# Reglement Datalekken

Vaststelling/ goedkeuring/ positief advies
DiB, GMR, RvT, BMT dd. 01-01-2023

SKOWF
Kerkstraat 79
1687 AM Wognum
0229 - 544 810
info@skowf.nl
SKOWF.NL

# Inhoudsopgave

## Aanleiding

Geregeld meldt de media dat gegevens van werknemers, leerlingen of patiënten letterlijk op straat liggen; dossiers die worden aangeboden als oud papier, een gestolen smartphone of een verloren USB-stick. Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, is sprake van een datalek. Een datalek is niet per se een digitaal lek. Het risico op dat soort datalekken wordt groter, omdat persoonsgegevens in steeds meer databanken en/of op -dragers zijn opgeslagen. Er zijn verschillende categorieën datalekken; bepalend is dat sprake moet zijn van:

*inbreuk op een beveiligingsmaatregel en dat er ernstige nadelige gevolgen zijn voor de privacy van betrokkene(n).*

De meldplicht datalekken is per 1 januari 2016 van kracht.

Het reglement meldplicht datalekken SKO West-Friesland is onderdeel van een reeks reglementen en richtlijnen op het gebied van borging van de privacy van leerlingen, ouders/verzorgers en medewerkers van Stichting SKO West-Friesland. Het reglement is gebaseerd op: de meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) / Beleidsregels voor toepassing van artikel 34a van de Wbp.

**Doel**

In dit reglement wordt uiteengezet wat nodig is om aan de meldplicht datalekken te voldoen. [1] Stichting SKO West-Friesland kiest voor een centrale procedure, waarbij twee dagen doorlooptijd (van ontdekking van het datalek tot de melding aan de Autoriteit Persoonsgegevens (AP)) wordt geborgd. De melding aan de AP wordt centraal gedaan door het bestuur / een aangewezen functionaris van het bestuurskantoor. De scholen, en overige partijen zoals samenwerkingspartners die persoonsgegevens verwerken, melden door hen ontdekte datalekken aan het bestuur/ de functionaris. De interne SKO West-Friesland procedure legt focus op de geldende criteria en de verantwoordelijke ‘spelers’ in de procedure.

**Wat is een datalek?**

Bij een datalek gaat het 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 daarmee niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Een datalek is een incident dat valt onder de categorie van beveiligingsincidenten.

1. De meldplicht datalekken valt onder de Wet Bescherming Persoonsgegevens (Wbp) De meldplicht datalekken is beschreven in de beleidsregels voor toepassing van artikel 34a van de Wbp.

**Wat is een beveiligingsincident?**
Onder een beveiligingsincident wordt een inbreuk verstaan op de beveiliging die leidt tot grote kans op ernstige nadelige gevolgen, dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die worden verwerkt.

Een datalek kan nadelige gevolgen hebben voor persoonlijke levenssfeer van betrokkene(n) doordat de weggelekte gegevens oneigenlijk gebruikt worden. Identiteitsfraude is hiervan een voorbeeld. Ook kan gedacht worden aan ongewenste profilering of doorbreking van bewust gekozen anonimiteit. Om nadelige consequenties voor de bescherming van persoonsgegeven te beperken, is de meldplicht datalekken per 1 januari 2016 van kracht. Dit houdt in dat de verantwoordelijke een [2] verplichting heeft om datalekken te melden. Onderwijs- en onderzoeksinstellingen die persoonsgegevens verwerken moeten bepaalde inbreuken op de beveiliging, die leiden tot diefstal, verlies of misbruik van persoonsgegevens, rapporteren aan zowel de Autoriteit Persoonsgegevens als aan betrokkenen . Als een instelling hieraan niet voldoet, riskeert zij een boete van maximaal [3] 820.000 euro. Dit kan in de toekomst veranderen/

De meldplicht heeft, zoals gezegd, alleen betrekking op doorbrekingen van de maatregelen voor de beveiliging van persoonsgegevens.

