

Procedure Melding Datalekken Stichting Zomerkind 2018

Interne melding datalek bij de Stichting Zomerkind

Bij constatering van een datalek of een vermoedelijk datalek moet dat direct worden gemeld aan de IT Beheerder van Zomerkind. In bepaalde gevallen moet Zomerkind binnen 72 uur na het datalek een melding hebben gedaan bij de Autoriteit Persoonsgegevens (AP). Het is dus van belang om een (mogelijk) datalek onmiddellijk nadat het zich heeft voorgedaan door te geven.

Dit kan door een mail te sturen aan privacy@zomerkind.nl. Een datalek kan daarnaast telefonisch worden gemeld aan het IT-beheer (+31 6 24179313) of aan de voorzitter van de Raad van Bestuur (+31 6 30365971).

De melding moet tenminste de volgende gegevens bevatten:

- de aard van de inbreuk (dus: wat is er gebeurd?);
- de oorzaak van het datalek (hack, diefstal, verlies, etc.);
- beschrijving van de gelekte persoonsgegevens (aard van de gegevens, hoeveelheid, etc.);
- eventuele maatregelen die genomen zijn/worden genomen om het datalek te dichten;
- een inschatting van het risico dat de betrokkenen kunnen lopen;
- contactgegevens van de melder.

Weet je bepaalde onderdelen niet in te vullen, sla deze dan over. Zorg wel dat je contactgegevens doorgeeft waarop je goed bereikbaar bent (eventueel buiten werktijd).

1. De IT-beheerder onderzoekt de melding.
2. De IT-beheerder beoordeelt of er sprake is van een datalek en welke vervolgacties genomen zouden moeten worden. Indien er twijfel bestaat of er sprake is van een datalek wordt overlegd met de Functionaris Gegevensbescherming (FG).
3. Als er sprake blijkt van een datalek wordt de FG geïnformeerd.
4. Indien er acuut (technische)maatregelen noodzakelijk zijn om de gevolgen van het datalek te beperken worden deze door de IT-beheerder genomen, nog voor de rapportage aan de FG of de Raad van Bestuur.
5. De IT-beheerder en de Functionaris Gegevensbescherming maken een bondig plan van aanpak op dat ziet op de volgende punten:
 - a. technische- en organisatorische maatregelen;
 - b. wel- of niet melden aan de Autoriteit Persoonsgegevens
 - c. wel- of niet melden aan betrokkenen;
 - d. wel- of niet melden aan belanghebbenden (cliënten, verwanten, overige betrokkenen).
6. Het plan wordt aan de portefeuillehouder van de Raad van Bestuur voorgelegd.
7. De acties zoals besloten door de portefeuillehouder worden uitgevoerd:
 - De FG: verzorgt de melding naar de Autoriteit Persoonsgegevens;
 - a. De IT-beheerder: neemt (zo nodig) technische maatregelen om beperking van de impact van het datalek te beperken of herhaling te voorkomen;
 - b. Overige (informatie)acties: zoals besloten in het plan van aanpak.

8. Het incident wordt, samen met de ondernomen acties en maatregelen, geregistreerd door de FG in het register datalekken.

Indien één van de partijen zoals genoemd in dit protocol niet (tijdig) kan reageren kunnen de overige betrokken partijen naar eigen inzicht afwijken van dit protocol en zullen zij zich achteraf verantwoorden.

Externe partijen

De interne meldplicht aan de directie geldt niet alleen voor medewerkers van Zomerkind, maar ook voor leveranciers en partners van Zomerkind, voor zover die leveranciers of partners persoonsgegevens van Zomerkind verwerken. Een verwijzing naar deze procedure Melding Datalekken dient opgenomen te worden in de overeenkomst met de betreffende leveranciers en partners.

Aldus vastgesteld in de vergadering van de Raad van Bestuur van de Stichting Zomerkind d.d. 11 december 2018 en goedgekeurd door de Raad van Toezicht van de Stichting Zomerkind in haar vergadering van 17 december 2018.

Mr. M.J. Toet
Voorzitter Raad van Bestuur Stichting Zomerkind.