Procedure Meldplicht Datalekken van Heilige Oda parochie

Doel van deze procedure is op een juiste wijze om te gaan met de gevolgen van een datalek. Aan de hand van een stappenplan wordt bepaald of er gemeld moet worden en hoe dit moet gebeuren. Deze procedure is bedoeld voor medewerkers van Heilige Oda parochie, zodat zij op de hoogte zijn hoe te handelen ingeval van (vermoeden van) een datalek.

1. Inleiding

Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Ook als er goede technische en organisatorische beschermingsmaatregelen zijn genomen, kan er sprake zijn van een datalek. Het kan hier gaan om een kwijtgeraakte USB-stick of een gestolen laptop met persoonsgegevens, maar ook om een inbraak in een datasysteem of per ongeluk verstrekte toegang tot gegevens aan personen of instanties die daartoe geen toegang zouden mogen hebben. Het verzenden van een e-mail aan een adressenbestand waarin alle e-mailadressen voor iedereen zichtbaar zijn is ook al een datalek.
Een datalek moet mogelijk worden gemeld bij de Autoriteit Persoonsgegevens (AP) en soms ook aan de betrokkene.

Criterium melding AP: een datalek moet worden gemeld, tenzij het niet waarschijnlijk is dat de datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Hiervan is volgens de AP sprake in de volgende gevallen:

- Als het gaat om persoonsgegevens van gevoelige aard;
- Er is om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens.

Criterium melden bij betrokkene: de inbreuk heeft een hoog risico voor de rechten en vrijheden van natuurlijke personen. Hiervan is volgens de AP sprake in de volgende gevallen:

- De gelekte gegevens zijn niet (goed) versleuteld,
- De gevolgen voor betrokkenen kunnen niet meer worden ingeperkt;
- Het datalek heeft om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene.

2. Procedure

Als er een datalek is ontstaan (of het vermoeden daarvan) dan moet dit direct gemeld worden bij de persoon die binnen onze organisatie de contactpersoon is als het gaat om het verwerken van persoonsgegevens: Peter van den Boogaard, penningmeester.

Vervolgens worden de volgende stappen doorlopen:

1. De verantwoordelijke neemt indien nodig direct technische en/of organisatorische maatregelen om de schade van een datalek zo veel mogelijk te beperken
2. De verantwoordelijke binnen de organisatie informeert het bestuur
3. Inwinnen benodigde feitelijke informatie betreffende het (veronderstelde) datalek en/of beveiligingsinbreuk. Dit kan met behulp van de volgende vragen:
    a. Wat is de aard van de inbreuk? Gaat het om verlies van een USB-stick, verlies laptop, of een hack?
    b. Op welk type informatie heeft de inbreuk betrekking: cliëntendossiers, vrijwilligersgegevens, personeelsgegevens, of een combinatie?

   c. Betreft het uitsluitend gegevens van een overleden cliënt? – er is geen sprake van een datalek, tenzij er ook gegevens van nabestaande zijn gelekt
   d. Van hoeveel betrokkenen is er (mogelijk) informatie gelekt en hoe gevoelig is deze informatie? Gaat het bijvoorbeeld 'slechts om e-mailadressen of 'zijn mogelijk medische dossiers gelekt.
4. Als de omstandigheden daar aanleiding toegeven: extern advies inwinnen
5. Een risicoanalyse maken met de betrekking tot de ernst van de situatie
6. Vaststellen of de datalek moet worden gemeld bij de AP
7. Vaststellen of er voldoende grond is om de datalek te melden bij betrokkenen.

Voor het maken van een analyse en belangenafweging kan gebruikt gemaakt worden van de beslisboom op de volgende website: https://www.it-jurist.nl/nieuws/beslisboom-datalekken

3. Melding van een datalek

Indien melding bij de AP vereist is, doet Heilige Oda parochie dit zonder onredelijke vertraging en in ieder geval binnen 72 uur na ontdekking van het datalek via het meldpunt datalekken AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

De melding omvat de volgende punten:

- De aard en omvang van de inbreuk;
- waar mogelijk de categorieën van betrokkenen, de persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en contactgegevens van de contactpersoon waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die Heilige Oda parochie heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Heilige Oda parochie meldt datalekken aan betrokkene(n) indien het datalek een hoog risico inhoudt voor betrokkene(n). Indien melding wordt gedaan aan een betrokkene, bevat deze melding de volgende punten:

- een omschrijving van de aard van het datalek;
- de naam en contactgegevens van de Functionaris voor Gegevensbescherming of ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het datalek;
- de maatregelen die Heilige Oda parochie heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4 Registratie datalek

Heilige Oda parochie registreert alle datalekken die plaatsvinden, ook de datalekken die niet aan de Autoriteit Persoonsgegevens gemeld moeten worden. Bij de lekken die niet gemeld worden, wordt beargumenteerd waarom dit niet gebeurd is.

Dit protocol is opgesteld op 9 september2018