Hekkelman advocaten | notarissen

Stappenplan procedure meldplicht datalekken

Vanaf 1 januari 2016 geldt de meldplicht datalekken voor iedere organisatie. Bij het invoeren van een procedure voor deze meldplicht kan de onderstaande checklist een hulpmiddel zijn.

Inbreuk op de beveiliging

Zijn persoonsgegevens verloren gegaan of is sprake van onrechtmatige verwerking (beveiligingsincident)?

- Vernietiging of verlies (brand datacenter,ongewild verwijderen van een bestand zonder back-up)
- Aantasting, onbevoegde kennisneming, onjuiste verstrekking (verloren USB stick, gestolen laptop, malware, hack, e-mail naar verkeerde ontvanger)

Incidentenbeheer

Detecteren van beveiligingsincidenten

Geautomatiseerde controle op hacks, malware e.d.

Melden van ieder intern beveiligingsincident bij een vast aanspreekpunt.

- Bijvoorbeeld een team van een IT specialist, een jurist en een PR medewerker
- Zorg voor interne procedures en training/awareness

Afspraken over melden van externe beveiligingsincidenten

- Bij wie en hoe snel moeten bewerkers beveiligingsincidenten melden?
- Controle op de naleving

Onderzoeken van het incident

Wat is precies met de gegevens gebeurd?

Wat is de aard van de getroffen persoonsgegevens?

- Bijzondere persoonsgegevens: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond en strafrechtelijke gegevens.

- Persoonsgegevens van gevoelige aard: financieel of economisch (schulden), stigmatiserend (verslaving, naaktfoto's, specifieke problemen), inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude (kopie ID, BSN, handtekening, biometrische gegevens), gegevens die vallen onder beroepsgeheim.

Hekkelman advocaten | notarissen

Wat is de omvang van het incident?

- Aantal getroffen personen.
- Hoeveelheid gegevens per getroffen persoon.
- Worden de getroffen gegevens binnen een keten gedeeld?

Wat is de impact op de betrokkenen (klanten/prospects/personeel)?

- Is sprake van kwetsbare groepen (kinderen, zieken, verstandelijk beperkten, bedreigde personen)?
- Is er kans op financieel nadeel?

Repareren van de inbreuk

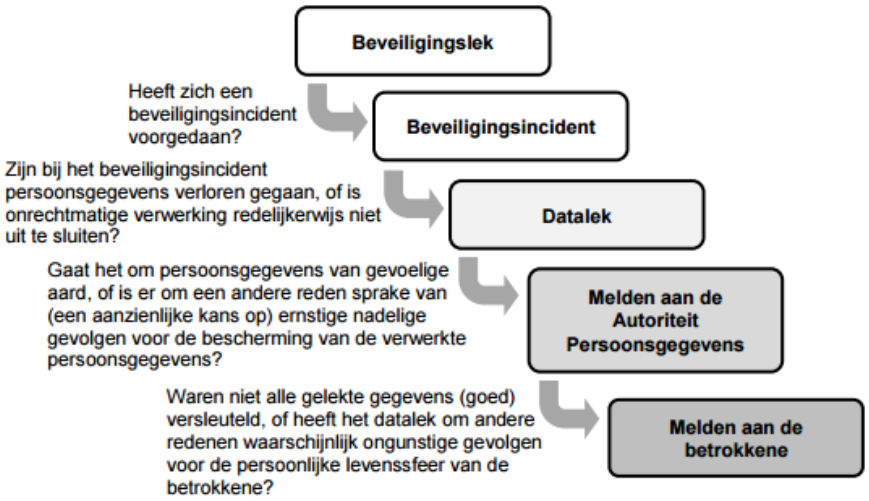
Maatregelen treffen om de gevolgen van het incident te beperken.

Voorkomen van soortgelijke incidenten in de toekomst.

Meldplicht Autoriteit Persoonsgegevens

Melden is verplicht indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Zelf afwegen aan de hand van de aard van de gegevens, de omvang van het incident en de impact op de betrokkenen (zie hiervoor bij onderzoeken van het incident). Daarbij kan het beslisschema uit de Beleidsregels meldplicht datalekken handig zijn:



Hekkelman advocaten | notarissen

'Onverwijld': binnen 72 uur - daarna kan de melding evt. aangevuld of ingetrokken worden.

Via het meldloket datalekken van de Autoriteit Persoonsgegevens (AP)

Informeren betrokkenen

De personen die zijn getroffen door het datalek dienen te worden geïnformeerd indien de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer.

Alleen in geval van meldplicht AP.

Informeren hoeft niet indien de getroffen persoonsgegevens onbegrijpelijk of ontoegankelijk zijn gemaakt (versleuteling of remote wissen)

- Bij vernietiging (geen back-up) of aantasting (wijziging) van gegevens helpen deze beschermingsmaatregelen niet.
- Alle persoonsgegevens moeten zijn versleuteld op moment van de inbreuk.
- De versleuteling moet adequaat zijn (standaardalgoritme, sleutel niet gelekt en toekomstvast) - check publicaties ENISA (EU Agency for Network and Information Security) en NCSC (Nationaal Cyber Security Centrum).

Afweging ongunstige gevolgen persoonlijke levenssfeer.

- Kan betrokkene last krijgen van de inbreuk, materiële of immateriële schade lijden (aard gegevens, impact, kwetsbare groep)?
- Kan betrokkene zichzelf beter beschermen als hij de inbreuk kent?

Bij zwaarwegende belangen kan informatie aan betrokkenen achterwege blijven.

AP kan alsnog verlangen dat betrokkenen worden geïnformeerd.

De informatie moet betrokkenen in staat stellen om de inbreuk op hun persoonlijke levenssfeer zoveel mogelijk te beperken

Registratie beveiligingsincidenten

Overzicht bijhouden van alle incidenten die gemeld moeten worden aan het AP. Bewaar het overzicht minimaal één jaar en bij niet informeren betrokkenen drie jaar.

Communicatie en reputatie

Denk na over de wijze van communiceren met betrokkenen en de pers.
Hoe kan worden omgegaan met signalen van buitenaf over een mogelijk datalek?
Is het inschakelen van externe deskundigen gewenst?

Verzekering meldplicht datalekken of cyberverzekering

Let op dekking voor aansprakelijkheidstelling door derden, 'eigen kosten' (kosten onderzoek, PR, informeren klanten, evt. opzetten klanten call center, inschakelen experts) en boetes.

Monique Hennekens

Hekkelman Advocaten N.V.
T 024 - 382 83 29
M 06 - 281 393 87
m.hennekens@hekkelman.nl