**Wanneer moet melding worden gedaan aan de AP?**
Om te beoordelen of een datalek gemeld moet worden, zijn drie vragen van belang. Alle drie moeten bevestigend beantwoord worden:

1. Is er sprake van een inbreuk op de beveiligingsmaatregelen (een datalek)?
2. Zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
3. Heeft deze blootstelling geleid tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de privacy van de betrokkenen?

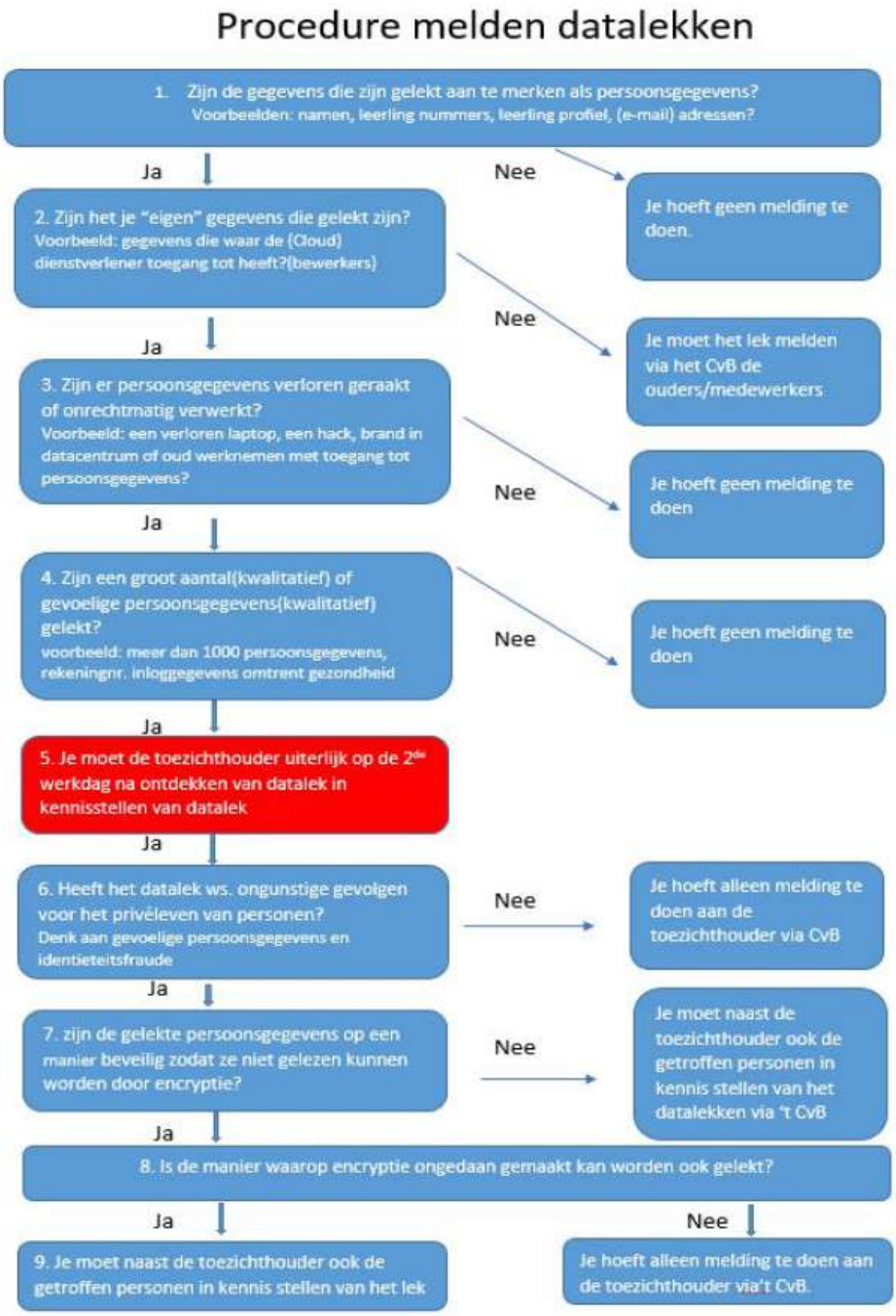
Bij de beantwoording van de eerste vraag moet niet alleen gedacht worden aan actieve handelingen om de beveiliging te doorbreken, zoals hacken van bestanden, maar moet ook diefstal of verlies van dragers waarop persoonsgegevens zijn opgeslagen worden meegenomen. Wanneer gegevens zodanig zijn beveiligd (encryptie) dat redelijkerwijs is uitgesloten dat een datalek leidt tot kennisname van persoonsgegevens door onbevoegden, kan melding aan de AP en betrokkene(n) achterwege blijven. Blootstelling aan ernstige nadelige gevolgen in de vorm van onrechtmatige verwerking moet objectief en naar feitelijke omstandigheden van het geval worden vastgesteld.

