Protocol meldplicht datalekken

Dit protocol is van toepassing op alle vestigingen van Home Instead Thuisservice en integraal onderdeel van het Privacybeleid.

Op grond van de Algemene Verordening Gegevensbescherming (AVG) geldt een meldplicht datalekken. In dit protocol wordt omschreven wat de meldplicht datalekken inhoudt en welke stappen ondernomen moeten worden om daaraan te voldoen.

Definitie datalek

Een datalek is een inbreuk op de beveiliging die per ongeluk, of op onrechtmatige wijze, tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins als verwerkte gegevens leidt.

Het kan 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 voorbeeld van een datalek.

Als er sprake is van een datalek met ernstige gevolgen voor betrokkene moet de verwerkingsverantwoordelijke het datalek verplicht melden aan de Autoriteit Persoonsgegevens en in sommige gevallen ook aan de betrokkene zelf.

Mededeling aan de Autoriteit Persoonsgegevens (AP)

Verplichte mededeling	Als het datalek een risico met zich meebrengt voor de rechten en vrijheden van de betrokkene(n). *Bij twijfel, raadpleeg hoofdstuk IV van de Guidlines meldplicht datalekken.*
Niet verplichte mededeling	Als het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. *Bij twijfel, raadpleeg hoofdstuk II van de Guidlines meldplicht datalekken.*
Hoe	Via het online Meldloket van de Autoriteit Persoonsgegevens.
Termijn	Uiterlijk binnen 72 uur nadat het datalek is ontdekt, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene(n). Is de melding niet binnen 72 uur, dan moet bij de melding een motivatie worden gevoegd voor de vertraging.
Welke informatie	▪ De contactgegevens van de organisatie, melder, contactpersoon en functionaris voor gegevensbescherming. ▪ Gegevens over het datalek (o.a. tijdlijn en aard van inbreuk). ▪ De persoonsgegevens die betrokken zijn bij het datalek; ▪ De betrokkene(n) ▪ De maatregelen die zijn getroffen voordat het datalek plaatsvond. ▪ De gevolgen van het datalek. ▪ De vervolgacties naar aanleiding van het datalek.

Registratieplicht	De mededeling moet worden gedocumenteerd in het eigen datalekregister.

Mededeling aan de betrokkene(n)

Verplichte mededeling	Als het datalek waarschijnlijk een hoog risico inhoud voor de rechten en vrijheden van de betrokkene(n). *Bij twijfel, raadpleeg hoofdstuk IV van de Guidlines meldplicht datalekken.*
Niet verplichte mededeling	▪ Als de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen heeft genomen om de persoonsgegevens vóór inbreuk te beschermen, met name maatregelen die de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling. ▪ Als de verwerkingsverantwoordelijke onmiddellijk na inbreuk maatregelen heeft genomen om ervoor te zorgen dat he hoge risico voor de rechten en vrijheden van de betrokkene(n) zich waarschijnlijk niet meer zal voordoen. ▪ Het onevenredige inspanningen zou vergen om contact op te nemen met de betrokkene(n). In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij de betrokkene(n) even doeltreffend worden geïnformeerd. *Bij twijfel, raadpleeg hoofdstuk III van de Guidlines meldplicht datalekken.*
Hoe	Per specifiek bericht, dus niet samen met andere informatie. • E-mail • Per post • Bericht op de website (extra, nooit alleen)
Termijn	Per omgaande (zo snel mogelijk)
Welke informatie	▪ Een beschrijving van de aard van de inbreuk. ▪ De naam en contactgegevens van de contactpersoon en/of functionaris voor gegevensbescherming. ▪ Een beschrijving van de waarschijnlijke gevolgen. ▪ Een beschrijving van de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen heeft om het datalek aan te pakken, met inbegrip van, in voorkomend geval, maatregelen om de mogelijke nadelige gevolgen te beperken.
Registratieplicht	De mededeling moet worden gedocumenteerd in het eigen datalekregister.

N.B. Niet ieder beveiligingsincident is per definitie een datalek. Er dient sprake ten zijn van een daadwerkelijk beveiligingsincident, waarbij de preventieve maatregelen die zijn getroffen niet voldoende waren om het te voorkomen. Wanneer er alleen sprake is van een dreiging of van een beveiligingslek die zou kunnen leiden tot een datalek, is er dus nog geen sprake van een datalek.

Home Instead
Thuisservice

Stroomschema meldplicht datalekken

N.B. In dit stroomschema is ervan uitgegaan dat het vermoedelijk datalek door of bij de franchiseondernemer is ontdekt. Als het vermoedelijk datalek door of bij de franchisegever wordt ondekt, dan neemt de PO de plek in van de LPO.