Meldingsprotocol datalekken

Dit protocol beschrijft de procedure met daarin te nemen maatregelen die binnen Akorda Onderwijsdienstverlening genomen moeten worden bij een datalek volgens de toepasselijke privacywetgeving zoals de AVG.

Reikwijdte van de meldplicht datalekken

Indien er sprake is van een inbreuk op de beveiliging van persoonsgegevens 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 bestaat de mogelijkheid dat dit bij de Autoriteit Persoonsgegevens moet 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.

Meldingen

Een datalek kan door een klant, medewerker of een bewerker van Akorda worden ontdekt. Deze ontdekking wordt medegedeeld aan de adjunct-directeur van Akorda, mw. mr. A.M. Hoekstra-Borzymowska (hier aangeduid als "de directie") en aan de Functionaris Gegevensbescherming van Akorda (hierna "de FG"), Paul Suk (Suk@rein.nl), die vervolgens over zal gaan tot de beoordeling of er sprake is van een datalek. De FG bepaalt vervolgens het plan van aanpak voor een onderzoek. Hierbij is aandacht voor de volgende aspecten:

a. wat is de aard van het datalek?
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 FG indien nodig binnen 72 uur na ontdekking zorgdragen voor een melding bij de Autoriteit Persoonsgegevens. Verder zal de FG een overzicht bijhouden van alle datalekken binnen Akorda. 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. De Autoriteit Persoonsgegevens zal contact met de FG opnemen mocht na een melding aanleiding zijn om nadere stappen te ondernemen. Hierbij zal met name de herkomst van de melding worden geverifieerd en kan Akorda 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. Ook een medewerker van Akorda 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 Akorda die direct of indirect kennis draagt of krijgt van een datalek, is verplicht dit direct te melden aan de FG en de directie van Akorda;
2. De directie is tezamen met de FG verantwoordelijk voor het onderzoeken van het incident;
3. De directie is tezamen met de FG 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 tezamen met de FG verantwoordelijk voor de melding van datalekken bij de Autoriteit Persoonsgegevens;
5. De directie is tezamen met de FG verantwoordelijk voor het bijhouden van een overzicht van alle datalekken die onder de meldplicht vallen voor minimaal 1 jaar;
6. De directie is tezamen met de FG verantwoordelijk voor het ondernemen van preventieve, reparatoire en repressieve maatregelen.

Interne controle

1. De meldingen van datalekken worden jaarlijks geëvalueerd en indien nodig wordt er een verbeterplan ter voorkoming van datalekken opgesteld.
2. De directie beoordeelt tezamen met de FG 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.

Contact met advocaat

Bij spoed kan de directie rechtstreeks contact opnemen met de advocaten van Rein Advocaten & Adviseurs, Jeroen Sprangers (06-55382103) of Paul Suk (06-22009650).