Protocol Datalekken en beveiligingsincidenten

Datum: 06-11-2018

Aanleiding voor het protocol

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat de organisaties een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. In een aantal gevallen moet de organisatie het lek ook melden bij de betrokkenen (de personen van wie de gegevens zijn gelekt). Door de invoering van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 is de procedure voor melding aangepast. In de hele Europese Unie (EU) geldt dezelfde privacywetgeving. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR). [1]

Kader

Iedereen heeft recht op eerbiediging van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de AVG en verwerkt in het Privacy Reglement van OPOPS. In de wet staat dat de persoonsgegevens die OPOPS-scholen verwerken, beveiligd moeten worden tegen verlies en tegen onrechtmatige verwerking.

Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens als:

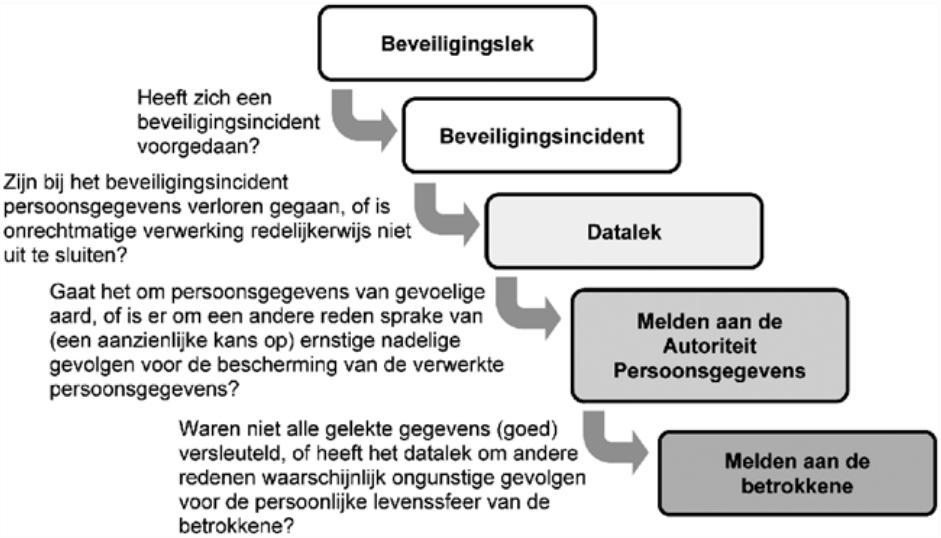
- het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens;
- het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens Daarnaast moet het datalek gemeld worden aan de betrokkenen;
- indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer;

OPOPS hecht veel waarde aan de bescherming van de persoonlijke levenssfeer en een zorgvuldige omgang met persoonsgegevens. Medewerkers van OPOPS verrichten hun werkzaamheden binnen de kaders van het Privacy protocol. Met derden die gegevens verwerken voor OPOPS is een verwerkersovereenkomst afgesloten.

[1] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg

Afwegingen

Bij de beslissing of een gebeurtenis moet worden gemeld aan de AP (en eventueel de betrokkenen), moeten een aantal afwegingen gemaakt worden. Het onderstaande schema geeft deze afwegingen weer:



[2]

Wat is een 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. Dit wordt beoordeeld door de (toekomstige) functionaris gegevensbescherming in samenspraak met de bestuurder.

Wie beoordeelt een datalek?

Elke medewerker binnen OPOPS, die een datalek vermoedt, geeft dit in eerste instantie aan bij de directie van de school. De directie bepaalt vervolgens of dit vermoeden een reden vormt om dit aan de bestuurder te melden. Indien dit het geval is, vullen de leidinggevende en betreffende persoon het document in en melden ze dit via *meldpuntdatalek@opops.nl*. De manager IBP bepaalt of de (toekomstige) functionaris gegevensbescherming hierover moet worden ingelicht. De (toekomstige) functionaris gegevensbescherming meldt het datalek bij de Autoriteit Persoonsgegevens (AP).

[2] https://wetten.overheid.nl/BWBR0037346/2015-12-16

Noodzakelijke acties betreffende medewerker bij een datalek.