2 De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen: het bevoegd gezag.

3.De betrokkene is degene op wie een persoonsgegeven betrekking heeft, al dan niet vertegenwoordigd door diens wettelijke vertegenwoordiger. In dit reglement gaat het om leerlingen.

Bij de beantwoording van de laatste vraag zijn vooral: de aard en omvang van de inbreuk van belang, de aard van de gelekte persoonsgegevens en de mate waarin technische beschermingsmaatregelen zijn getroffen op de desbetreffende persoonsgegevens. Het gaat om een inschatting van de ernst van de gevolgen. *Bij twijfel: intern aan het bestuur via de functionaris van het bestuurskantoor!*

Het onderstaande schema beschrijft de beslispunten in het kort:




Voor aanpassing schema infographic procedure melden datalek

**Hoe moet melding worden gedaan aan de AP?**
De procedure geeft aan:

1. Wie de verantwoordelijke(n) is (/zijn) en;
2. Welke afdeling/functionaris/betrokken wordt als een datalek wordt geconstateerd (het bestuur of een gemandateerde eigenaar van de gegevens, een functie op het gebied van gegevensbescherming, een soort veiligheidsfunctionaris;
3. De rollen en taken van deze afdelingen/functionarissen moeten worden vastgelegd. Aansluiting op bestaande processen binnen de instelling is daarbij een pré. Zo kan de procedure nauw aansluiten op de procedure van beveiligingsincidenten, die de afhandeling van beveiligingsincidenten beschrijft. In de procedure moet in ieder geval worden geregeld aan wie een datalek intern wordt gemeld, welke maatregelen door wie, binnen welke termijn moeten worden genomen en hoe het datalek naar buiten wordt gecommuniceerd. Een communicatieplan voor het naar buiten brengen van de melding maakt hier deel van uit. Als laatste moet worden nagegaan of het datalek gemeld moet worden bij de verzekering en of misschien een advocaat ingeschakeld moet worden. Deze procedure moet vergezeld gaan van voldoende interne training;
4. Voor Stichting SKO West-Friesland is, zoals gezegd, gekozen voor een centraal georganiseerde procedure. Dat houdt in dat ongeacht de plaats van ontdekken van het datalek het bestuur/de aangewezen medewerker van het bestuurskantoor verantwoordelijk is voor het doen van de melding aan de AP en/of de betrokkene(n). Dit betekent dat de medewerkers van de scholen en de diverse samenwerkingspartners de zogenaamde bewerkers na ontdekking van een datalek melding doen aan de verantwoordelijke [4] medewerker van het bestuur bureau Stichting SKO West-Friesland. Ook als getwijfeld wordt of het wel om een datalek gaat.

**De stappen in de procedure: wie doet wat bij een incident?**
*1. Actie: school, bewerker, bestuurskantoor:* Als een incident plaats heeft gehad, wordt vastgesteld of het gaat om een beveiligingsincident. Als dat niet zo is, wordt het incident gemeld aan de afdeling ICT en stopt de procedure. Als het om een beveiligingsincident gaat, wordt bezien of het om een datalek gaat. Als dat inderdaad zo is, wordt melding gedaan aan het bestuur of de 'eigenaar'/ beschermer van de betreffende persoonsgegevens. Ook bij twijfel of het om een datalek gaat wordt melding gedaan aan het bestuur of de 'eigenaar'/ beschermer van de betreffende persoonsgegevens. Als het niet om een datalek gaat, wordt (in geval van een beveiligingsincident, waarbij het gaat om bijvoorbeeld elektronische gegevensdragers) de afdeling ICT gevraagd het incident op te lossen. Het verzoek wordt via een melding of ticket ingediend.

