STICHTING VOORTGEZET ONDERWIJS EEMSDELTA

Meldplicht datalekken

Status	Goedgekeurd SLO d.d. januari 2022 Goedgekeurd CvO d.d. januari 2022 Goedgekeurd DMR d.d. maart 2022 Goedgekeurd GMR d.d. 28 maart 2022 Plaatsing intranet d.d. juli 2022 Plaatsing website d.d. - Ouderapp d.d. -
Bewaker	Functionaris gegevensbeheer (FG-er)
Herzieningstermijn	Jaarlijks
Documentgeschiedenis	
Aangemaakt d.d.	Februari 2022
Update d.d.	

Wet meldplicht datalekken

Datum	**:**
Status	**: ter informatie (eveneens te verstrekken aan de RvT)**
Ten behoeve van	**: gehele MR (RvT)**
Datum bespreking	**:**

Meldplicht datalekken

De laatste jaren en dan met name de laatste maanden is veel te doen geweest rondom privacy, ook binnen het onderwijswijs, denk bijv. maar aan privacy van leerlinggegevens maar ook breder. Met enige regelmaat komt in het nieuws dat een website is gehackt of laptops zijn gestolen met vertrouwelijke informatie erop, waardoor persoonsgegevens zijn vrijgekomen. Om dergelijke datalekken te voorkomen en om de schade te beperken als dit toch niet lukt, is de Wet meldplicht datalekken (een wijziging van de Wet bescherming persoonsgegevens) aangenomen die per 1 januari 2016 in werking is getreden. Deze wet houdt in dat organisaties -zowel bedrijven als (semi-)overheden- direct via een speciaal daartoe ingericht 'meldloket datalekken' een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. Afhankelijk van de ernst van de datalek moet dit ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Datalek

De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan. Bij een datalek gaat het dus om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Anders gezegd: Er is sprake van een datalek als derden, die geen toegang zouden mogen hebben tot bepaalde **persoonsgegevens**, toch die informatie in handen krijgen

De Wet Bescherming Persoonsgegevens *(Wbp) verstaat in artikel 1a. onder persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;*

In een toelichting op www.rijksoverheid.nl lezen we dat er 3 groepen persoonsgegevens zijn:
Directe persoonsgegevens
Sommige persoonsgegevens geven directe en feitelijke informatie over een persoon. Bijvoorbeeld iemands geboortedatum, adres of geslacht. Dit geldt ook voor gegevens die een waardering geven over een bepaalde persoon. Een voorbeeld hiervan is iemands IQ.
Indirecte persoonsgegevens
Er zijn ook gegevens die indirect iets vertellen over een bepaald persoon. Bijvoorbeeld over de maatschappelijke status van deze persoon. Zo zegt de winst van een eenmanszaak iets over het inkomen van haar eigenaar. Als deze gegevens zijn te herleiden tot een bepaalde persoon is sprake van persoonsgegevens.

Bijzondere gegevens
Bijzondere persoonsgegevens zijn onder andere gegevens over iemands: ras, godsdienst, levensovertuiging, politieke gezindheid, gezondheid, strafrechtelijke verleden, seksuele leven, lidmaatschap van een vakvereniging.

Voorbeelden van datalekken

Tot datalekken kunnen de volgende voorbeelden gerekend worden:
een kwijtgeraakte USB-stick met persoonsgegevens, het laten slingeren van wachtwoorden, een gestolen laptop of een inbraak in een databestand door een hacker, ook het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld) kan al als datalek worden aangemerkt. En zelfs verlies van gegevens zoals bij een brand in het datacentrum terwijl er geen back up beschikbaar is, ziet de wet als een datalek.
Datalekken beperken zich niet alleen tot digitale gegeven; ook persoonsgegevens op papier kunnen worden gelekt. In dit verband wordt het aanbieden aan de afvalverwerker van oude personeelsdossiers als oudpapier als een lek gezien.

