Datalekprotocol CodeIQ

1. Inleiding

Dit document beschrijft de procedure die CodeIQ hanteert bij een datalek, zoals vereist onder de Meldplicht Datalekken van de Algemene Verordening Gegevensbescherming (AVG).

2. Verantwoordelijkheden

Functionaris	**Verantwoordelijkheden**
Directie	Ontvangen en registreren van meldingen over datalekken
Directie	Melden van datalekken aan de Autoriteit Persoonsgegevens
Directie	Evalueren van gevolgen en vastleggen van te nemen maatregelen
Directie	Goedkeuren en coördineren van uit te voeren maatregelen
Directie	Informeren van betrokkenen in geval van een ernstig risico voor de privacy

3. Beschrijving van de procedure

Een datalek betreft een inbreuk op de beveiliging van persoonsgegevens, waarbij de gegevens worden blootgesteld aan verlies of onrechtmatige verwerking. Datalekken kunnen ontstaan door:

- Opzettelijke acties (zoals hacking, phishing, identiteitsfraude);
- Technische storingen (bijv. netwerkuitval, IT-storingen);
- Menselijke fouten (bijvoorbeeld verkeerde ontvangers, eenvoudige wachtwoorden);
- Calamiteiten (brand, waterschade);
- Verlies van apparaten (zoals USB-sticks, laptops);
- Fouten in communicatie (bijv. e-mails met open CC-lijsten).

3.1 Melden bij de Autoriteit Persoonsgegevens

Indien een datalek een risico vormt voor de rechten en vrijheden van betrokkenen, moet dit binnen 72 uur na constatering worden gemeld aan de Autoriteit Persoonsgegevens. CodeIQ volgt hiervoor de “Guidelines Meldplicht Datalekken” van de Autoriteit Persoonsgegevens.

Indien een hoog risico voor betrokkenen wordt vermoed, moeten ook de betrokkenen worden geïnformeerd.

3.2 Interne Meldprocedure

Stap 1: Interne Melden van een Datalek

Alle medewerkers en verwerkers zijn verplicht om datalekken direct te melden aan de directie. Deze melding moet gedocumenteerd worden en bevat in ieder geval:

- Naam van de melder;
- Datum en tijd van de melding;
- Aard van de inbreuk;
- Welke persoonsgegevens zijn betrokken;
- Aantal gegevensrecords en/of betrokken personen;
- Gedane en geplande acties door de melder;
- Verwachte gevolgen voor betrokkenen;
- Contactpersoon voor verdere afhandeling.

Stap 2: Evalueren van Gevolgen en Maatregelen

Na ontvangst van een melding beoordeelt de directie:

- Te nemen vervolgstappen, zoals verdere beveiliging of extra logging;
- Inhoud van de melding aan de Autoriteit Persoonsgegevens, indien van toepassing;
- Potentiële gevolgen voor betrokkenen;
- Aanbevelingen voor betrokkenen om mogelijke schade te beperken;
- Interne afhandeling en communicatie naar alle relevante partijen;
- Potentiële aansprakelijkheden en mogelijke betrokkenheid van derde partijen;

- Noodzaak voor een juridische en/of externe adviseur.

Stap 3: Goedkeuring

De directie accordeert de geadviseerde acties en neemt zo nodig extra maatregelen voordat deze worden uitgevoerd.

Stap 4: Melding bij Autoriteit Persoonsgegevens

Binnen 72 uur doet de directie melding van het datalek bij de Autoriteit Persoonsgegevens. In de melding worden ten minste de volgende elementen opgenomen:

- Aard van de inbreuk en betrokken categorieën van personen;
- Beschrijving van verwachte gevolgen;
- Maatregelen die CodeIQ heeft getroffen of zal treffen;
- Aanbevelingen voor betrokkenen om verdere schade te voorkomen;
- Contactinformatie voor betrokkenen.

Stap 5: Ontvangstbevestiging

CodeIQ ontvangt een bevestiging van de melding van de Autoriteit Persoonsgegevens. In gevallen waarbij verdere actie door de Autoriteit vereist is, volgt mogelijk nader contact.