Protocol Datalekken en beveiligingsincidenten

LUCAS ONDERWIJS

Datum: 14-5-2018

Geactualiseerd en met instemming van de GMR (datum) door het CvB vastgesteld (datum)

Inhoud

Aanleiding

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat organisaties een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In een aantal gevallen moet de organisatie het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Door de invoering van de AVG op 25 mei 2018 is de procedure voor melding aangepast.

Kader

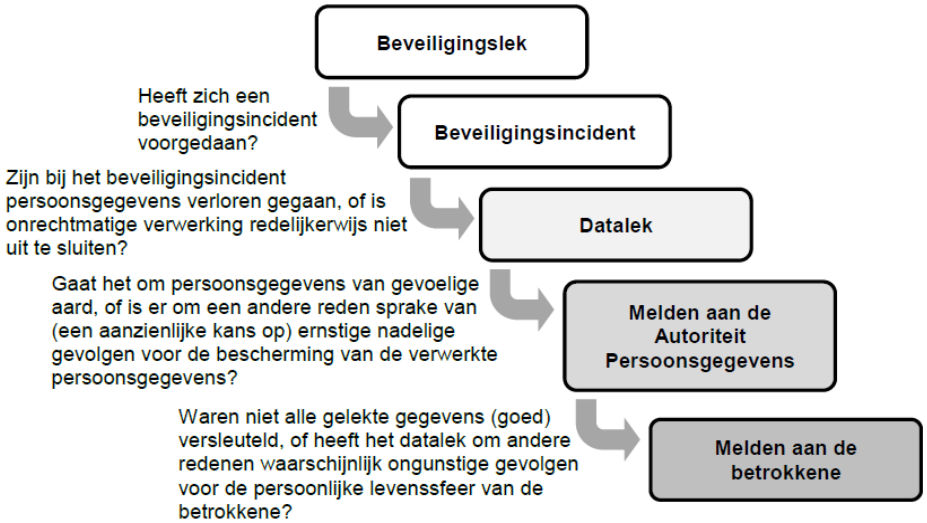
Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de AVG. Hierin staat dat de persoonsgegevens die Lucas Onderwijs verwerkt moeten worden beveiligd tegen verlies en tegen onrechtmatige verwerking.

Een datalek moet vanaf 1 januari 2016 worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Lucas Onderwijs hecht grote waarde aan de bescherming van de persoonlijke levenssfeer en een zorgvuldige omgang met persoonsgegevens. Medewerkers van Lucas Onderwijs verrichten hun werkzaamheden binnen de kaders van het Lucas Onderwijs Privacy protocol. Dit protocol vindt zijn oorsprong in en volgt de AVG. Met anderen die gegevens verwerken voor Lucas Onderwijs (de zogenaamde verwerkers) is een verwerkersovereenkomst afgesloten. Binnen deze verwerkersovereenkomst wordt het protocol datalekken meegenomen.

Afwegingen

Bij de beslissing of een gebeurtenis die zich heeft voorgedaan moet worden gemeld aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moeten een aantal afwegingen gemaakt worden. Het onderstaande schema geeft deze afwegingen weer.



Datalek

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident kan gedacht worden aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker, vermissing van een papieren dossier of dossierstukken.

Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs uitgesloten kunnen worden.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens.

Melden aan de autoriteit Persoonsgegevens

Lucas Onderwijs is in een aantal gevallen verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens. Volgens de wet moet Lucas Onderwijs een melding doen aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk.

Bij persoonsgegevens van gevoelige aard moet gedacht worden aan:

- Bijzondere persoonsgegevens
    - Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.
- Gegevens over de financiële of economische situatie van de betrokkene
    - Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
    - (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens
    - De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden *misbruikt voor (identiteits)fraude*
    - Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Melden aan betrokkene

In een aantal gevallen waarin een datalek gemeld wordt aan de Autoriteit Persoonsgegevens moet deze ook worden gemeld aan de betrokkene. De wet geeft aan dat Lucas Onderwijs een melding moet doen aan de betrokkene als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Daarbij kan bijvoorbeeld gedacht worden aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits-)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt dan moet het datalek ook gemeld worden aan de betrokkene.