NB 1: Persoonsgegeven dienen altijd beveiligd worden opgeslagen; gegevens die niet beveiligd (hoeven) opgeborgen (te) worden vormen geen datalek.
NB 2: Lekken waarbij andere gegevens dan persoonsgegevens verloren zijn geraakt of gestolen worden, zijn geen datalekken.

Inbreuk op beveiliging van gegevens
De meldplicht staat in nauw verband met de beveiligingsverplichting van art. 13 van de Wbp.[1] En heeft alles te maken met de zgn. inbreuk op de beveiliging van persoonsgegevens.
Dit artikel schrijft voor om *passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of een andere vorm van onrechtmatige verwerking*.
Zelfs als goede beveiligingsmaatregelen zijn getroffen kan er echter sprake zijn van een inbreuk op de beveiliging. Beveiligingsmaatregelen kunnen teniet gedaan worden of omzeild. Ook tekortschietende beveiligingsmethoden of fouten van ondergeschikten kunnen leiden tot een inbreuk op de beveiliging. Denk in dit verband aan het eerder genoemde laten slingeren van usb sticks, wachtwoorden of per ongeluk verkeerd adresseren van een email met persoonsgegevens. Deze inbreuken kan de verantwoordelijke worden aangerekend. De betrokkene van wie de persoonsgegevens openbaar zijn

[1] Artikel 13
De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

geworden heeft altijd de mogelijkheid om de verantwoordelijk aansprakelijk te stellen voor schade die ontstaan is door het vrijkomen van de gegevens.

Al of niet melden datalek

De Autoriteit Persoonsgegevens is toezichthouder en ziet als overheidsinstantie toe op een zorgvuldig gebruik van persoonsgegevens. Bij deze autoriteit moet een datalek gemeld worden. Of een datalek wel of niet gemeld moet worden, hangt af van de ernst van het datalek: melding is alleen nodig als een datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als een aanzienlijke kans bestaat dat dit gebeurt.

De Autoriteit Persoonsgegevens slaat de melding op in een register met alle ontvangen meldingen over datalekken. Dit register is niet openbaar. Overigens worden meldingen überhaupt niet openbaar gemaakt; het is namelijk belangrijk dat gegevens over de beveiliging van de gegevensverwerking of over gelekte persoonsgegevens vertrouwelijk blijven. Soms maakt een organisatie (=verantwoordelijke) m.b.t. verwerking van persoonsgegevens gebruik van een dienst van een andere organisatie (=bewerker). Mocht zich hier onverhoopt een datalek voordoen dan is de verantwoordelijke organisatie verantwoordelijk voor de melding. De verantwoordelijke organisatie moet ervoor zorgen dat zij tijdig weet dat er sprake is van een datalek. Er zullen daarom schriftelijke afspraken moeten worden gemaakt waarin wordt vastgelegd op welke wijze de verantwoordelijke door de bewerker op de hoogte wordt gesteld van een datalek. Het is aan te bevelen om in een zgn. bewerkersovereenkomst op te nemen dat de bewerker aan de verantwoordelijke organisatie meldt dat er sprake is van een eventuele datalek.

Inhoud van de melding

Een datalek moet binnen 72 uur gemeld worden bij de toezichthouder.
De melding aan de toezichthouder omvat in elk geval:

- de aard van de inbreuk;
- de instanties waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

Informeren betrokkenen

In bepaalde gevallen dienen ook de betrokkenen geïnformeerd te worden over het datalek. Dat zijn de personen van wie de gegevens zijn verwerkt.
Zij hoeven alleen geïnformeerd te worden **als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer.** Vaak zullen zij naar aanleiding van het lek direct actie moeten ondernemen, bijvoorbeeld als het gaat om loginnaam en wachtwoord die veranderd moeten

worden. De melding aan betrokkenen kan eventueel achterwege gelaten worden als er passende technische beschermingsmaatregelen zijn getroffen, waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Bijvoorbeeld goede encryptie.
De melding omvat in elk geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken. Het College Bescherming Persoonsgegevens heeft beleidsregels gepubliceerd die kunnen helpen om te bepalen of sprake is van waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkenen. Ook helpen deze beleidsregels met de vraag of de door de organisatie getroffen technische beschermingsmaatregelen de gegevens onbegrijpelijk of ontoegankelijk hebben gemaakt voor onbevoegden. Zijn betrokkenen niet geïnformeerd over het datalek terwijl dit volgens de wet wel noodzakelijk is, dan kan de Autoriteit Persoonsgegevens vragen om dat alsnog te doen. Overigens kunnen betrokkenen zelf ook een datalek melden.

