

## Datalekprotocol

### 1. Inleiding

Dit document beschrijft de verschillende stappen die binnen Fruitcake BV genomen worden bij een datalek, die valt onder de Meldplicht Datalekken.

### 2. Verantwoordelijkheden

Functionaris	Verantwoordelijkheden
Directie	Aannemen en registreren van meldingen van datalekken
Directie	Melden van datalek bij Autoriteit Persoonsgegevens
Directie	Beoordelen en vastleggen van gevolgen en te nemen maatregelen
Directie	Fiatteren van maatregelen
Directie	Melden van datalekken van persoonsgegevens

### Beschrijving procedure

De meldplicht datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en treedt in werking met ingang van 1 januari 2016. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van email met emailadressen van alle geadresseerden;
- het onrechtmatige verwerking van gegevens.

### **3.1 Melden bij Autoriteit persoonsgegevens**

#### **3.1.1 Autoriteit persoonsgegevens**

Wanneer een datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen moet deze onverwijld (binnen 2 dagen) nadat de verantwoordelijke binnen Fruitcake BV er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens gemeld worden. Fruitcake BV hanteert hiervoor de door de autoriteit persoonsgegevens gestelde "Guidelines meldplicht datalekken". Wanneer het waarschijnlijk is dat een datalek ook een hoog risico oplevert voor de rechten en vrijheden van betrokkenen moet het lek ook worden gemeld bij deze betrokkenen, met behulp van de opdrachtgever. In het geval van Fruitcake BV zijn dit over het algemeen de gebruikers van de systemen van de opdrachtgever van het specifieke project. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer. Een verwerker is verplicht om een datalek te melden bij de verantwoordelijke.

1. Verantwoordelijke: directie Fruitcake BV. De verantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De verantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten);
2. Verwerker: degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen (ook extern). De verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. De verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.

### **3.2 Stappenplan intern melden**

#### **3.2.1 Stap 1: Melden van datalek**

Alle datalekken van persoonsgegevens moeten intern worden gemeld aan directie en worden gedocumenteerd door directie. De melding kan door iedere medewerker en iedere verwerker worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van Fruitcake BV. De melding moet direct worden gedaan bij de directie en schriftelijk worden vastgelegd. Buiten kantoor tijden is de directie bereikbaar.

De directie legt vast:

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

### **3.2.2 Stap 2: Inventariseren gevolgen en te nemen maatregelen**

Na ontvangst van een melding datalek wordt door de directie van Fruitcake BV beoordeeld en vastgelegd:

- de noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- hetgeen gemeld gaat worden bij de Autoriteit Persoonsgegevens door directie (naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records);
- de mogelijke gevolgen voor de betrokkenen;
- de maatregelen die Fruitcake BV neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
- de maatregelen die betrokkenen kunnen 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(-en) en teamleider(s);
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit Fruitcake BV of wanneer er onvoldoende maatregelen zijn getroffen om ongeregelheden te voorkomen. Indien gewenst vindt overleg plaats met de juridisch adviseur;
- hetgeen intern gecommuniceerd wordt, op welk moment;
- hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden;
- of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd worden;



- op welke wijze er intern wordt gerapporteerd, inclusief actiehouder;
- of eventuele schade is gedekt door de verzekeringspolis.

### 3.2.3 Stap 3: Fattering

De directie accordeert de uit te voeren activiteiten, zoals vastgesteld, of stelt de uit te voeren activiteiten bij. De door de directie vastgestelde activiteiten worden uitgevoerd.

### 3.2.4 Stap 4: Melding bij Autoriteit Persoonsgegevens

De directie meldt binnen 2 dagen het datalek bij de Autoriteit Persoonsgegevens. In ieder geval zal gemeld moeten worden:

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

### 3.2.5 Stap 5: ontvangstbevestiging Autoriteit Persoonsgegevens

Is er een melding gedaan, dan ontvangt Fruitcake BV een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met Fruitcake BV om de herkomst van de melding te verifiëren.