4 Een bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen. Van verwerking door een bewerker is bijvoorbeeld sprake bij het verwerken van persoonsgegevens in de Cloud of bij externe hosting van een website waar persoonsgegevens worden verwerkt.

2. Actie: bestuur/ functionaris bestuurskantoor. Stel vast dat het daadwerkelijk om een datalek gaat: er is een aanzienlijke kans dat het lek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens die worden verwerkt. Indien er geen sprake is van een datalek, wordt het lek als een beveiligingsincident gemeld bij ICT die voor een oplossing van het beveiligingsincident zorgt. De drie vragen, die gesteld worden:

a. Is er sprake van een inbreuk op de beveiligingsmaatregelen (een datalek)?
b. Zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
c. Heeft deze blootstelling geleid tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de privacy van de betrokkenen?

Zijn alle drie vragen bevestigend beantwoord, dan worden verdere acties ondernomen om te melden. Zijn de vragen ontkennend beantwoord, dan wordt de procedure gestopt.

*3. Actie: bestuur/ functionaris bestuurskantoor.* De drie vragen zijn bevestigend beantwoord. Stel nu een communicatieplan voor de melding samen. Voor deze actie en de vervolgacties geldt, dat sprake is van een samenwerking tussen het bestuur of de verantwoordelijke functionaris binnen het bestuurskantoor en overige betrokkenen. Het formeren van een 'taskforce' of datalekmeldingsteam is afhankelijk van het type datalekmelding en welke afdelingen en medewerkers het betreft. Als bij de analyse van het datalek duidelijk is dat een of meerdere leerlingen en / of ouders ingelicht moeten worden, is een rol van de schooldirectie gewenst. De school staat immers dichter bij de betrokkenen. Als een relatie bestaat tussen het lek en P&O, huisvesting, of B&F of actie van deze afdelingen is nodig dan worden acties bij deze afdelingen belegd.

*4. Actie: bestuur /functionaris bestuurskantoor.* Meld het datalek bij de AP. Maak deze actie onderdeel van het communicatieplan. Een daartoe aangewezen functionaris doet de uiteindelijke melding aan de AP.

*5. Actie: bestuur/ functionaris bestuurskantoor.* Komt uit de analyse van het datalek naar voren dat de betrokkene(n) moet worden ingelicht: meld het datalek aan de betrokkene(n). Maak deze actie onderdeel van het communicatieplan. Is de betrokkene(n) een leerling of een ouder/ verzorger dan wordt in overleg met de directie van school overlegd wie de betrokkene(n) informeert.

*6. Actie bestuur/ functionaris bestuurskantoor.* Komt uit de analyse van het datalek naar voren dat de verzekeraar moet worden ingelicht: meld het datalek aan de verzekeraar. Maak deze actie onderdeel van het communicatieplan. Een daartoe aangewezen functionaris doet de uiteindelijke melding aan de verzekeraar.

7. Actie bestuur/ functionaris bestuurskantoor. Komt uit de analyse van het datalek naar voren dat een wetstechnisch consultant moet worden ingelicht: meld het datalek aan de consultant. Maak deze actie onderdeel van het communicatieplan. Een daartoe aangewezen functionaris doet de uiteindelijke melding aan de consultant.

*8. Actie: afdeling ICT.* Dichten van het beveiligingsincident. Zorg dat het beveiligingsincident wordt opgelost. Bepaal of dit incident binnen de procedure van “reguliere” incidenten valt, of laat het incident onderdeel blijven van deze procedure. Maak deze actie onderdeel van het communicatieplan. Communicatie vindt plaats binnen de reguliere incidentbeheer-procedure of binnen de meldplicht datalekken procedure.

*9. Actie: afdeling ICT.* Dichten van het beveiligingsincident/ het datalek: Zorg dat het datalek wordt opgelost. Maak deze actie onderdeel van het communicatieplan. Communicatie vindt plaats binnen de meldplicht datalekken procedure.

