PROTOCOL DATALEKKEN

Melden incident

De meldplicht datalekken geldt voor de gehele organisatie en iedere medewerker. Iedere medewerker die te maken heeft met vermissing/diefstal van zaken die van Greenflash Internet of haar opdrachtgevers zijn, of met een informatiebeveiligingsincident, dient dit te melden bij de directie in de persoon van de heer Rob Naaijkens. Dit kan telefonisch via 06 81473817 of via e-mail: rob.naaijkens@greenflashinternet.nl

De melder wordt verzocht zijn/haar naam en contactgegevens te verstrekken, samen met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en voor een eventuele melding aan de AP.

Indien de melder twijfelt of er sprake is van een incident of wat hij moet doen, kan hij de directie raadplegen.

Registratie

De directie registreert de incidentmelding. De directie analyseert of er bij het incident persoonsgegevens betrokken zijn. Indien de melding telefonisch is gedaan, vraagt de directie dit na bij de melder.

Nadat telefonisch contact heeft plaatsgevonden, stuurt de melder aanvullend een e-mail met de inhoud van de melding. In die e-mail worden de volgende vragen beantwoord:

1. Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?

   Vermeld hier ook de naam van het betrokken systeem.

2. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?

   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.

3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?

   Geef a.u.b. een minimum en maximum aantal personen.

4. Omschrijving groep personen om wiens gegevens het gaat.

   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.

5. Zijn de contactgegevens van de betrokken personen bekend?

   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?

6. Wat is de oorzaak van het beveiligingsincident?

   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?

   Geef dit a.u.b. zo specifiek mogelijk aan.

Beoordelen of er sprake is van een datalek

Zo snel mogelijk na de melding van een incident beoordeelt de directie of er sprake is van een datalek dat valt onder de meldplicht van de AVG.

De directie stuurt een e-mail met een gemotiveerde beoordeling en een advies van het incident aan de directie. Indien de directie beoordeelt dat het incident geen datalek in de zin van de AVG betreft, dan zorgt de directie ervoor dat de beoordeling schriftelijk wordt teruggekoppeld aan de melder en de directie. Is het incident wel een datalek in de zin van de AVG, dan zal de directie de melding bij de toezichthouder (Autoriteit Persoonsgegevens) doen.

De directie is er verantwoordelijk voor dat het meldingsformulier van de toezichthouder wordt ingevuld en vervolgens wordt toegestuurd aan de toezichthouder. De melding dient door alle betrokken medewerkers direct en met hoogste prioriteit te worden opgepakt.

De directie houdt een register bij waarin alle datalekken die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.

Beslisboom voor de melding aan toezichthouder

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat alleen een inbreuk hoeft te worden gemeld als deze leidt tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen. Hierbij spelen de volgende factoren een rol:

1) Zijn er persoonsgegevens van gevoelige aard gelekt? Het betreft hier een incident waarbij bijzondere persoonsgegevens zoals medische/politiegegevens, gegevens over gezondheid, ras of religie of financiële gegevens zijn gelekt.

2) Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu? Naarmate er meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

Er moet in ieder geval gemeld worden als één van onderstaande vragen positief wordt beantwoord.

Zijn gegevens (definitief) verloren gegaan?

Ja → melden

Zijn de gegevens bijzonder of zeer omvangrijk?

Ja → melden

Zijn de gegevens in onbevoegde handen geraakt?

Ja → melden

Aanzienlijk risico op schade aan persoonlijke levenssfeer?

Ja → melden

Nee op alle vragen →niet melden

Mogelijk is op het moment dat er gemeld moet worden nog geen volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval vindt de melding plaats op basis van de gegevens waarover Greenflash Internet op dat moment beschikt. Eventueel kan de melding naderhand nog worden aangevuld of zelfs worden introkken.

Melden aan betrokkene?

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van de datalek. Indien er sprake is van een datalek moet deze aan de betrokkene worden gemeld, als de inbreuk een hoog risico brengt op schade aan diens persoonlijke levenssfeer. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld.

Voor de beoordeling of aan de betrokkene(n) gemeld moet worden, zijn de volgende vragen van belang.

Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?

Nee → Melden

Zijn de gegevens versleuteld of ontoegankelijk voor degene die geen recht op inzage heeft in deze gegevens?

Nee → Melden

Artikel 34(3) van de AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is. Dit geldt in de volgende situaties:

1. Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens vooraf aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.
3. Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

Termijn van melden

Voor het melden van een datalek aan betrokkenen geldt dat dit ‘onverwijld’ moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Gelet hierop dient een datalek binnen 72 uur te worden gemeld aan de toezichthouder.

