Datalek Protocol Van Tilburg - Bastianen Groep

Inleiding

Van Tilburg - Bastianen Groep B.V. (en alle onderliggende juridische entiteiten; hierna: TB) moet aan de meldplicht datalekken voldoen. In dit protocol wordt weergegeven hoe gehandeld dient te worden in geval van een datalek en een beveiligingsincident. Elke medewerker binnen TB dient op de hoogte te zijn van dit protocol en conform dit protocol te handelen in geval van een datalek. Meer informatie is te vinden in het AVG beleid van TB.

Onder datalek wordt verstaan:

Van een datalek is sprake:

- als persoonsgegevens op ongeoorloofde wijze in de openbaarheid komen, bijvoorbeeld omdat derden er toegang toe hebben gekregen
- als persoonsgegevens ongewenst zijn veranderd
- als persoonsgegevens ongewenst verloren zijn gegaan

Er zijn dus drie categorieën:

1. inbreuk op de vertrouwelijkheid: deze gegevens zijn openbaar geworden
2. inbreuk op de integriteit: deze gegevens zijn gewijzigd terwijl dit niet de bedoeling was
3. inbreuk op de beschikbaarheid: er is sprake van verlies of vernietiging of er is geen toegang tot deze gegevens meer

Heb je een datalek geconstateerd? Neem dan de volgende stappen:

1. Direct (dus zonder vertraging) contact opnemen met de Privacy Officer Ton van Oosten. 06-27098853 / privacy@tb.nl.
2. Geef daarbij een zo compleet mogelijke beschrijving van het datalek:
    a. geef op waar het incident om gaat
    b. datum en tijdstip van het incident
    c. gaat het om gelekte of vernietigde gegevens?
    d. is duidelijk wie er toegang heeft gehad tot de gegevens?
    e. etc.
3. Blijf beschikbaar voor eventuele vragen en beantwoord deze met spoed.

Stappenplan

1.a.Vormen (crisis) responsteam

Uitgangspunt is dat een datalek van eenvoudige aard door de Privacy Officer wordt afgehandeld.

Als het datalek ernstig is qua aard en mogelijke gevolgen voor de betrokkenen wordt een team geformeerd met daarin de volgende functies:

- CFO / directeur: voorzitter
- IT Manager
- Marketing Manager
- Privacy Officer

Daarnaast kan afhankelijk van de aard van het datalek het responsteam aangevuld worden met relevante functies. De Groepsdirectie zal van een ernstig incident op de hoogte worden gebracht.

De voorzitter van het responsteam belegt indien wenselijk de vergaderingen waarbij de eerste prioriteit is gericht op:

1. het onderzoek naar de feiten die relevant zijn voor de vraag of TB een meldplicht heeft bij de Autoriteit Persoonsgegevens (hierna: AP) en benadeelden.
2. de wenselijke te nemen acties die erop gericht zijn om de gevolgen van het datalek te beperken.
3. desgewenst krijgen medewerkers een instructie omtrent het incident en hoe in het geval te handelen. In ieder geval wordt voor elke vorm van externe communicatie cf. het beleid van TB verwezen naar het responsteam die een woordvoerder aanwijst.

1.b. Registratie in register van alle incidenten

Tussentijds draagt de Privacy Officer er zorg voor dat het incident in het incidentenregister van TB wordt vastgelegd. Het register wordt indien nodig tussentijds aangevuld met relevante feiten.

2. Melden datalek

Indien er sprake is van een datalek in de zin van de AVG zal de Privacy Officer van TB -na overleg met de directie- ervoor zorg dragen dat deze binnen 72 uur na kennisname aan de Autoriteit Persoonsgegevens via de website van de AP wordt gemeld. Deze termijn wordt niet onderbroken door feestdagen dan wel het weekend. De voorzitter van het responsteam kan bij de melding betrokken worden.

Ook indien nog niet alle gegevens binnen 72 uur zijn verzameld, zal de melding worden gedaan, deze melding wordt tijdig aangevuld. Ook is het mogelijk om de melding in te trekken.

3. Melden betrokkenen / communicatie

Indien op basis van de feiten blijkt dat betrokkenen door het incident waarschijnlijk een hoog risico (op misbruik) lopen, zal TB deze betrokkenen hiervan op de hoogte brengen. Ook in dit geval vindt eerst overleg plaats met de directie. De communicatie functionaris bereidt de nodige communicatie uitingen voor die aan het respons team en zo nodig ook aan de directie worden voorgelegd. Het responsteam bepaalt op advies van de communicatie functionaris op welke manier zal worden gecommuniceerd (intranet, website TB, persoonlijk bericht, etc.).

De directie beslist (op advies van het responsteam) welke stakeholders op de hoogte zullen worden gesteld. Daarnaast wordt uit het responsteam een eerste aanspreekpunt voor de AP aangewezen. Alle berichten van de AP zullen in dat geval direct aan de deze functionaris worden doorgestuurd.

4. Evaluatie / verbeteren

Het responsteam draagt er zorg voor dat er een evaluatie plaats vindt, waarbij de volgende vragen kunnen worden beantwoord:

1. Welke verbeterpunten kunnen in processen worden doorgevoerd om het datalek in de toekomst te voorkomen ?
2. Heeft het responsteam haar taken adequaat uitgevoerd waardoor bijvoorbeeld de gevolgen van het datalek zijn beperkt? Heeft TB tijdig aan de verplichtingen uit hoofde van de meldplicht voldaan, etc. ?

Indien relevant worden actiepunten benoemd met een actiehouder die binnen een nader overeen te komen periode worden opgevolgd. De opvolging van deze actiepunten wordt door het responsteam gemonitord en indien relevant aan de directie gerapporteerd.