Rector Hellemonsstraat 1b
4702 RG Roosendaal
Telefoon: 0165 – 330 966
E-mail: secretariaat@po3002.nl

PO3002.nl
Samenwerkingsverband Passend Onderwijs
Roosendaal, Moerdijk en omgeving

Meldplicht datalekken

Op 1 januari 2016 gaat de meldplicht datalekken in. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En in een aantal gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).
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 u de persoonsgegevens die u verwerkt moet beveiligen tegen verlies en tegen onrechtmatige verwerking (artikel 13 Wbp). 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, 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). Bij de beslissing of u een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet u een aantal afwegingen maken.

Datalek

Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident kan bijvoorbeeld gedacht worden aan het kwijtraken van een USB-stick, de diefstal van een laptop of aan een inbraak door een hacker. Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.
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 te worden gedaan aan de Autoriteit Persoonsgegevens.

Melden aan de Autoriteit Persoonsgegevens

Niet ieder datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet een melding gedaan worden aan de Autoriteit Persoonsgegevens als het datalek 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.

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 gaat het om:

Rector Hellemonsstraat 1b
4702 RG Roosendaal
Telefoon: 0165 – 330 966
E-mail: secretariaat@po3002.nl

- *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 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).

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen aanleiding zijn om het datalek te melden. Maar let op: als de aard van de gelekte gegevens daar aanleiding toe geeft is het mogelijk dat een datalek moet worden gemeld waar de persoonsgegevens van slechts één persoon bij betrokken zijn.

De melding moet worden gedaan zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar. Via dit webformulier kan de melding zo nodig worden aangevuld of ingetrokken.

Melden aan betrokkene

Als een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens, dan betekent dit niet automatisch dat dit datalek ook moet worden gemeld aan de betrokkene. Hiervoor moet een aparte afweging worden gemaakt.

De wet geeft aan dat een melding moet worden gedaan 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 worden gedacht aan onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan kan er in principe van uit worden

Rector Hellemonsstraat 1b
4702 RG Roosendaal
Telefoon: 0165 – 330 966
E-mail: secretariaat@po3002.nl

gegaan dat het datalek niet alleen moet worden gemeld aan de Autoriteit Persoonsgegevens, maar ook 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. De wet schrijft voor dat de melding onverwijld moet worden gedaan. Er moet rekening worden gehouden met het feit dat de betrokkene naar aanleiding van de melding mogelijk maatregelen moet nemen om zich te beschermen tegen de gevolgen van het datalek. Hoe eerder de betrokkene daarover wordt geïnformeerd, hoe eerder deze in actie kan komen.

Als er passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege blijven. Bij deze beschermingsmaatregelen moet bijvoorbeeld gedacht worden aan cryptografische bewerkingen zoals encryptie en hashing. Per geval zal bepaald moeten worden of de maatregelen die zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

Het Samenwerkingsverband en datalekken

Het Samenwerkingsverband Passend Onderwijs Roosendaal-Moerdijk e.o. (30.02) heeft zich als volgt voorbereid op de meldplicht datalekken:
Het SWV heeft een analyse gemaakt van de gegevens die worden verwerkt. Inventariseer waar in de onderwijs- en onderzoeksorganisatie welke gegevens worden verwerkt. Oftewel, breng de datastromen van de organisatie in kaart. Let daarbij op gevoelige gegevens die worden verwerkt zoals bijvoorbeeld medische en etnische gegevens van studenten en medewerkers. Denk ook aan de gegevens die in het kader van wetenschappelijk onderzoek worden verwerkt.
• Neem de huidige beveiligingsmaatregelen onder de loep. Inventariseer de mogelijke risico's van verlies van gegevens en pas waar nodig het beveiligingsbeleid aan. Basis voor deze risicoanalyse kan het SURFnet model Privacy Impact Assessment4 of de Hoger Onderwijs Referentie Architectuur (HORA) zijn waar al in staat aangegeven welke gegevensentiteiten vertrouwelijke gegevens bevatten.
• Opstellen duidelijke interne procedure (actieplan); Zorg voor een procedure waaruit duidelijk blijkt wie de verantwoordelijke is en welke afdeling/functionaris betrokken moet worden indien een datalek wordt geconstateerd. Denk hierbij aan het bestuur of hun gemandateerde eigenaar van de gegevens, de functionaris gegevensbescherming, de veiligheidsfunctionaris, de juridische afdeling en niet te vergeten de afdeling communicatie. Beschrijf hierbij de rollen en taken van deze afdelingen/functionarissen en sluit hierbij aan op bestaande processen binnen de instelling. Zo zou bijvoorbeeld de melding van een datalek overeen kunnen komen met de afhandeling van meldingen in het kader van Computer Security Incident Response Teams (CSIRT). In de procedure moet in ieder geval worden geregeld aan wie een datalek intern wordt gemeld, welke maatregelen door wie binnen welke termijnen moeten worden genomen en hoe het datalek naar buiten toe wordt

Rector Hellemonsstraat 1b
4702 RG Roosendaal
Telefoon: 0165 – 330 966
E-mail: secretariaat@po3002.nl

gecommuniceerd. Indien er een functionaris gegevensbescherming aanwezig is moet deze in ieder geval in kennis gesteld worden. Een communicatieplan voor het naar buiten brengen van de melding zal hier ook deel van uitmaken. Denk er verder over na of het datalek gemeld moet worden bij de verzekering en of er een advocaat ingeschakeld moet worden. Zorg ook voor voldoende interne training met betrekking tot deze procedure.

• Zorg voor een strikt beleid met betrekking tot het verwerken van persoonsgegevens. Hiervoor kunt u gebruik maken van het SURFnet model privacy beleid5 . Stel richtlijnen op voor het opslaan van persoonsgegevens door werknemers/studenten op draagbare apparatuur. Het opstellen van een protocol inclusief een procedure voor melding aan de AP en betrokkenen kan hier eveneens deel van uitmaken;

• Inventariseer de contracten met de bewerkers en zorg dat die waar nodig worden aangepast. Neem de verplichting op dat de bewerker onverwijld een melding aan de organisatie moet doen als er bij hem een datalek heeft plaatsgevonden. Vraag aan de bewerker een beschrijving van de gevolgen van de inbreuk en de maatregelen om de gevolgen te verhelpen. Spreek duidelijk met de bewerker af wie bepaalt of een datalek wel of niet meldingsplichtig is (bij voorkeur de instelling). Maak ook duidelijk welke datalekken gemeld moeten worden (dit zijn bij voorkeur alle incidenten en niet alleen de meldingsplichtige beveiligingsincidenten). Regel daarnaast hoe 4 Model privacy impact assessment en PIA risico formulier, versies december 2014, https://www.surf.nl/themas/digitale-rechten/privacy/implementatie-algemene-verordeninggegevensbescherming-avg/privacy-impact-assessment-pia/index.html 5 Model Beleid Verwerking Persoonsgegevens, versie januari 2015, https://www.surf.nl/themas/digitalerechten/privacy/implementatie-algemene-verordening-gegevensbescherming-avg/privacymodelbeleid/index.html Meldplicht datalekken 8/11 wordt omgegaan met eventuele boetes die als gevolg van een datalek bij de bewerker aan de organisatie worden opgelegd. Stel van te voren vast hoe omgegaan wordt met een keten van bewerkers/sub-bewerkers en sub-subbewerkers. Wees duidelijk over de geschillenprocedure hiervoor.

• Overweeg encryptie waardoor melding aan betrokkenen achterwege gelaten kan worden.