Datalek Protocol

De Autoriteit Persoonsgegevens omschrijft een datalek als het krijgen van toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. De oorzaak daarvan is een inbreuk op de beveiliging van die gegevens. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.

Concrete voorbeelden van datalekken zijn het versturen van persoonsgegevens aan een verkeerde geadresseerde; inzage in een medisch dossier door een onbevoegde medewerker; en het verlies van een USB-stick met niet-versleutelde persoonsgegevens. Indringendere voorbeelden van datalekken zijn cyberaanvallen waarbij persoonsgegevens zijn buitgemaakt of een besmetting met ransomware (gijzelsoftware) waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Datalekken kunnen worden onderverdeeld in drie soorten en kunnen het gevolg zijn van handelingen van een onbevoegd persoon of per ongeluk door een bevoegd persoon:

1. Inbreuk op de vertrouwelijkheid: persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens door derden.
2. Inbreuk op de integriteit: persoonsgegevens zijn gewijzigd.
3. Inbreuk op de beschikbaarheid: de organisatie waar het datalek is (geweest) kan niet meer bij de persoonsgegevens komen. Of de gegevens zijn vernietigd.

Originzorg probeert informatie zo goed mogelijk te beschermen en preventieve maatregelen te treffen zodat onbevoegden geen toegang krijgen tot persoonsgegevens. Maatregelen zien ook op het per ongeluk verloren gaan van dergelijke informatie. Desondanks is het niet mogelijk om datalekken volledig uit te sluiten. Datalekken kunnen ontstaan en inbreuk op informatiebeveiliging is mogelijk. Dit protocol ziet op de te hanteren handelswijze als wordt vastgesteld dat een datalek is ontstaan.

Handelswijze bij een datalek

Als je een datalek veroorzaakt of een datalek vaststelt, stel je leidinggevende dan op de hoogte door de volgende informatie door te geven:

- De datum waarop het datalek heeft plaatsgevonden. Als de precieze datum niet kan worden achterhaald, maak dan een inschatting;
- De datum waarop en op welke manier het datalek is ontdekt;
- Op welke wijze het datalek is ontstaan, bijvoorbeeld doordat een onbevoegde medewerker autorisaties heeft in een digitaal systeem waarmee diegene inzicht heeft in persoonsgegevens;
- Om wat voor soort informatie het gaat, zoals telefoonnummers of medische informatie;
- Van hoeveel personen naar inschatting persoonsgegevens zijn gelekt;
- Hoe het datalek heeft kunnen plaatsvinden. Bijvoorbeeld doordat een onervaren medewerker een nieuwe, onbevoegde collega verkeerd heeft geautoriseerd in digitale systemen;
- Wat de (mogelijke) gevolgen zijn van het datalek.

De leidinggevende maakt met de aangeleverde informatie een melding van het datalek via de website van de Autoriteit Persoonsgegevens.