

Procedure meldplicht datalekken

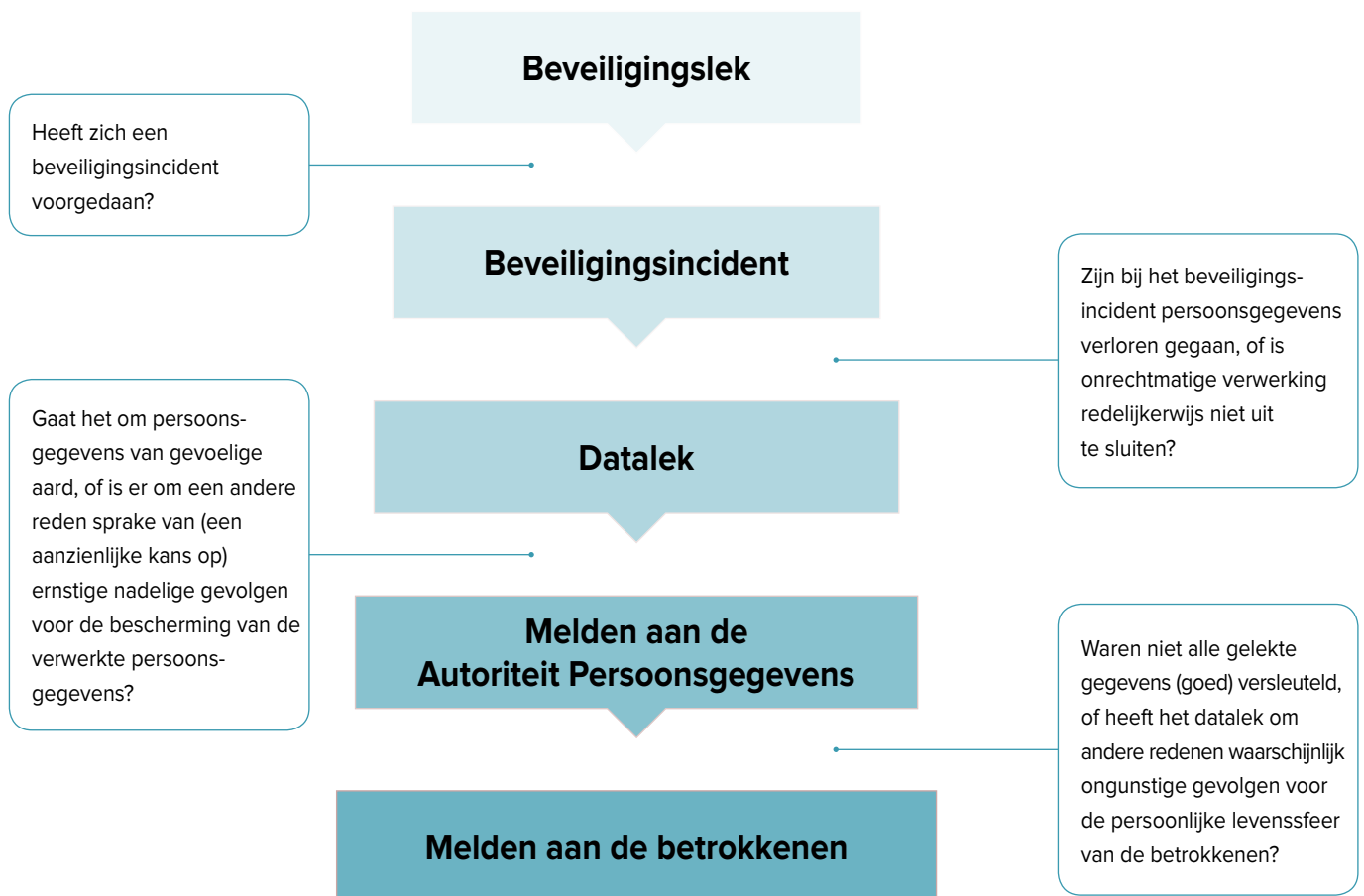
Procedure meldplicht datalekken

Sinds 1 januari 2016 geldt de meldplicht datalekken. Dit betekent dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. In sommige gevallen moet dit datalek ook aan de betrokkenen (mensen van wie de persoonsgegevens zijn gelekt) worden gemeld.

