Toelichting beveiligingsincidenten- en datalekkenregister

Waarom dit beveiligingsincidenten- en datalekkenregister?

De AVG verplicht organisaties om een beveiligingsincidenten- en datalekkenregister bij te houden van alle voorgevallen beveiligingsincidenten en datalekken met persoonsgegevens. Hierin staan o.a. de aard van het incident, op welke manier het is afgehandeld en - ingeval van melding bij de Autoriteit Persoonsgegevens - ook het registratienummer van deze melding.

Ook is het verplicht om de overwegingen vast te leggen die gemaakt zijn bij de beslissing om een inbreuk al dan niet te melden (overleg hierover altijd met de FG!). Met name als een datalek níet wordt gemeld, moet de toezichthouder kunnen nagaan welke argumenten een organisatie hiervoor heeft gebruikt. Als vastlegging in het register ontbreekt, loopt de organisatie het risico op reputatieschade en een (hoge) boete als er iets mis gaat.

Maak het register onderdeel van het incidenten- en datalekkenbeleid/protocol en bespreek de registraties regelmatig binnen de organisatie als onderdeel van een plan-do-check-act (PDCA) cyclus: zo kan de organisatie aantoonbaar leren van fouten.

Voor wie is dit incidentenregister bedoeld?

Dit incidentenregister is bedoeld voor privacy-coördinatoren of andere personen die operationeel verantwoordelijk zijn voor het behandelen/registreren van beveiligingsincidenten en datalekken (eerste lijn). De Functionaris Gegevensbescherming (tweede lijn) kan hierbij adviseren, m.n. als er sprake is van melding bij de toezichthouder.

Hoe moet je dit incidentenregister gebruiken?

- Handel het beveiligingsincident of datalek af volgens de stappen in het incidenten- en datalekkenprotocol van je organisatie en start direct met vastlegging in het register.
- Let daarbij vooral op de termijnbewaking: een meldenswaardig datalek moet binnen 72 uur bij de Autoriteit Persoonsgegevens worden gemeld, dus registratie van de datum en tijd van de constatering van een vermeend datalek en van de melding is noodzakelijk.
- Vul zoveel mogelijk gegevens in en maak gebruik van de **10 tips** van de Autoriteit Persoonsgegevens.
- Stem een meldenswaardig datalek áltijd af met de Functionaris Gegevensbescherming: raadpleeg de FG ook bij twijfel over overige beveiligingsincidenten/datalekken.
- Zorg voor duidelijk versiebeheer, hierdoor maak je inzichtelijk wanneer het register voor het laatst is gewijzigd en door wie.

Lumen Group kan ondersteunen bij het implementeren van dit incidentenregister. Neem vrijblijvend contact op via fg@lumengroup.nl of 030 889 65 75 om de mogelijkheden te bespreken.

versie 2.0 21-07-2021