

Protocol bij beveiligingsincidenten persoonsgegevens of een datalek

Inleiding

In dit protocol worden de activiteiten beschreven die de Verwerker dient uit te voeren in geval van een beveiligingsincident persoonsgegevens of een (mogelijk) Datalek.

Definities

Autoriteit Persoonsgegevens: de Autoriteit Persoonsgegevens (AP) is de Nederlandse gegevensbeschermingsautoriteit en het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

Beleidsregels: de opgestelde beleidsregels voor toepassing van de AVG.

Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

Verwerker: verwerker in de zin van de AVG.

Datalek: een inbreuk op de beveiliging van Persoonsgegevens die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Functionaris Gegevensbescherming: de Functionaris Gegevensbescherming (FG) is iemand die binnen een bedrijf of organisatie verantwoordelijk is voor naleving van de regelgeving die voortvloeit uit de (AVG).

Incident: een inbreuk op de beveiliging van persoonsgegevens waarvan nog moet worden vastgesteld of deze leidt tot de aanzienlijke kans op ernstige, nadelige gevolgen, dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Verantwoordelijke: de verantwoordelijke voor de verwerking in de zin van de AVG.

AVG: de Algemene Verordening Gegevensbescherming.

Functionaris Gegevensbescherming

De Verwerker heeft een Functionaris Gegevensbescherming aangesteld. Deze Functionaris Gegevensbescherming is bij de Autoriteit Persoonsgegevens bekend onder nummer FG012236.

Meldingsprocedure

Wanneer zich een Incident of een Datalek voordoet bij de Verwerker, meldt de Verwerker het Incident of Datalek onmiddellijk bij de Verantwoordelijke.

De melding door Verwerker bevat de volgende informatie:

1. de aard van het Incident of Datalek;

2. de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
3. de geconstateerde en vermoedelijke gevolgen van het Incident of Datalek voor de verwerking van persoonsgegevens;
4. de maatregelen die zijn getroffen om de gevolgen te verhelpen of te matigen.

Eventuele vragen van de Verantwoordelijke als gevolg van de melding, worden door Verwerker beantwoord.

De volgende informatie wordt door Verwerker schriftelijk vastgelegd en schriftelijk gemeld aan Verantwoordelijke:

- a) vragen van de Verantwoordelijke inclusief bijbehorende antwoorden van Verwerker;
- b) informatie die door Verwerker wordt verkregen gedurende de afhandeling en oplossing van het Incident of Datalek;
- c) de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Incident of Datalek te beperken en herhaling te voorkomen;
- d) de mededeling dat het Incident of Datalek is opgelost.

De Verantwoordelijke zal een Datalek zelf melden bij de Autoriteit Persoonsgegevens.

Evaluatie

Na het afhandelen van het Incident of Datalek vindt een evaluatie plaats ter beoordeling of aanvullende beheersmaatregelen moeten worden getroffen. De resultaten van de evaluatie worden schriftelijk vastgelegd.