Logboek met datalekken bijhouden

Een organisatie heeft de plicht een logboek bij te houden van alle lekken die ernstig genoeg waren om aan de toezichthouder te moeten melden.
Preciezer geformuleerd (art. 34a): *"De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens."* Denk hierbij aan de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Als het datalek ook aan de getroffen personen is gemeld, is het belangrijk de communicatie hierover te bewaren. Voor het bewaren van de voornoemde gegevens dient uitgegaan te worden van een minimale bewaartermijn van één jaar.

Mogelijk extra kosten na datalek

Als persoonsgegevens door een datalek of fout geopenbaard worden, kan daar schade uit voortvloeien voor de betrokkenen. De aansprakelijkheid voor die schade ligt bij de organisatie die de fout heeft gemaakt. Deze aansprakelijkheid is niet nieuw, maar door de brede meldplicht zullen fouten eerder bekend worden. Dat zal leiden tot meer schadeclaims van de personen die slachtoffer zijn geworden van een datalek.

Implicaties voor de Stichting Voortgezet Onderwijs Eemsdelta

De stichting Voortgezet Onderwijs Eemsdelta (hierna: de stichting) als onderwijsorganisatie beschikt over persoonsgegevens van verschillende groepen o.a. (oud)medewerkers, sollicitanten, stagiaires, (oud)leerlingen, ouders, vrijwilligers. Het is niet alleen zaak om deze conform de Wbp te verwerken maar tevens om ervoor te zorgen dat deze gegevens door de juiste d.w.z. daartoe geautoriseerde medewerkers worden verwerkt voor het daartoe strekkend doel.

Passende technische en organisatorische maatregelen

De Wbp schrijft in artikel 13 voor dat de verantwoordelijke van de organisatie i.c. de directeur/bestuurder van de stichting ervoor te zorgen dat deze gegevens door middel van passende technische en organisatorische maatregelen worden beveiligd tegen verlies of tegen enige vorm van onrechtmatige verwerking. In dit verband wordt onderstaand aangegeven welke acties er nodig zijn om aan te kunnen voldoen aan de Wbp en aan de Wet meldplicht datalekken.

ACTIELIJST

Dit overzicht wordt de MR en de RvT ter kennisname aangeboden. Daar waar de (p)MR c.f. het reglement medezeggenschap een formele speelt zal de (p)MR gevraagd worden om advies dan wel instemming.

Nr	Onderwerp	Verantwoordelijke	MR	Status	
1	Invoeren c.q. actualiseren privacyreglement verwerking gegevens personeel (incl overzicht wettelijke bewaartermijn)	Dir/best	instemmen		
2	Invoeren c.q. actualiseren privacyreglement verwerking gegevens leerlingen (incl overzicht wettelijke bewaartermijn)	Dir/best	Instemmen		
3	Ontwerpen procedure melding en afhandeling datalekken (incl. : wie beoordeelt een evt. datalek/wie doet de melding/wie informeert betrokkenen etc alsmede beleidsregels die bepalen of er sprake van ernstige nadelige gevolgen)	Data Sec. Off.	nee		
4	Ontwerpen en invoeren logboek i.g.v. datalek	Data Sec. Off	nee		
5	Opstellen protocol/werkvoorschrift inzake vernietiging van persoonsgegevens na bewaartermijn				
6	Inventariseren van gebruikers van door de stichting verschafte ict-middelen die buiten de werkplek om gebruikt kunnen worden (o.a. mobiele telefoons, laptops, tablets etc)	ICT-coord.	nee		

