Datum: **1-4-2024**

Voor vragen neem contact op met: Functionaris Gegevensbescherming

**Protocol melden datalek/beveiligingsincident**

1. **Inleiding**

Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Het kan gaan om een kwijtgeraakte USB-stick of een gestolen laptop met persoonsgegevens, maar ook om een inbraak in een datasysteem of per ongeluk verstrekte toegang tot gegevens aan personen of instanties die daartoe geen toegang zouden mogen hebben. Het verzenden van een e-mail aan een adressenbestand waarin alle e-mailadressen voor iedereen zichtbaar zijn is ook al een datalek.

Als sprake is van een ernstig datalek[[1]](#footnote-1), dan zijn we op grond van de Algemene verordening gegevensbescherming (AVG) verplicht om dit te melden aan de Autoriteit Persoonsgegevens en soms ook aan de betrokkenen[[2]](#footnote-2). Om te zorgen voor een eenduidig beleid binnen onze organisatie en om te voorkomen dat datalekken die wel gemeld hadden moeten worden, dat niet worden en dat datalekken die niet gemeld hoeven te worden, dat wel worden, heeft Stichting Primo Schiedam ervoor gekozen de meldingen centraal te laten verlopen via het meldpunt [datalek@primoschiedam.nl](mailto:datalek@primoschiedam.nl). Deze wordt beheerd door de privacy officer.

**2. Het protocol**

2.1 Onmiddellijk nadat een medewerker/vrijwilliger/ouder ontdekt of ter ore komt dat sprake kan zijn van verlies of onrechtmatige verwerking van persoonsgegevens binnen Stichting Primo Schiedam, meldt hij dat aan het meldpunt datalek@primoschiedam.nl.

2.2 Het meldpunt datalek overlegt met de functionaris gegevensbescherming van Primo Schiedam of er sprake is van een (mogelijk) datalek en zo ja, of dit datalek moet worden gemeld bij de Autoriteit Persoonsgegevens en/of bij de betrokkene(n).

Bepalen melden bij Autoriteit Persoonsgegevens:

Afbeelding met schermafbeelding

Automatisch gegenereerde beschrijving

2.3 De functionaris gegevensbescherming draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).

2.4 Als de medewerker/vrijwilliger/ouder het niet eens is met de beslissing van het meldpunt datalek om het (mogelijke) datalek wel - of niet te melden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan richt hij zich tot het bestuur.

1. Het melden van een datalek hoeft alleen als dit lek leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Daarvan is sprake als er een grote hoeveelheid persoonlijke data is gelekt of als het om gegevens van gevoelige aard gaat. Dat zijn financiële of medische gegevens, maar ook gegevens over relatieproblemen, inloggegevens of BSN. Maar als er bijvoorbeeld alleen een betrekkelijk beperkt aantal NAW-gegevens van ouders en collega’s op een gestolen laptop staan, hoeft dat incident niet te worden gemeld bij de toezichthouder. Dat kan in bepaalde gevallen anders zijn, maar in veel gevallen kan melding in dergelijke gevallen achterwege blijven. [↑](#footnote-ref-1)
2. Je hoeft een datalek alleen te melden aan de betrokkenen als het datalek ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. Daarvan zal natuurlijk snel sprake zijn als er veel gegevens of gegevens van gevoelige aard zijn gelekt. Maar als de gelekte gegevens beveiligd zijn (bijvoorbeeld door encryptie of hashing) kan melding aan de betrokkenen toch niet verplicht zijn. Datzelfde geldt als je bepaalde zwaarwegende redenen hebt om niet te melden. [↑](#footnote-ref-2)