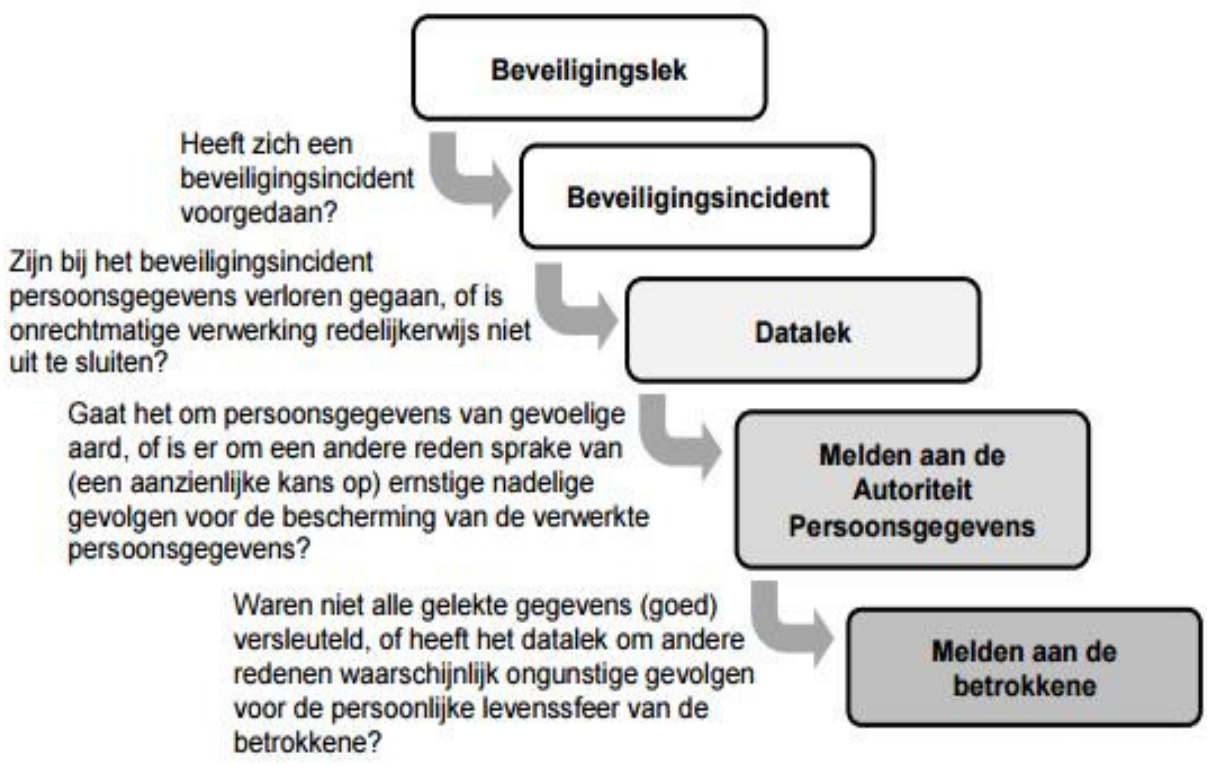
Stappenplan beoordeling meldplicht datalekken
Checklist 2

Als de eerste contactpersoon een geconstateerde of gemeld beveiligingsincident aan de hand van de "Vragenlijst meldplicht datalekken eerste contactpersoon" heeft geregistreerd kan de informatie door naar de persoon of het team dat het incident beoordeelt.

Aan de hand van de informatie over een beveiligingsincident moet worden beoordeeld of i) het incident gemeld moet worden aan de Autoriteit Persoonsgegevens en ii) de betrokkenen geïnformeerd moeten worden. Daarvoor is dit stappenplan bedoeld. Deze is opgesteld aan de hand van de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens (AP). Een melding moet zonder onnodige vertraging (in ieder geval binnen 72 uur na de ontdekking van het incident) gedaan worden via het meldloket.

Beslisschema AP

In dit schema van de AP staan de afwegingen schematisch weergegeven:



Stappenplan beoordeling meldplicht datalekken

STAP 1: Moet het beveiligingsincident gemeld worden aan de AP?

1. Zijn persoonsgegevens verloren gegaan?

Vernietiging, verlies of onbereikbaarheid van de gegevens zonder dat er een complete en actuele back-up of kopie beschikbaar is van de gegevens.