**Bijlage:**
**Veelgestelde vragen**

Wat moet de organisatie weten over de meldplicht datalekken?

1. **Moet de onderwijsorganisatie straks elk datalek registreren?**
Nee, de verplichting om binnen de instelling een overzicht bij te houden van alle inbreuken is niet nodig, gezien de lasten die dit met zich meebrengt. Het uitvoeren van de juiste acties in de daartoe bestemde procedures en het tijdig en doeltreffend behandelen van het lek is voldoende.

**2. Moet de onderwijsorganisatie straks elk datalek gaan melden?**
Ook als een medewerker bijvoorbeeld een telefoon of usb-stick verliest? Nee, alleen een datalek met ernstige nadelige gevolgen voor de privacy van de betrokkenen moet worden gemeld. Gaat het bijvoorbeeld om het verliezen van een telefoon van een medewerker en de telefoon is goed beveiligd, dan hoeft het verlies normaal niet te worden gemeld. Is de telefoon echter niet goed beveiligd en bevat deze gevoelige gegevens van betrokkenen, bijvoorbeeld verzuimgegevens, dan dient het datalek wel te worden gemeld.

**3. Hoe dient de melding eruit te zien?**
In geval van een datalek dient te worden geregistreerd en eventueel aan de AP te worden doorgegeven
- de aard van de inbreuk,
- de persoon of instantie waar meer informatie kan worden verkregen en
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken. Bij een melding aan de AP dient daarnaast te worden gemeld
- de gevolgen van de inbreuk voor de verwerking van persoonsgegevens en
- de maatregelen om deze gevolgen te verhelpen.

**4. Moet de instelling een datalek ook melden aan de betrokkenen?**
Als een datalek ernstige nadelige gevolgen heeft voor de privacy van de betrokkenen en indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer, dan moet dit ook aan de betrokkenen worden gemeld. Het informeren aan de betrokkenen kan achterwege worden gelaten als de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens, tenzij de AP alsnog beveelt om een melding aan de betrokkenen te doen. De melding aan de betrokkene moet op een zodanige wijze gebeuren dat deze op een behoorlijke en zorgvuldige wijze wordt geïnformeerd.

**5. Wanneer moet de organisatie een boete betalen? En hoe hoog zal deze boete zijn?**
De AP kan handhavend optreden als niet aan de verplichtingen met betrekking tot de meldplicht datalekken wordt voldaan. Er gelden geen vaste boetebedragen. De AP is vrij te bepalen óf en welk

boetebedrag zij in een gegeven geval wenselijk acht. Onder de wetswijziging van de WBP (meldplicht datalekken) kan de AP een boete opleggen van maximaal EUR 820.000.

**6. Welke afspraken moet ik maken met mijn leveranciers?**
Met betrekking tot de contracten met de leveranciers legt de wetgever de verplichting dat de leverancier een melding aan de onderwijsorganisatie doet als er bij hem een datalek heeft plaatsgevonden. Daarnaast is het raadzaam afspraken te maken over hoe partijen omgegaan met eventuele boetes die als gevolg van een datalek bij de leverancier aan de onderwijsorganisatie worden opgelegd.

**7. De Europese Privacyverordening (AVG) is op komst.**
Heeft dit invloed op de meldplicht datalekken? De Europese Privacy verordening zal de WBP op den duur vervangen. In de ontwerpverordening is een vergelijkbare meldplicht datalekken opgenomen. De AVG kent overigens een nog hoger boetemaximum voor het niet voldoen aan de meldingsplicht. Naar verwachting zal de verordening niet eerder dan in 2016 in werking treden.

**8. Wanneer treedt de wetgeving met betrekking tot de meldplicht datalekken in werking?**
Op het moment van schrijven is de wetswijziging van de WBP (meldplicht datalekken) aangenomen door zowel de Tweede Kamer als de Eerste Kamer. De datum van inwerkingtreding is 1 januari 2016.

