

IZEBOUD Z♥RG

Zorg vanuit ons hart

MELDPLICHT DATALEKKEN:

1. Inleiding:

F. Izeboud Beheer B.V. (verder te noemen Izeboud Beheer) wil zorgvuldig omgaan met de gevoelige gegevens van cliënten en medewerkers. Cliënten en medewerkers hebben er recht op dat de informatie die gebruikt wordt ten behoeve van hun herstel/ontwikkeling vertrouwelijk wordt behandeld en zo veel mogelijk wordt beschermd tegen datalekken. Het is en blijft echter een risico wat niet ten allen tijde kan worden voorkomen.

2. Doel:

De procedure meldplicht datalekken is opgesteld op basis van de Wet Bescherming Persoonsgegevens (WBP). Deze meldplicht houdt in dat bedrijven en overheden direct een melding moeten doen bij de Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens (CBP)) zodra zij een ernstig datalek hebben.

De meldplicht datalekken is 1 januari 2016 in werking getreden.

3. Definitie datalek:

Bij een datalek gaat het om toegang tot persoonsgegevens of vernietiging, wijziging of vrijkomen van gegevens zonder dat dat de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook het onrechtmatig verwerken van gegevens. Er is sprake van een datalek als er inbreuk is op de beveiliging zoals bedoeld in artikel 13 van de WBP.

4. Overtreding meldplicht datalekken:

Indien een datalek ten onrechte niet wordt gemeld bij de Autoriteit Persoonsgegevens dan kan deze een aanzienlijk hoge geldboete geven. De maximale geldboete is tot 820.000 EURO of, als dat niet passend is 10% van de netto jaaromzet van de rechtspersoon. Bij een overtreding van de WBP wordt een bestuurlijke boete van de 2e categorie opgelegd met een maximum van 500.000 EURO.

5. Melden datalekken:

1. Registreren van het geconstateerde datalek:

- Bij het ontdekken van een datalek wordt deze direct en zonder aarzeling gemeld aan de DGA. Deze behandelt het gemelde beveiligingsincident onmiddellijk als code rood. Hij beoordeelt het gemelde incident.

2. Beoordeling datalek:

- De directie besluit of het beveiligingsincident gemeld moet worden aan de Autoriteit Persoonsgegevens.
- Een datalek hoeft alleen gemeld te worden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als een aanzienlijke kans bestaat dat dit gebeurt.
- Bij een meldingsplicht dient het datalek te worden gemeld middels het formulier “Meldloket datalekken” dat te vinden is op de website van de Autoriteit Persoonsgegevens.

3. De DGA besluit of het datalek gemeld moet worden aan de betrokkenen:

- De betrokkenen, cliënten en/of medewerkers, hoeven alleen geïnformeerd te worden als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.
- De melding aan de betrokkenen mag eventueel achterwege gelaten worden als er passende technische beschermingsmaatregelen zijn getroffen, waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden door bijvoorbeeld goede encryptie.

4. Het beoordelen van de noodzaak om maatregelen te treffen:

- Als de oorzaak bekend is, wordt bekeken of het noodzakelijk is om corrigerende maatregelen te treffen. De beslissing om te komen tot corrigerende maatregelen dient beoordeeld te worden tijdens het vaste teamoverleg of tussentijds in overleg met de DGA en de Raad van Commissarissen.

5. Het vaststellen en doorvoeren van de benodigde maatregelen:

- Het vaststellen van de benodigde maatregelen wordt vastgelegd in notities, e-mails/brieven, notulen, verslagen, procedures of rapporten.
- Alle betrokkenen worden geïnformeerd en verzocht te handelen zoals de maatregel aangeeft.

6. Het beoordelen van de getroffen maatregelen:

- Afhankelijk van de uitslag van de beoordeling wordt vastgesteld of een herbeoordeling noodzakelijk is, of er wederom maatregelen genomen moeten worden, of dat de maatregel voldoende is geweest. Verificatie van de doeltreffendheid van maatregelen wordt gedaan bij het vaststellen van de doeltreffendheid van de afgehandelde actiepunten.

Sanctiebeleid:

Sancties zoals bepaald in de arbeidsovereenkomst als onderdeel van de geheimhoudingsverklaring voor met name bewuste acties die de organisatie schaadt zijn o.a. ontslag op staande voet en/of het verhalen van de gevolgschade op de betrokkenen.