



PCBO Leiderdorp

Protestants Christelijk Basisonderwijs

Protocol Datalekken PCBO Leiderdorp

De meldplicht datalekken in de wet bescherming persoonsgegevens (WBP)

Datum: 14 april 2016

S. Stouten

Inhoud

Aanleiding:	3
Kader:	3
Afwegingen:	3
Datalek:	4
Melden aan de autoriteit Persoonsgegevens:.....	4
Melden aan betrokkene:.....	5
Afspraken met de bewerker:.....	5
Meldingsprotocol PCBO:.....	6
Gegevens Privacy functionarissen PCBO:.....	6
Vastleggen meldingen:	6
Bronnen:.....	6
Relevante webadressen:	6
Meldprocedure datalek:	7

Aanleiding:

Op 1 januari 2016 gaat de meldplicht datalekken in. 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). In dat kader wordt met ingang van 1 januari 2016 dit protocol van kracht.

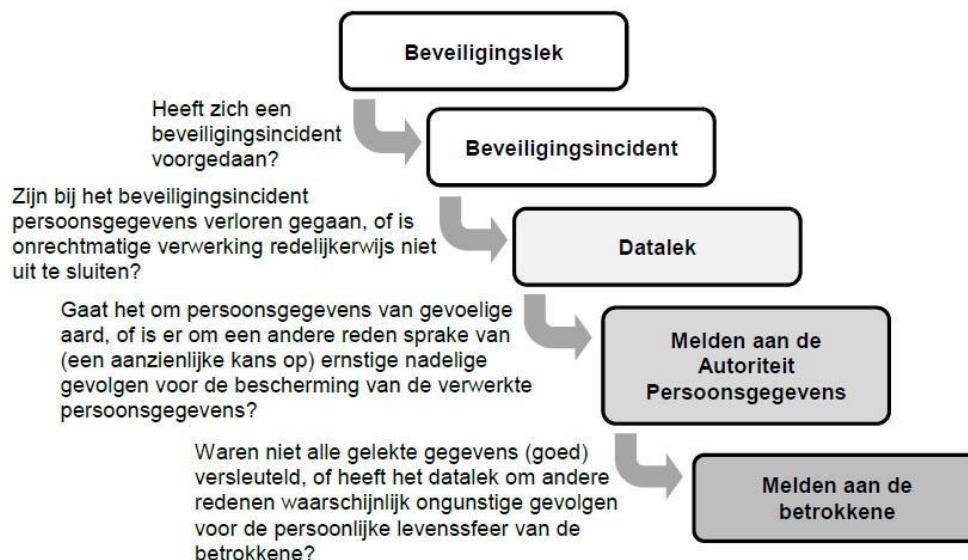
Kader

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 Wet bescherming persoonsgegevens (WBP). Hierin staat dat de persoonsgegevens die PCBO verwerkt moeten worden beveiligd tegen verlies en tegen onrechtmatige verwerking (artikel 13 WBP)

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 (artikel 34a, eerste lid, WBP). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (artikel 34a, tweede lid, WBP). De beleidsregels zijn vastgelegd door het CBP en op deze link te vinden <https://www.cbpweb.nl/nl/nieuws/cbp-publiceert-beleidsregels-meldplicht-datalekken>

Afwegingen:

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



Figuur 1 Bron: de meldplicht datalekken (wbp), CBP 8-12-2015

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 kan worden uitgesloten

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

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

Een factor die hierbij een rol speelt is de aard van de geleeke persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn geleeke, dan is over het algemeen een melding noodzakelijk. Bij persoonsgegevens van gevoelige aard moet gedacht worden aan:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 WBP. 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 betrokkenen. 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 (identiteit)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 ook worden gemeld aan de betrokkene. De wet geeft aan dat de PCBO 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, zal DHS 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.

Boete

Bij overtreding van de meldplicht datalekken uit de WBP kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze bestuurlijke boete bedraagt ten hoogste het bedrag van de zesde categorie van artikel 23, vierde lid, van het Wetboek van Strafrecht. Dat is per 1 januari 2016 maximaal € 820.000. Indien de overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen voorafgaand aan eventuele oplegging van een bestuurlijke boete.

Afspraken met de bewerker

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

De PCBO maakt de volgende afspraken met de bewerker:

1. De bewerker informeert de PCBO over alle relevante incidenten.
2. De bewerker meldt zelf datalekken aan de Autoriteit Persoonsgegevens en verzendt een afschrift van deze melding naar de Functionaris gegevensbeheer.
3. De bewerker houdt de PCBO 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.

Meldingsprotocol PCBO

Alle medewerkers van de PCBO zijn verplicht 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 toegangscode van applicaties enz.

De melding dient te gebeuren bij de datalek-coördinator en bij de directeur van de school. De datalek-coördinator beoordeelt het datalek en vormt een crisisteam. Het crisisteam doet onderzoek naar de oorzaak en gevolg van het datalek. Op basis van dit onderzoek wordt aan de hand van de leidraad van het CBP: [Beleidsregels meldplicht datalekken](#), beslist of er gemeld moet worden bij de Autoriteit Persoonsgegevens en/of de betrokkene(n). De datalek-coördinator legt het advies t.a.v. de melding voor aan de raad van toezicht van de PCBO.

Gegevens Datalek-coördinator

Naam:
Telefoon:
Emailadres:

Het mailadres:

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.

Bronnen:

1. De meldplicht datalekken in de wet bescherming persoonsgegevens (WBP), beleidsregels voor toepassing van artikel 34a van de WBP
2. Wet Bescherming Persoonsgegevens

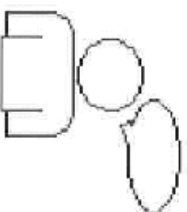
Relevant webadres:

1. <https://www.cbpweb.nl/nl>

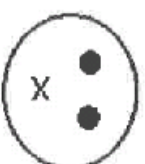
Meldprocedure datalek



Er is een datalek
wat moet ik doen?



Meld het lek bij de
datalek-coördinator
Dat is:.....



Houd het lek
daarna GEHEIM!!



Er volgt een onderzoek naar
naar oorzaak en gevolg



Een crisisteam
wordt gevormd



De coördinator beoordeelt
de ernst van het lek



Een melding kan volgen bij de
Autoriteit persoonsgegevens
en betrokkenen