7	Inventariseren van externe bewerkers van persoonsgegevens	P&O	nee		
8	Opstellen bewerkingsovereenkomsten met externe bewerkers incl. een non disclosure agreement	P&O, Data Sec. Off.	nee		

INTERN → Procedure melding en afhandeling datalek tbv D/B

Inleiding

Dit document beschrijft de verschillende stappen die binnen de stichting Voortgezet Onderwijs Eemsdelta (hierna: de stichting) genomen worden bij een datalek, dat valt onder de Meldplicht Datalekken. De meldplicht datalekken is een wijziging van de Wet Bescherming Persoonsgegevens (Wbp)en is met ingang van 1 januari 2016 in werking getreden. Op 25 mei 2018 is de vernieuwde AVG van kracht geworden. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van Wbp). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

Datalekken kunnen o.a. ontstaan door:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick, mobiele telefoon of laptop;
- verzenden van email met emailadressen van alle geadresseerden of het verzenden van onbedoelde bijlagen.
- het onrechtmatige verwerking van gegevens .

Constatering dan wel vermoeden van datalek

Indien een medewerker vaststelt dat er sprake is van een datalek dan wel een ernstig vermoeden heeft van een datalek, stelt hij onmiddellijk zijn directeur hiervan op de hoogte. Laatstgenoemde stelt terstond daarna de directeur/bestuurder op de hoogte.

Melden

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd. De melding kan door iedere medewerker en iedere (externe) bewerker worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van de stichting. De melding van laatstgenoemde moet vervolgens dan direct worden gedaan bij één van de directeur dan wel bij de directeur/bestuurder. Indien de directeur/bestuurder beslist dat er sprake is van een datalek

waarvoor op grond van de richtsnoer van het College Bescherming Persoonsgegevens (CBP) een meldingsplicht bestaat dan zal hij het lek direct –doch uiterlijk binnen twee dagen- melden bij de Autoriteit Persoonsgegevens (vm. CBP). Indien de inbreuk op persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkene dient deze onverwijld in kennis te worden gesteld van de inbreuk. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. In het geval van de stichting zijn dit over het algemeen personeelsleden dan wel leerlingen en/of hun ouders. Een (externe) bewerker van persoonsgegevens is verplicht om een datalek te melden bij de verantwoordelijke i.c. de directeur/bestuurder van de stichting.

Vastlegging door vestigingsdirecteur

Indien de melding wordt gedaan bij de directeur dan legt deze in ieder geval schriftelijk vast

- naam van de melder;
- datum en tijd van de melding;
- aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- welke persoonsgegevens vallen onder de melding;
- om welk aantal en/of gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen;
- de contactpersoon voor de melding.

Crisisteam datalek → eerste analyse

De directeur/bestuurder zorgt ervoor dat direct na de melding van de datalek of een ernstig vermoeden daarvan de Datasecurity Officer op de hoogte wordt gebracht. Deze zorgt er vervolgens voor dat het Crisisteam Datalek bijeengeroepen wordt.
Dit team bestaat uit de volgende functionarissen:

a. de directeur/bestuurder;
b. de datasecurity officer;
c. de verantwoordelijk directeur van de afdeling waar het lek is geconstateerd;
d. het hoofd ICT (afhankelijk van de aard van het datalek);
e. het hoofd HRM (afhankelijk van de aard van het datalek).

Tijdens deze bijeenkomst van het crisisteam wordt beoordeeld of er daadwerkelijk sprake is van een datalek c.q. van een inbreuk en of deze redelijkerwijs leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden. Is dit volgens de directeur/bestuurder niet het geval, dan vindt alleen registratie van de melding plaats.