Indien een datalek ontstaat door verlies of diefstal van apparatuur zoals laptops, tablets en/of smartphones dienen de volgende acties direct uitgevoerd te worden:

1. Aanvragen van een nieuw wachtwoord voor Office 365. Met de inloggegevens van Office 365 heeft iedere gebruiker toegang tot de mail van de gebruiker en tot de delen van SharePoint waar die persoon voor gemachtigd is. Wachtwoordwijziging zorgt ervoor dat het mailaccount en SharePoint met het oude wachtwoord niet meer toegankelijk zijn. Deze actie voert de medewerker onmiddellijk zelf uit.
2. Wijzigen van inloggegevens van overige webbased systemen, zoals bijvoorbeeld Parnassys en basispoort. Medewerker benadert hiervoor onmiddellijk de ICT-er van de school en vraagt onmiddellijk een nieuw wachtwoord aan. Bovenschools worden de meldingen vanuit de scholen vastgelegd door het bestuurskantoor (manager IBP). Deze doet, indien nodig, nader onderzoek. Bevindingen hiervan worden doorgesproken met de bestuurder.

Wie meldt een datalek?

De melding bij AP wordt namens OPOPS gedaan door de (toekomstige) functionaris gegevensbescherming.

Wie verzorgt de communicatie richting interne en externe betrokkenen bij een datalek?

De bestuurder en manager IBP zijn verantwoordelijk voor de juiste interne en externe communicatie bij een datalek. Uiteraard wordt binnen de organisatie altijd eerst overleg gevoerd met de betreffende directies voordat berichten ‘naar buiten’ gaan.

Melden aan de autoriteit Persoonsgegevens

OPOPS is in een aantal gevallen verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens. Volgens de wet moeten we 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
  o 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
  o Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
  o (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

o 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
  o Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

De melding wordt gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na het ontdekken van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar (https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0). Via dit webformulier kunt u de melding zo nodig aanvullen of intrekken.

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 OPOPS 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 OPOPS 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. Dit doet OPOPS zo snel mogelijk na het constateren van de datalek, zodat de betrokkene zo snel mogelijk in actie kan komen.

Stappenplan ter voorkoming van een datalek

Handelingen op de werkplek (in het klaslokaal, directieruimte(s), IB-ruimte en administratieve ruimte:

- Voor de vaste computer/laptop:
    - De gebruiker logt altijd in op zijn/haar eigen account.
    - Bij verlaten van de ruimte moet het systeem vergrendeld worden

1. De gebruiker logt altijd in op zijn/haar eigen account.
2. Bij verlaten van de ruimte moet het systeem vergrendeld worden (bij Windows is dit de Windowstoets en de L-toets/bij Apple computers is dit control-shift-power)*
3. Bij printen van gevoelige informatie moet het document vastgehouden geprint worden. Door middel van een code kan het document geprint worden bij de printer.
4. Gevoelige documenten worden opgeslagen in de Cloud (office 365, Parnassys) en niet op de computer zelf, USB-sticks, externe harde schijven e.d.
5. Wanneer een gevoelig document gedownload dient te worden, zodat het bijvoorbeeld in een ander programma geupload kan worden, wordt het document hierna van de computer verwijderd.

- Voor het digibord/touchscreen:
    - Bij niet lesgebonden gebruik staat het bord/scherm uit (b.v. bij beantwoorden email, inloggen Parnassys)

- Voor werktelefoons en –tablets:
    - Om het gebruik te activeren moet gebruik gemaakt worden van een sterk wachtwoord (of vingerafdruk)

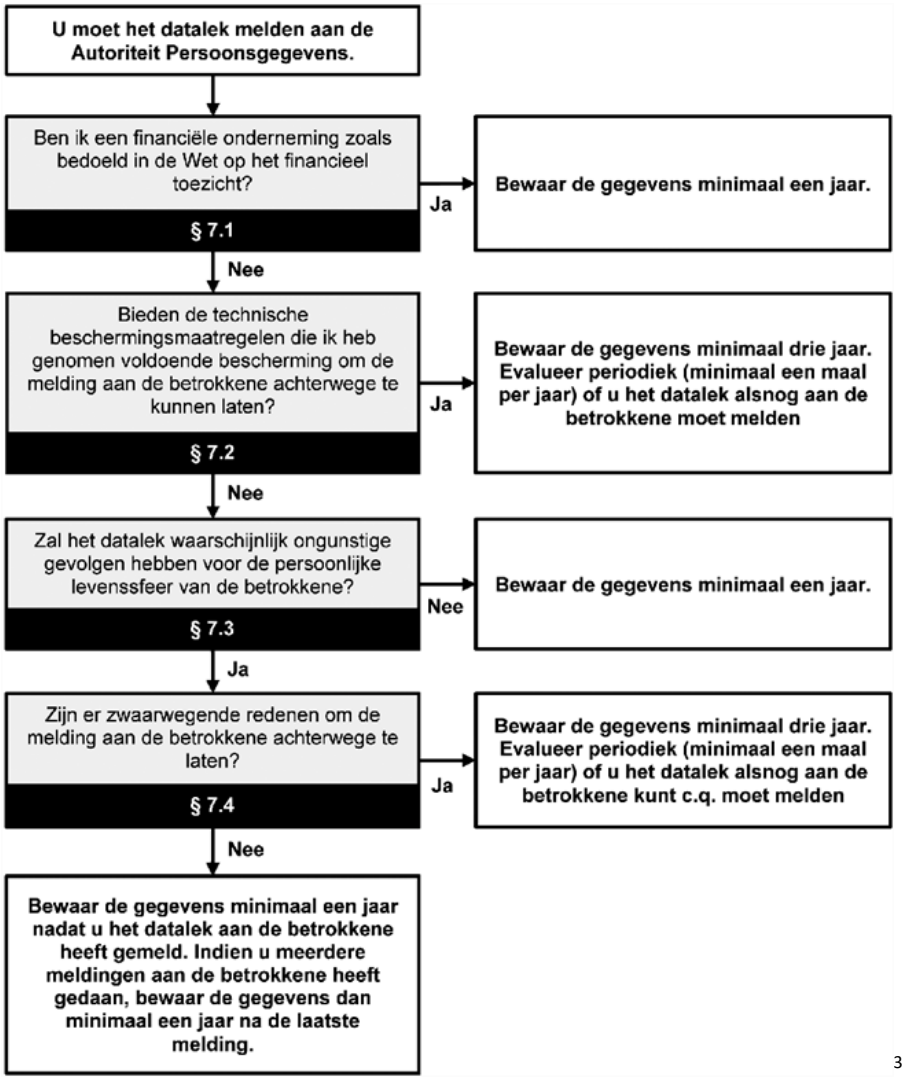
- Voor wachtwoorden:

