PROTOCOL MELDING DATALEKKEN voor ZorgPlus V.O.F.

Dit protocol beschrijft de procedure met daarin te nemen maatregelen die binnen ZorgPlus genomen moeten worden bij een datalek volgens de meldplicht datalekken van de Algemene Verordening gegevens-bescherming (AVG). De meldplicht data-lekken is een onderdeel in de AVG. De AVG treedt in werking op 25-05-2018.

Reikwijdte van de meldplicht datalekken
Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens als bedoeld in de AVG die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens dan wordt dit als een datalek gekwalificeerd en zal dit bij de Autoriteit Personengegevens moeten worden gemeld. Er moet dus sprake zijn van het 'lekken van data' en dat het lekken een onbedoelde of onwettige vernietiging, verlies of wijziging van, of een niet geautoriseerde toegang tot verwerkte persoonsgegevens tot gevolg heeft.
Een enkele tekortkoming of kwetsbaarheid in de beveiliging is geen datalek. Dit is wel het geval wanneer redelijkerwijs niet kan worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid.

Datalekken kunnen ontstaan door:
- • moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- • technisch falen (ICT-storingen);
  • menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega’s en externen);
- • calamiteit (brand datacentrum, wateroverlast);
- • verloren USB stick of laptop;
- • verzenden van email met emailadressen van alle geadresseerden;
- • maar ook het onrechtmatige verwerking van gegevens (DDS applicatie aantekening VOA).

Meldingen
Een datalek kan door een medewerker of een bewerker van ZorgPlus worden ontdekt. Deze ontdekking wordt aan de directie medegedeeld die vervolgens over zal gaan tot de beoordeling of er sprake is van een datalek. De directie onderzoekt het incident. Hierbij is aandacht voor de volgende aspecten:
1 Bewerker is degene die de gegevens ten behoeve van ZorgPlus verwerkt zonder aan haar rechtstreeks gezag te zijn onderworpen (ook extern). De bewerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van ZorgPlus. Het is daarom belangrijk om goede afspraken te maken en deze vast te leggen in een bewerkersovereenkomst zodat de bewerker ZorgPlus tijdig en adequaat informeert over alle relevante incidenten.
- a. wat is de aard van het datalek (bijzondere of gevoelige gegevens dienen per definitie te worden gemeld) ;
- b. wat is de oorzaak dat dit incident heeft plaatsgevonden;
- c. is er sprake van het niet nakomen van of een tekortkoming in de beveiligingsprocedures;
- d. is de organisatie verwijtbaar.

Indien sprake is van een datalek dan zal de directie binnen 2 dagen maar niet later dan 72 uur na ontdekking zorg dragen voor een melding bij de Autoriteit Persoonsgegevens.
Verder zal de directie van ZorgPlus een overzicht bijhouden van alle datalekken binnen ZorgPlus.
Per datalek wordt in het overzicht aangegeven wat de feiten en gegevens zijn van de aard van de inbreuk.
Een datalek wordt voor minimaal 1 jaar in het overzicht bewaard. Na de melding datalek ontvangt ZorgPlus

een ontvangstbevestiging van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens zal contact met ZorgPlus opnemen mocht na een melding aanleiding zijn om nadere te ondernemen.
Hierbij zal met name de herkomst van de melding worden geverifieerd en kan ZorgPlus aanwijzingen van de Autoriteit Persoonsgegevens krijgen.
Wanneer vaststaat dat een datalek bij de Autoriteit Persoonsgegevens gemeld moet worden dan dient hierna beoordeeld te worden of een datalek ook aan betrokkene moet worden gemeld. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. In het geval van ZorgPlus zijn de betrokkenen over het algemeen de cliënten. Ook medewerker van ZorgPlus kan als betrokkene worden aangemerkt indien het om persoonsgegevens gaat van die medewerker.
Een betrokkene moet ook onverwijld in kennis worden gesteld van de inbreuk. Indien de inbreuk waarschijnlijk geen ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene of wanneer de technische beschermingsmaatregelen (bijvoorbeeld encryptie) die zijn genomen voldoende bescherming bieden, kan melding van het datalek aan de betrokkene achterwege blijven.

Taken, verantwoordelijkheden en bevoegdheden

1. Iedere medewerker of bewerker van ZorgPlus die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden de directie van ZorgPlus.
2. De directie van ZorgPlus is verantwoordelijk voor het onderzoeken van het incident;
3. De directie is verantwoordelijk voor de beoordeling of een datalek aan de Autoriteit Persoonsgegevens gemeld moet worden respectievelijk of een datalek aan de betrokkene moet worden gemeld;
4. De Directie is verantwoordelijk voor de melding van datalekken bij de Autoriteit Persoonsgegevens;
5. De directie is verantwoordelijk voor het bijhouden van een overzicht van alle datalekken die onder de meldplicht vallen voor minimaal 1 jaar;
6. De Directie is verantwoordelijk voor het ondernemen van preventieve, preparatoire en repressieve maatregelen.

Interne controle

1. De directie analyseert jaarlijks de meldingen datalekken en stelt indien nodig een verbeterplan ter voorkoming van datalekken.
2. De directie beoordeelt minimaal jaarlijks of de procedure en de uitvoering van dit protocol nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure geactualiseerd moet worden of dat medewerkers geïnstrueerd moeten worden op een juiste toepassing van het protocol.

Opgemaakt op 26-04-2018 door de directie van ZorgPlus V.O.F.:

R.H.J.A. Hieltjes