Procedure meldplicht datalekken

Stichting 1Thuis

September 2019
Versie 1.0

Doel

De procedure meldplicht datelekken is opgesteld op basis van de Algemene verordening gegevensbescherming (AVG). Deze meldplicht houdt in dat bedrijven en overheden direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) (voorheen College bescherming persoonsgegevens (CBP)) zodra zij een ernstig datalek hebben. De meldplicht datalekken is 1 januari 2016 inwerking getreden.

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.

Overtreding meldplicht datalekken

Indien een datalek ten onrechte niet wordt gemeld bij de Autoriteit Persoonsgegevens dan kan die 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 AVG wordt een bestuurlijke boete van de 2e categorie opgelegd met een maximum van 500.000 EURO.

Melden datalekken

1. *Registreren van het geconstateerde datalek:*

Het datalek wordt als incident geregistreerd middels een incidentmelding en wordt direct doorgegeven aan de directie en kwaliteitsmedewerker. De directie beoordeelt het gerapporteerde beveiligingsincident in samenspraak kwaliteitsmedewerker.

2. *De directie besluit of het datalek 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 directie besluit of het datalek gemeld moet worden aan de betrokkenen (werknemer/cliënt):*

De betrokkenen 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 wordt uitgevoerd door directie in samenwerking met de kwaliteitsmedewerker:*

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 de vaste overleggen of tussentijds in overleg met de directie.

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

6. 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/per direct de opdracht intrekken bij de ZZP-er en/of het verhalen van de gevolgschade op de betrokken personeelsleden/opdrachtnemer. Sancties m.b.t. slecht omgaan met bedrijfsmiddelen (zoals bepaald in het bedrijfsreglement) zijn gericht op het verhalen van de reparatiekosten aan de bewuste persoon/personen.

Indien werkzaamheden worden uitbesteed aan derden dan wordt er met deze leveranciers / freelancers een verwerkingsovereenkomst afgesloten.