

Protocol datalekken

Algemeen

De PGH heeft haar privacy beleid vastgelegd in een Privacyverklaring en enkele uitvoeringsdocumenten, waaronder dit Protocol datalekken.

Op grond van de AVG moet een datalek binnen 72 uur gemeld worden aan de Autoriteit Persoonsgegevens.

Iedere persoon die binnen de kerkelijke organisatie met persoonsgevoelige informatie werkt of deze in bezit heeft, kan te maken krijgen met een datalek.

De gevolgen van een datalek kunnen behoorlijk van omvang zijn en invloed hebben op het kerkelijk functioneren.

Uitwerking

1. Onder een datalek wordt verstaan:
 - ❖ Het opzettelijk of onopzettelijk vrijgeven van beveiligde informatie aan een onvertrouwd publiek
2. Voor het herkennen en melden van datalekken is door de Protestantse Kerk Nederland een stappenplan opgesteld dat als bijlage bij dit protocol is gevoegd.
3. De Coördinator Gegevensverwerking draagt zorg voor invoering en naleving van het stappenplan Datalekken bij een ieder die met privacygevoelige informatie werkt.
4. Ingeval van het vermoeden van een datalek dient hiervan zo snel mogelijk (binnen 24 uur) melding gemaakt te worden bij de Coördinator Gegevensverwerking
5. De Coördinator Gegevensverwerking volgt bij het melden van een datalek bij de Autoriteit Persoonsgegevens het stappenplan.

Stappenplan datalekken

Stap 1:

Is er iets gebeurd met
Persoonsgegevens wat niet
de bedoeling was?

nee

Er is geen sprake van een datalek en u hoeft
geen actie te ondernemen.
Eventueel moet u de beveiliging op orde maken

Ja

Stap 2:

Is er een risico voor de rechten
en vrijheden van hen van wie de
gegevens zijn?

nee

Er moet een interne registratie gemaakt worden
maar er hoeft geen melding gedaan te worden bij
de Autoriteit Persoonsgegevens

Ja

Stap 3:

Is er **hoog** risico voor de rechten
en vrijheden van hen van wie de
gegevens waren

nee

Er moet een interne registratie gemaakt worden **en**
er moet melding gemaakt worden bij de
Autoriteit Persoonsgegevens

ja

Er moet een interne registratie gemaakt worden **en**
er moet melding gemaakt worden bij de
Autoriteit Persoonsgegevens **en** aan de personen
over wie het gaat

Voorbeelden

- | | |
|--------|---|
| Stap 1 | U trof een onbevoegd persoon aan voordat deze in de dossiers kan kijken.
Dit is een beveiligingsincident maar geen datalek |
| Stap 2 | Bij een brand zijn gegevens verloren gegaan
Een lijst met vrijwilligers is ergens blijven liggen en de lijst wordt later teruggebracht |
| Stap 3 | nee: Een document met inlogcode en namen raakt verloren maar uit het document blijkt niet dat het gegevens van de kerk zijn |
| Stap 3 | ja: De computer is gehackt en er komt een melding dat bestanden – bijv. een uitdraai uit ledenadministratie – versleuteld zijn |