Deze meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. Wel stelt de AVG strengere eisen aan de eigen registratie van de data-lekken die zich binnen je organisatie hebben voorgedaan. Zo moeten alle datalekken worden gedocumenteerd, zodat de AP kan controleren of je aan deze meldplicht hebt voldaan. De Autoriteit Persoonsgegevens heeft 'beleidsregels meldplicht datalekken' opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de AP en eventueel aan de betrokkenen.

Afwegingen

Er dienen een aantal afwegingen gemaakt te worden bij de beslissing of een gebeurtenis die zich heeft voorgedaan gemeld moet worden aan de Autoriteit Persoonsgegevens en eventueel ook aan de betrokkenen. Deze afwegingen zie je in onderstaand schema.



Schema uit 'De meldplicht datalekken in de Wbp' door de Autoriteit Persoonsgegevens.

Datalek

Heeft zich daadwerkelijk een beveiligingsincident voorgedaan? Dan is er sprake van een datalek. Een datalek is de inbreuk op de beveiliging van persoonsgegevens. Dit betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen had getroffen. Als er alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek.

Voorbeelden van een datalek:

- Gestolen werkapparaten, zoals je werklaptop;
- Een kwijtgeraakte USB-stick met persoonsgegevens;
- De verzending van een e-mail met onbeveiligde bestanden met persoonsgegevens in bijv. de bijlage;
- Het verstrekken van een wachtwoord aan een derde;
- Een inbraak door een hacker;
- Een besmetting met ransomware als er geen bruikbare back-up kan worden teruggezet.

Melden aan de Autoriteit Persoonsgegevens

Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als dit lek 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. Een belangrijke factor die hierbij een rol speelt, is de aard van de gelekte persoonsgegevens. Als hier persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk. Persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

Persoonsgegevens van gevoelige aard zijn bijvoorbeeld:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 9, lid 1 AVG. Iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.
- Gegevens over de financiële of economische situatie van de betrokkene zoals schulden en salarisgegevens.
- Gegevens die kunnen leiden tot uitsluiting van de betrokkene, bijvoorbeeld gegevens over verslavingen, schoolprestaties of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens.
- Gegevens die kunnen worden gebruikt voor (identiteits)fraude zoals BSN-nummers en biometrische gegevens.

Factoren zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie persoonsgegevens zijn gelekt, kunnen ook aanleiding zijn om het datalek te melden. De melding moet zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek worden gedaan.

Melden aan de betrokkenen

Een datalek moeten melden bij de Autoriteit Persoonsgegevens betekent niet automatisch dat dit datalek ook gemeld moet worden aan de betrokkenen. Dit hoeft namelijk pas als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkenen. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Als er bijzondere persoonsgegevens zijn gelekt, dan kun je er in principe van uit gaan dat het datalek ook gemeld moet worden aan de betrokkenen.

Hoe eerder de betrokkenen worden geïnformeerd, hoe beter. Door de melding van het datalek onverwijld te doen, stel je de betrokkenen in staat om zo snel mogelijk maatregelen te nemen om zich te beschermen tegen de gevolgen van het datalek.

Bij passende technische en organisatorische beveiligingsmaatregelen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, is het niet nodig de betrokkenen te informeren.

Stappenplan Procedure meldplicht datalekken

Wanneer moet je een datalek nu concreet melden bij de Autoriteit Persoonsgegevens?

Volg de 5 stappen:

STAP 1 • Persoonsgegevens

Zijn de gegevens die gelekt zijn aan te merken als persoonsgegevens?

Een gegeven is een persoonsgegeven als deze redelijkerwijs, zonder onevenredige inspanning, te herleiden is naar een individueel persoon. Doeltreffende technische en organisatorische maatregelen kunnen het mogelijk maken de gegevens te anonimiseren. Er is dan geen sprake van een datalek.

