



Cadanz Welzijn
SAMEN. LEVEN. DOEN. EEMSDelta.

DATALEKPROCEDURE

Datalekprocedure Cadanz Welzijn

Inleiding

Cadanz Welzijn is een organisatie die bijzondere persoonsgegevens verwerkt. Het kenmerk van bijzondere persoonsgegevens is dat deze privacygevoelige informatie bevatten en misbruik hiervan mogelijk nadelig kan zijn voor de betrokkene. De wet schrijft voor dat verlies of vernietiging van deze gevoelige gegevens gesignaleerd en de oorzaak ervan onderzocht moeten worden.

Wanneer er inderdaad gevoelige gegevens op straat zijn komen te liggen of verloren zijn gegaan, moet hiervan een melding worden gedaan aan de Autoriteit Persoonsgegevens (AP).

Als het aannemelijk is dat de betrokkene schade kan hebben van het inzien van zijn/haar gegevens door anderen, moet ook de betrokkene hiervan in kennis worden gesteld.

Beveiligingsincidenten en datalekken

Voorbeelden van een beveiligingsincident of datalek zijn;

- ❖ inbraak in computers of een registratiesysteem waarbij mogelijk gevoelige gegevens waren in te zien;
- ❖ een persoon heeft zonder toestemming ingelogd met een wachtwoord van een ander persoon en heeft daarbij mails en andere informatie kunnen lezen;
- ❖ verlies van een papieren dossier, een USB-stick met privacygevoelige gegevens, een laptop;
- ❖ een notitie met naam en adresgegevens die in een openbare ruimte of bij de printer is blijven liggen.

Stroomschema melding

De Wet Bescherming Persoonsgegevens (WBP) hanteert onderstaand stroomschema om te bepalen of een datalek gemeld moet worden aan de AP en aan betrokkene.



Procedure binnen Cadanz Welzijn

Cadanz Welzijn hanteert de volgende procedure in geval van datalekken:

- ❖ de functionaris gegevensbescherming is het eerste aanspreekpunt bij datalekken. Bij afwezigheid is de Privacy Officer de eerste vervanger;
- ❖ melden van een beveiligingsincident of datalek kan via fg@cadanzwelzijn.nl of via telefoonnummer 06-55822928;
- ❖ een (vermoedelijk) beveiligingsincident of datalek moet zo spoedig mogelijk gemeld worden. Een eventuele melding aan de AP moet namelijk binnen 72 uur na ontdekking worden gedaan;
- ❖ de functionaris gegevens bescherming (FG) registreert de melding in een incidenten registratie;
- ❖ de functionaris gegevensbescherming onderzoekt de melding samen met de Privacy Officer;
- ❖ voor meer informatie over het incident kan eventueel contact worden opgenomen met de melder;
- ❖ na analyse van de melding stelt de FG de verwerkingsverantwoordelijke (directeur-bestuurder) in kennis van het incident en geeft dan aan of het gemeld moet worden aan de AP;
- ❖ de functionaris gegevensbescherming (of diens vervanger) doet de melding aan de AP;
- ❖ betreft het een inbraak in het computersysteem dan wordt direct ICT ingeschakeld om passende maatregelen te nemen;
- ❖ er wordt intern onderzoek gedaan naar het incident en actie ondernomen om soortgelijke incidenten in de toekomst te voorkomen;
- ❖ de actie/ opvolging wordt geregistreerd in de incidenten registratie.

Een medewerker van Cadanz Welzijn meldt een beveiligingsincident of data lek aan de FG bij:

- ❖ verlies van een laptop, telefoon of USB-stick;
- ❖ verlies van een papieren dossier of bij het vermoeden van ontvreemde papieren of kopieën uit een dossier;
- ❖ het vermoeden van inbraak of ongeoorloofde inzage in de laptop of kantoorssystemen;
- ❖ ongeoorloofde toegang tot kantoor waarbij men in kasten met dossiers heeft kunnen kijken;
- ❖ twijfel of iets een mogelijk beveiligingsincident of data lek kan zijn.