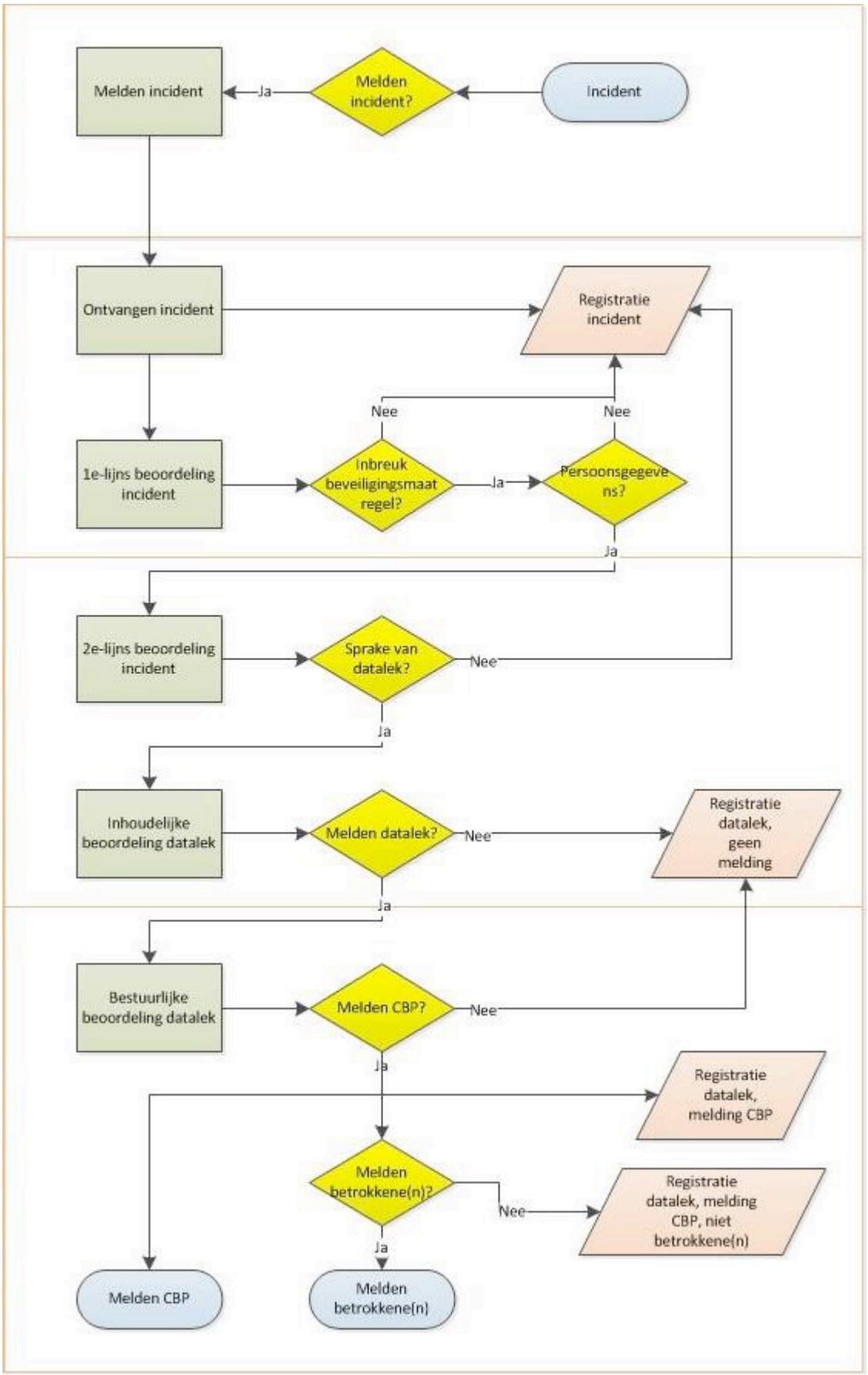
Melden aan andere partijen?

Indien sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) zal Greenflash Internet moeten beoordelen of een datalek-incident aan de externe partij gemeld moet worden. Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn.

Bij de uitwerking van de communicatiestrategie vindt afstemming plaats welke doelgroepen/ overige partijen worden geïnformeerd over het datalek en op welke wijze.

AFHANDELEN MELDING

De directie houdt een register bij van de meldingen van datalekken. In dit register verwerkt zij de interne en externe meldingen.


Melden incident
Ja
Melden incident?
Incident
Ontvangen incident
Registratie incident
Nee
Nee
1e-lijns beoordeling incident
Inbreuk beveiligingsmaatregel?
Ja
Persoonsgegevens?
Ja
2e-lijns beoordeling incident
Sprake van datalek?
Nee
Ja
Inhoudelijke beoordeling datalek
Melden datalek?
Nee
Registratie datalek, geen melding
Ja
Bestuurlijke beoordeling datalek
Melden CBP?
Nee
Ja
Registratie datalek, melding CBP
Melden betrokkene(n)?
Nee
Registratie datalek, melding CBP, niet betrokkene(n)
Ja
Melden CBP
Melden betrokkene(n)