1. Uitgereikte wachtwoorden worden veranderd in persoonlijke wachtwoorden
2. Wachtwoorden moeten regelmatig gewijzigd worden (automatisch bij Office 365)
3. Wachtwoorden worden niet aan anderen verstrekt
4. Wachtwoorden dienen op een veilige (digitale) manier bewaard te worden

Indien bij de bovenstaande stappen mogelijk een misstap is begaan, dient men de directie op de hoogte te stellen.

Welke gegevens moet ik vastleggen over een datalek

Er moet een overzicht bijgehouden worden van alle datalekken die onder de meldplicht vallen. Per datalek moet het overzicht in ieder geval feiten en gegevens over de aard van de inbreuk bevatten. Als het noodzakelijk was om het datalek te melden aan de betrokkene, dan moet ook de tekst ter kennisgeving worden opgenomen.
Er is volgens de wet geen vaste regel voor de bewaartermijn van de gegevens, maar ga uit van tenminste een jaar. Soms kan het nodig zijn om de gegevens langer te bewaren. Onderstaand schema geeft hier informatie over:



3

Bij aanvang van de AVG is er een aanpassing gedaan voor het bewaren van gegevens over het datalek. Over alle datalekken moeten nu gegevens worden bewaard, niet meer alleen van de datalekken die gemeld zijn bij de AP. Hierin moeten de feiten worden opgenomen, de gevolgen van het datalek en de acties die zijn ondernomen. Middels deze documentatie moet de AP kunnen controleren of OPOPS zich houdt aan de meldplicht.
Het bovenstaande schema gaat ervan uit dat de gegevens alleen bewaard worden met één van de volgende doeleinden:

- Lering trekken uit het datalek en de wijze waarop is gehandeld door OPOPS;
- Antwoord kunnen geven op vragen van betrokkenen en anderen;
- Alsnog melden van het datalek aan de betrokkenen, als dit in eerste instantie niet nodig leek.

[3] https://wetten.overheid.nl/BWBR0037346/2015-12-16#Circulaire.divisie10

Stroomschema datalekken

[4]

[4] https://www.privacy-web.nl/cms/files/2018-02/meldplicht-datalekken-1.1.pdf

Bronnen:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
https://wetten.overheid.nl/BWBR0037346/2015-12-16#Circulaire.divisie10
https://www.privacy-web.nl/cms/files/2018-02/meldplicht-datalekken-1.1.pdf

Bijlage 1: Incidentenregistratie

Via onderstaande link kom je in het document waar de incidenten worden bijgehouden en opgeslagen.
Het document moet ingevuld worden bij een datalek en de melding moet worden gedaan via meldpuntdatalek@opops.nl.

https://opops.sharepoint.com/:x:/r/sites/werkgroepict/Gedeelde%20%20documenten/IBP/3.%20Realiseren/2.%20Aan%20de%20slag/Incidenten%20registratie.xlsx?d=w70af9c73657e4559baaecce9822c067a&csf=1&e=seCYGM

Bijlage 2: Poster privacy OPOPS t ter voorkoming van datalekken