2. Zijn persoonsgegevens onrechtmatig verwerkt?

Aantasting van de gegevens, onbevoegde kennisneming, wijziging of onjuiste verstrekking (bijv. ransomware of cryptoware, e-mail naar verkeerde ontvanger, gestolen laptop).

Als het antwoord op één van deze vragen **JA** is, dan moet verder gegaan worden met de beoordeling.

Let op: bij een hack of diefstal ook aangifte doen bij de politie.

Is het antwoord **NEE**, dan is geen sprake van een datalek en hoeft niet gemeld te worden.

3. Zijn persoonsgegevens van gevoelige aard gelekt?

Bijzondere gegevens: godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond, strafrechtelijke gegevens en gegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod (bijv. straatverbod wegens stalken).

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

Als het antwoord op deze vraag **JA** is dan zal moeten worden gemeld aan de AP. Ga dan door naar **STAP 2**.

Is het antwoord **NEE**, ga dan verder met de beoordeling (zie ook pagina's 27 en 28 van de beleidsregels).

Stappenplan beoordeling meldplicht datalekken

4. Wat is de omvang van het incident?

Hoe groot is het aantal getroffen personen (meer dan 1.000?)

Hoeveel gegevens zijn per getroffen persoon gelekt (meerdere gegevens per persoon betekent vaak meer nadeel en langer last voor de persoon)

Zijn de beslissingen die kunnen worden genomen aan de hand van de gegevens ingrijpend voor betrokkenen (worden de gegevens bijv. gebruikt om financiële beslissingen met betrekking tot die persoon te nemen)

Worden de getroffen gegevens binnen een keten gedeeld (zoals bij een overheid, waardoor het voor betrokkenen lastiger is om zich te onttrekken aan de gevolgen)

5. Wat is de impact op de betrokkenen (cliënten/medewerkers/overig)

Is sprake van kwetsbare groepen (kinderen, zieken, verstandelijk beperkten, bedreigde personen)

Is er kans op financieel nadeel voor betrokkenen

Beoordeel aan de hand van de antwoorden op voorstaande vragen of een aanzienlijke kans op ernstig nadelige gevolgen is te verwachten.

zo **JA:** dan moet gemeld worden aan de AP en ga dan door naar STAP 2.

zo **NEE**: registreer dan de afwegingen die zijn gemaakt.

STAP 2: Moeten de getroffen betrokkenen worden geïnformeerd?

Uitsluitend indien wordt geoordeeld dat er moet worden gemeld bij de AP zal moeten worden beoordeeld of de betrokkenen moeten worden geïnformeerd. Het criterium is dat berokkenen moeten worden geïnformeerd indien het datalek **waarschijnlijk ongunstige gevolgen** zal hebben voor de persoonlijke levenssfeer. Zie ook schema pagina 34 van de beleidsregels.

Stappenplan beoordeling meldplicht datalekken

1. Zijn de getroffen persoonsgegevens adequaat onbegrijpelijk of ontoegankelijk zijn gemaakt?

Waren alle persoonsgegevens versleuteld op moment van de inbreuk?

Is de versleuteling adequaat (standaardalgoritme, sleutel niet gelekt en toekomstvast) - check bijv. publicaties ENISA (EU Agency for Network and Information Security) en NCSC (Nationaal Cyber Security Centrum)
o Is het restrisico acceptabel?

Is het antwoord op deze vragen JA dan hoeven betrokkenen niet te worden geïnformeerd.

2. Zijn de persoonsgegevens vernietigd (geen actuele back-up) of aangetast (wijziging of vermenging)?

Is het antwoord op deze vraag JA dan helpt versleuteling niet en zal door moeten worden gegaan met de beoordeling.

3. 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

Is het antwoord op deze vraag JA dan zullen betrokkenen moeten worden geïnformeerd. De informatie moet betrokkenen in staat stellen om de inbreuk op hun persoonlijke levenssfeer zoveel mogelijk te beperken

NB: Alleen bij zwaarwegende belangen kan informatie aan betrokkenen alsnog achterwege blijven. Indien betrokkenen niet worden geïnformeerd zou de AP alsnog kunnen verlangen dat betrokkenen toch worden geïnformeerd op basis van de melding aan de AP.

Hekkelman

Hekkelman advocaten | notarissen

Stappenplan beoordeling meldplicht datalekken

Meer weten?

Inhouse cursus volgen?

of één van de lunchsessies bij
Hekkelman advocaten en notarissen bijwonen?

Neem contact met op Monique Hennekens:

m.hennekens@hekkelman.nl

024-382 83 29