum goedkeuring
1.0	J. Petri/V. Harbers		3 Mei 2018

2 Inleiding

Bij een datalek gaat het om ongeoorloofde toegang, vernietiging, wijziging of verlies van persoonsgegevens. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. We spreken pas van een datalek als er een inbreuk is gedaan op de beveiliging, zoals bedoeld in artikel 14 van de AVG.

Een datalek dient alleen gemeld te worden (bij de Autoriteit Persoonsgegevens, binnen 72 uur) als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als een aanzienlijke kans bestaat dat dit gebeurt. De Functionaris Gegevensbescherming (FG) dient over specifieke kennis van de impactbepaling, wijze van melden en afhandeling van een datalek te beschikken.

In bepaalde gevallen moet TMI ook de betrokkenen informeren over het datalek. Dat zijn de personen, zoals werknemers en klanten, van wie persoonsgegevens worden verwerkt. Ook hierbij hangt het van de ernst van het datalek af of dit wel of niet moet gebeuren. De betrokkenen worden alleen geïnformeerd als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.

3 Werkinstructie

3.1 Fase 1 - Melding en registratie

1. Medewerker constateert een (potentieel) datalek;
2. Medewerker meldt het (potentiele) datalek zo spoedig mogelijk via e-mail (fg@.nl) aan Functionaris Gegevensbescherming (Vivian Harbers en Johan Petri);
3. De melding wordt geregistreerd in Excel sheet “Registratie Datalekken”. Bij de registratie van de melding is het van belang dat FG voldoende informatie verzamelt en er prioriteit aan verbindt;

3.2 Fase 2 - Privacy incident / Datalek

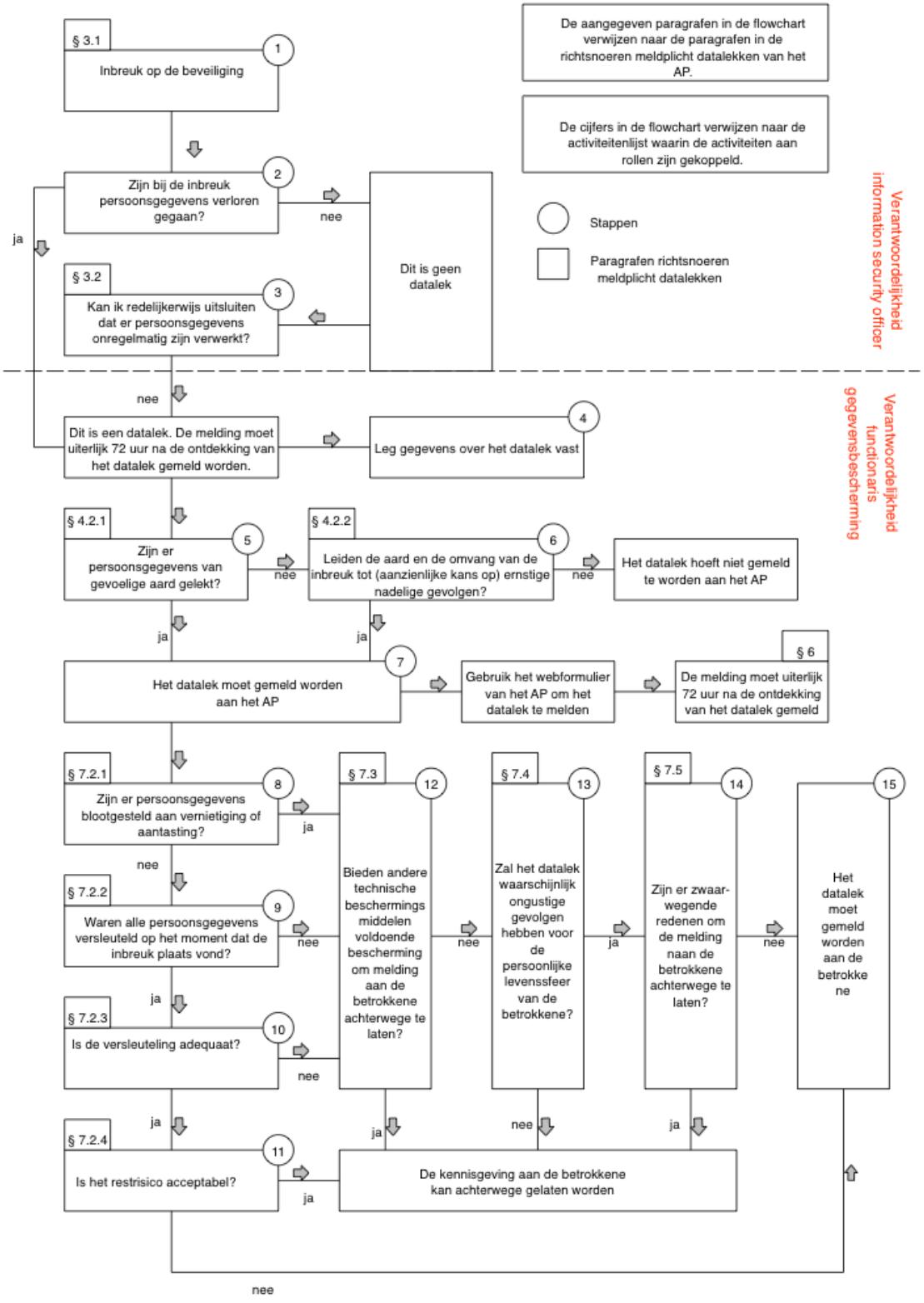
4. Bij vermoeden van een datalek roept de FG het crisisteam bij elkaar, bestaande uit de Functionaris Gegevensbescherming, de eigenaar van het getroffen bedrijfsproces of bedrijfsmiddel en de IT Manager.
5. Het crisisteam bekijkt de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is een melding aan de Autoriteit Persoonsgegevens waarschijnlijk noodzakelijk. Niet ieder datalek dient gemeld te worden aan de AP. Volgens de wet moet u een melding doen aan de AP als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
6. De meldingstermijn van 72 uur wordt scherp in de gaten gehouden.
7. Als het crisisteam tot de conclusie komt dat een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens, dan doet de Functionaris gegevens bescherming zo spoedig mogelijk melding van het datalek via het webformulier.
8. Indien niet meteen duidelijk is of de melding ook een datalek is kan er altijd een tijdelijke melding bij de Autoriteit Persoonsgegevens gedaan worden.
9. Het datalek wordt geregistreerd en de melding van het datalek bij de AP wordt opgeslagen in PDF-formaat in de Excelsheet “Registratie Datalekken”.
10. Als het crisisteam tot de conclusie komt dat de eigenaren van de persoonsgegevens eveneens op de hoogte moeten worden gebracht van het datalek dan wordt de Manager Marketing & Communicatie bijgeschakeld. Dit gebeurt tevens als er een groot datalek plaats heeft gevonden waarbij communicatie via persbericht o.i.d. noodzakelijk is.

