

Protocol Melding Datalekken Paques

Algemeen

Paques heeft dit protocol opgesteld in het geval van (een vermoeden van) een datalek. Van een datalek is volgens de Algemene verordening gegevensbescherming (AVG) sprake als er onbedoeld toegang mogelijk is tot persoonsgegevens, of als er persoonsgegevens worden verloren, vernietigd, gewijzigd of vrijkomen zonder dat dit is beoogd. Het gaat daarbij om een inbreuk op de beveiliging van persoonsgegevens. De Autoriteit Persoonsgegevens noemt als voorbeelden van een datalek het verlies van een USB-stick met niet-versleutelde persoonsgegevens, een cyberaanval waarbij persoonsgegevens zijn buitgemaakt of een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Interne Melding aan Privacy Officer Paques

Bij constatering van een data-lek of een vermoedelijk data-lek moet dat direct worden gemeld aan de Privacy Officer van Paques, Bart Commijs. Dit kan door een mail te sturen aan privacyofficer@paques.nl en/of telefonisch: 06-57 089 791.

De melding moet tenminste de volgende gegevens bevatten:

- de aard van de inbreuk (dus: wat is er gebeurd?)
- de oorzaak van het data-lek (hack, diefstal, verlies, etc.)
- de beschrijving van de gelekte persoonsgegevens (aard van de gegevens, hoeveelheid, etc.)
- de eventuele maatregelen die genomen zijn/worden genomen om het data-lek te dichten
- en een inschatting van het risico dat de betrokkenen kunnen lopen met de tevens de contactgegevens van de melder

De interne meldplicht aan de Privacy Officer geldt niet alleen voor medewerkers van Paques, maar ook voor leveranciers en partners van Paques, voor zover die leveranciers of partners persoonsgegevens van Paques verwerken.

Een verwijzing naar dit Protocol Melden Datalekken dient opgenomen te worden in de verwerkersovereenkomst met de betreffende leveranciers en partners.

Melding door Privacy Officer aan AP en betrokkenen

De Privacy Officer onderzoekt naar aanleiding van de interne melding of er sprake is van een datalek. Zo ja, dan meldt de Privacy Officer het datalek 'onverwijld' (uiterlijk op de tweede werkdag na het ontstaan van het incident) aan het Meldpunt Datalekken van de

AP. Deze melding wordt gedaan via het op de website van de AP gepubliceerde meldformulier.

De Privacy Officer informeert de afdeling Marketing en Communicatie, de RvB en, afhankelijk van de aard van de inbreuk, de overige relevante afdelingen (ICT en/of HR en/of het betreffende onderdeel van de lijnorganisatie) over het data-lek en de melding aan de AP.

De Privacy Officer stelt vervolgens in overleg met de relevante afdelingen vast of het data-lek een 'aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene(n) zijn verbonden' tot gevolg heeft. Als daar sprake van is, dienen de betrokkenen geïnformeerd te worden over het datalek.

De melding aan betrokkenen is niet nodig indien de persoonsgegevens versleuteld of onbegrijpelijk zijn gemaakt waardoor deze niet te lezen zijn door anderen. Dit moet van geval tot geval beoordeeld worden omdat de effectiviteit van de versleuteling mede afhangt van (i) het gebruikte algoritme en (ii) het moment / punt waarop de gegevens zijn versleuteld.

De berichtgeving aan betrokkenen kan door plaatsing van een bericht op de website van Paques en/of via een brief aan betrokkenen, een en ander ter beoordeling van de Privacy Officer en de afdeling Marketing en Communicatie.

De kennisgeving aan betrokkenen moet in ieder geval de volgende informatie bevatten:

- de aard van de inbreuk in verband met persoonsgegevens
- een telefoonnummer of webpagina waar meer informatie over de inbreuk kan worden verkregen
- aanbevelingen om mogelijke negatieve gevolgen van de inbreuk voor betrokkenen te beperken.

Bijhouden Overzicht

De Privacy Officer houdt een overzicht bij van de datalekken, met daarin onder meer de gevolgen van de datalekken en de herstelmaatregelen