De melding stelt de betrokkene in staat om alert te zijn op de mogelijke gevolgen van het datalek en om zich daar waar mogelijk tegen te wapenen door, bijvoorbeeld, een gelekt wachtwoord te vervangen. Indien er gemeld moet worden dan zal Lucas Onderwijs betrokkenen onverwijld op de hoogte stellen zodat de betrokkene naar aanleiding van de melding in staat wordt gesteld maatregelen te nemen om zich te beschermen tegen de gevolgen van het datalek.

Afspraken met de verwerker

Lucas Onderwijs heeft als verantwoordelijke een zorgplicht t.a.v. een eventueel opgetreden datalek bij een verwerker. Lucas Onderwijs zorgt er in dit geval voor dat zij haar wettelijke verplichting kan nakomen en legt met de verwerker vast dat zij tijdig en adequaat geïnformeerd wordt over datalekken waarvan hij/zij kennis krijgt. Lucas Onderwijs wil in alle gevallen geïnformeerd worden t.a.v. datalekken bij verwerkende partijen.

Lucas Onderwijs maakt de volgende afspraken met de verwerker:

1. De verwerker informeert Lucas Onderwijs onverwijld over alle relevante incidenten
2. De verwerker meldt zelf datalekken aan de Autoriteit persoonsgegevens en verzendt een afschrift van deze melding naar de Functionaris gegevensbescherming
3. De verwerker houdt Lucas Onderwijs op de hoogte van nieuwe ontwikkelingen rond het gemelde datalek incident en van de maatregelen die getroffen worden aan de kant van de bewerker om herhaling van het incident te voorkomen.

De gemaakte afspraken worden vastgelegd in de bij het Lucas Onderwijs privacy regelement behorende verwerkersovereenkomsten. Voor veel verwerkers geldt dat zij aangesloten zijn bij Privacy Convenant Onderwijs en daarmee het Privacy Protocol Onderwijs en de Verwerkersovereenkomst hanteren.

Meldingsprotocol

Alle medewerkers van Lucas Onderwijs zijn verplicht onverwijld een melding te doen van een geconstateerd datalek. Voorbeelden van datalekken zijn: een kwijtgeraakte gegevensdrager (usb stick, externe harddisk) met persoonsgegevens, een gestolen laptop, tablet, telefoon, of een inbraak in een databestand of applicatie, ontvreemding toegangscodes van applicaties en dergelijke.

De melding dient te gebeuren bij de directeur van de school of de directe leidinggevende van de melder. De directeur van de school of de directe leidinggevende van de melder doet de melding bij de privacy functionaris op het Stichtingskantoor. De privacy functionaris is functioneel ondergebracht bij de afdeling Informatiebeheer van het Stichtingskantoor. I.s.m. de privacy

functionaris neemt de directeur van de school maatregelen ter voorkoming van verdere schade. De privacy functionaris meldt het incident bij de Functionaris Gegevensbescherming van Lucas Onderwijs. Op basis van de melding wordt aan de hand van de leidraad van de Autoriteiten Persoonsgegevens: Beleidsregels meldplicht datalekken beslist of er gemeld moet worden bij de Autoriteit Persoonsgegevens en/of de betrokkene(n).

De Functionaris Gegevensbescherming informeert het College van Bestuur van Lucas Onderwijs.

Privacy Functionaris

Telefoon : 070-3001100

Email : avg@lucasonderwijs.nl

Functionaris Gegevensbeheer

Telefoon : de FG is te bereiken via de afdeling Informatiebeheer of direct via

Email : fg@lucasonderwijs.nl

Vastleggen meldingen

Meldingen van datalekken worden vastgelegd in een databank. Bij de melding wordt vastgelegd wat de aard is van de gegevens die zijn gelekt, onder welke omstandigheden het lek is ontstaan, door wie de melding is gedaan, of er een melding bij de Autoriteit Persoonsgegevens is gedaan (incl. opslag meldingsformulier), of de betrokkene (degene wiens gegevens zijn gelekt) is geïnformeerd, welke maatregelen er zijn genomen ter bescherming van de bij het datalek betrokken personen, de status van afhandeling en de genomen maatregelen ter voorkoming van de lekkage in de toekomst.

Dit protocol is met instemming van de Bureauraad op 17 mei 2018, GMR-VO op 22 mei 2018 en de GMR-PO op 23 mei 2018 tot stand gekomen. Vastgesteld door het College van Bestuur d.d. 24 mei 2018.

Stroomschema melding Datalekken