3.3 Fase 3 - Evaluatie, rapportage en afwikkeling

1. Elk datalek wordt geëvalueerd door het crisisteam en maatregelen om herhaling te voorkomen worden besproken.
2. Elk datalek wordt aan de Finance Manager en de Directeur gerapporteerd. Hierbij worden tenminste gerapporteerd:

a. Oorzaak van het datalek
b. Omvang van het datalek
c. Melding van het datalek aan de AP en eventueel aan klanten
d. Genomen stappen om herhaling te voorkomen.

4 Flowchart Meldplicht datalekken



5 Taken en verantwoordelijkheden binnen datalek proces

5.1 ICT-manager

- Verzamelt samen met de Functionaris gegevens bescherming verdere informatie over het (mogelijke) datalek:
    - Welke gegevens zijn verloren gegaan;
    - Hoeveel gegevens zijn verloren gegaan;
    - Wat was de mate van beveiliging van de gegevens (bijv. Versleuteling, gebruik van wachtwoord, etc.);
    - Wat is de oorzaak van het datalek;

5.2 Functionaris gegevens bescherming

- Beoordeelt de verzamelde informatie om te bepalen of het een datalek betreft;
- Beoordeelt de omvang van het datalek (hoeveel gegevens);
- Beoordeelt de impact van het datalek (gevoeligheid van de gegevens);
- Beslist op basis van de informatie of een melding van het datalek aan de Autoriteit Persoonsgegevens moet plaatsvinden;
- Houdt de termijn van 72 uur in de gaten voor het doen van een melding datalek;
- Registreert elke melding aan de Autoriteit Persoonsgegevens ook intern;
- Beslist op basis van de informatie of communicatie naar betrokkenen moet plaatsvinden;
- Neemt in dat geval contact op met de Communicatie afdeling;
- Informeert bij elke melding van een datalek bij de Autoriteit Persoonsgegevens de Finance Manager en de Directeur.