Ja Ga naar STAP 2

Nee Je hoeft geen melding te doen

STAP 2 • Verantwoordelijke/verwerker

Zijn het de eigen gegevens die gelekt zijn?

De verwerkingsverantwoordelijke is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Ja Ga naar STAP 3 • (verantwoordelijke)

Nee De verwerkingsverantwoordelijke moet melding doen • (verwerker) De meldplicht datalekken stelt dat de verwerkingsverantwoordelijke melding van het datalek moet doen bij de Autoriteit Persoonsgegevens. Als verwerker heb je echter wel de verantwoordelijkheid om de verantwoordelijke binnen redelijke termijn op de hoogte te stellen van het datalek.

STAP 3 • Datalek?

Aan de hand van 3 vragen wordt bepaald of er sprake is van een datalek.

Vraag 3.1 • Is er sprake van een inbreuk op de beveiliging?

Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan. Er is geen sprake van een dreiging of tekortkoming in de beveiliging, maar er heeft zich daadwerkelijk een beveiligingsincident voorgedaan. De preventieve beveiligingsmaatregelen waren niet voldoende om dit tegen te houden.

Ja Ga naar vraag 3.2 • (wel inbreuk) Het is een beveiligingslek. Is het ook een datalek?

Nee Je hoeft geen melding te doen • (geen inbreuk) Dit is geen datalek.

Vraag 3.2 • Zijn er persoonsgegevens verloren gegaan?

Bij het beveiligingsincident zijn persoonsgegevens vernietigd of op een andere manier verloren gegaan en we beschikken niet over een complete en actuele back-up van de gegevens.

Ja Ga naar STAP 4 • (wel verloren) Dit is een datalek.

Nee Ga naar vraag 3.3 • (niet verloren) Er kan toch sprake zijn van een datalek.

Vraag 3.3 • Kan er worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt?

Onrechtmatige vormen van verwerking zijn: aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

Ja Je hoeft geen melding te doen • (kan uitgesloten worden) Dit is geen datalek.

Nee Ga naar STAP 4 • (kan niet uitgesloten worden) Dit is een datalek.

STAP 4 • Melding Autoriteit Persoonsgegevens

Aan de hand van 2 vragen wordt bepaald of het datalek moet worden gemeld bij de Autoriteit Persoonsgegevens.

Vraag 4.1 • Zijn er bijzondere persoonsgegevens gelect?

Ja Ga naar STAP 5 • Dit moet gemeld worden bij de Autoriteit Persoonsgegevens.

Nee Ga naar vraag 4.2

Vraag 4.2 • Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

De aard en omvang van de getroffen verwerking is mede bepalend voor de beantwoording van de vraag of er bij een datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens.

Ja Ga naar STAP 5 • Dit moet gemeld worden bij de Autoriteit Persoonsgegevens.

Nee Dit datalek hoeft NIET gemeld te worden aan de Autoriteit Persoonsgegevens

STAP 5 • Melding betrokkenen

Aan de hand van 3 vragen wordt bepaald of het datalek moet worden gemeld aan de betrokkenen.

Vraag 5.1 • Heeft het datalek ongunstige gevolgen voor het privéleven van de betrokkenen?

Het datalek moet aan de betrokkenen worden gemeld als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Zo kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens belangen worden geschaad. Dit kan zowel van materiële of immateriële aard zijn.

Ja Ga naar vraag 5.2

Nee Dit datalek hoeft NIET gemeld te worden aan de betrokkenen

Vraag 5.2 • Zijn de gelecte persoonsgegevens dusdanig beveiligd dat ze niet gelezen of gebruikt kunnen worden?

Ja Ga naar vraag 5.3

Nee Dit datalek moet WEL gemeld worden aan de betrokkenen

Vraag 5.3 • Is de manier waarop de encryptie (beveiliging) ongedaan gemaakt kan worden bekendgemaakt?

Ja Dit datalek moet WEL gemeld worden aan de betrokkenen

Nee Dit datalek moet WEL gemeld worden aan de Autoriteit Persoonsgegevens maar NIET aan de betrokkenen