Acties van de responseteam datalek ingeval van melding plichtig datalek

Het Crisisteam datalek o.l.v. de directeur/bestuurder bespreekt en legt in ieder geval vast:

- het opstarten van noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- de melding aan de Autoriteit Persoonsgegevens (vm CBP);
- de wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en manager(s);
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;
- het al dan niet doen van aangifte en vaststellen of er sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit de stichting zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de juridisch adviseur;
- hetgeen intern gecommuniceerd wordt en op welk moment;
- hetgeen extern gecommuniceerd wordt en op welk moment. Er wordt vastgesteld of de pers dan wel de onderwijsinspectie geïnformeerd moet worden;
- of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd worden;
- of er individuen en /of instellingen geïnformeerd moeten worden;
- op welke wijze er intern wordt gerapporteerd;
- of eventuele schade is gedekt door een verzekeringspolis.

Bovenstaande punten worden vastgelegd in het logboek Datalek.

Melding bij de Autoriteit Persoonsgegevens

De directeur/bestuurder meldt binnen 2 dagen het datalek bij het Autoriteit Persoonsgegevens.

<u>In ieder geval zal gemeld moeten worden:</u>

- aard van de inbreuk, om welke persoonsgegevens het gaat, de betrokken categorieën, aantal betrokkenen, aantal gegevensrecord;
- beschrijving van de te verwachten gevolgen;
- getroffen en/of voorgestelde maatregelen;
- informatie reeds genomen en nog te nemen maatregelen door de stichting dan wel door betrokkene(n) om de nadelige gevolgen te beperken;
- contactgegevens voor betrokkene(n).

Ontvangstbevestiging Autoriteit Persoonsgegevens

Is er een melding gedaan, dan ontvangt de stichting een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal deze contact opnemen met de stichting om de herkomst van de melding te verifiëren.

INTERN → Melding datalek (logboek procedure)

Nr.	Onderwerp	Opmerkingen
1	**Oorspronkelijke melding** (inhoud, gemeld door wie bij wie en wanneer)	
2	**Omschrijving van het lek** (welke concrete gegevens zijn gelekt, om welke aantal en/of gegevensrecords gaat het)	
3	**Eerste inschatting van betrokken (groepen) personen** (wie worden er mogelijk 'geraakt' door het lek)	
4	**Directe actie door melder** (heeft melder zelf direct actie ondernomen, zo ja welke en met welk doel)	
5	**Directe actie door directeur** (welke acties, wie erbij betrokken en met welk doel)	
6	**Informeren directeur/bestuurder** (door wie gedaan en wanneer)	

Nr.	**Onderwerp**	**Opmerkingen**
7	**Acties van directeur/bestuurder** (welke en wanneer en met welk doel)	
8	**Betrokkenen** (wie zijn betrokkenen en waarom)	
9	**Ernstig nadelig gevolgen** (is er sprake van ernstige nadelige gevolgen voor betrokkenen, waarom wel of niet> indien wel< inhoud van de gevolgen en voor wie)	
10	**Informeren betrokkenen** (waarom wel of niet geïnformeerd, indien wel > wanneer en door wie)	
11	**Bijeenroepen crisisteam datalek** (is team bijeengeroepen, waarom wel of niet > indien wel, door wie en wanneer bijeenkomst)	
12	**Acties van crisisteam datalek** (welke acties, door wie en wanneer gerealiseerd)	

Nr.	**Onderwerp**	**Opmerkingen**
13	**Informeren Autoriteit Persoonsgegevens** (is deze geïnformeerd, waarom wel of niet > indien wel, door wie, wanneer en op welke wijze, met wie gesproken, inhoud melding)	
14	**Aangifte strafbaar feit** (is er aangifte gedaan, waarom wel of niet > indien wel, bij wie en door wie is aangifte gedaan en wat was de inhoud).	
15	**Interne communicatie** (waarom wel of niet > indien wel, met wie en door wie is er buiten het crisisteam gecommuniceerd, waarom, wanneer en wat was de inhoud)	
16	**Externe communicatie** (waarom wel of niet > indien wel, met wie en door wie is er extern gecommuniceerd, waarom, wanneer en wat was de inhoud)	
17	**Andere** …….	

18	**AANVULLING** Verslagen van crisisteam worden toegevoegd	