**9. Hoe kan onze organisatie zich het beste voorbereiden op de meldplicht datalekken?**
Zorgen voor een goed geïmplementeerde procedure ‘Meldplicht datalekken’ en de nodige voorbereidende acties (in kaart brengen van de dataflows binnen de organisatie, analyse van de huidige beveiligingsmaatregelen en inventarisatie van de mogelijke risico’s bij verlies van gegevens, een strikt beleid met betrekking tot het verwerken van persoonsgegevens (denk aan de juiste autorisatie tot inzien en/of mutatie van deze gegevens, bewerkersovereenkomsten met bewerkers en bezien of encryptie van gegevens op diverse gegevensdragers een oplossing kan bieden.

**10. Wat betekent de meldplicht datalekken voor de beveiliging?**
De meldplicht staat in nauw verband met de beveiligingsverplichting van artikel 13 van de Wet bescherming persoonsgegevens (WBP) op basis waarvan een verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

**11. Wat doet de Autoriteit Persoonsgegevens met de melding?**
De AP richt zich op naleving van de normen van de Wbp en andere wetten en regelingen op grond waarvan persoonsgegevens worden verwerkt. De wijze waarop de AP dit doet is neergelegd in haar Beleidsregels handhaving. De AP geeft prioriteit aan zaken waarbij zij het vermoeden heeft van:

- ernstige overtredingen; structurele overtredingen;

● overtredingen die veel mensen treffen;
● overtredingen waarbij de AP door de inzet van handhavingsinstrumenten effectief verschil kan maken;
● en overtredingen die vallen binnen de (jaarlijkse) aandachtspunten die door de AP bekend zijn gemaakt.

De AP handelt bij de inzet van handhavingsinstrumenten conform de algemene beginselen van behoorlijk bestuur en de Algemene Wet Bestuursrecht. Zij stelt prioriteiten met het oog op de beschikbare middelen en maakt zelfstandig een afweging bij het bepalen van de inzet van handhavingsinstrumenten. De inzet van handhavingsinstrumenten door de AP hangt mede af van de omstandigheden van het geval, waaronder de inhoud en de strekking van de overtreden norm en de daarbij betrokken belangen. Doel, effect en efficiëntie staan voorop. De Memorie van Toelichting (MvT) op de wetswijziging wijst erop dat het geen gegeven is dat de AP iedere melding laat volgen door een onderzoek of andere maatregelen. Volgens de MvT is het feit of een onderzoek of en verdere maatregelen volgen, afhankelijk van de omstandigheden. De AP zal de ingekomen meldingen moeten bezien en daarop reageren in overeenstemming met de door de AP zelf gestelde prioriteiten. Indien een instelling heeft gehandeld op de manier die van hem verwacht mag worden en zelf zo spoedig mogelijk de nodige maatregelen heeft getroffen om het datalek te dichten en herhaling te voorkomen zal een reactie van de AP naar verwachting veelal uitblijven. De AP zal de meldingen wel opslaan mede om daarover in het jaarverslag verantwoording af te leggen.

**12. Valt het verlies van een papieren dossier onder de reikwijdte van de meldplicht?**
Ja, het verlies van een papieren dossier valt ook onder de meldplicht indien er sprake is van inbreuk op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat die ernstige nadelige gevolgen heeft voor de bescherming van de verwerkte persoonsgegevens.

**13. Valt bewust lekken van een medewerker onder de meldplicht?**
Ja, als er redelijkerwijs kan worden aangenomen dat dit leidt tot ernstige nadelige gevolgen voor de privacy van de betrokkenen. Daarnaast is het dus zo dat als er opzet in het spel is, de AP niet verplicht is eerst een bindende aanwijzing te doen, en direct een boete kan opleggen.

**14. Kan de betrokkene zelf ook melden?**
Nee, de meldingsplicht rust op de verantwoordelijke; het is de instelling die de AP onverwijld in kennis moet stellen van een datalek.

**15. Komen er formulieren voor de melding?**
De MvT bij lid 5 van het nieuwe artikel 34a stelt dat er zonodig nadere regels kunnen worden gesteld voor gebruikmaking van een formulier.

**16. Krijg je altijd de maximum boete als je niet meldt?**

Dat is nog niet bekend, maar niet waarschijnlijk. Waarschijnlijk zal de AP hieromtrent boete-beleidsregels vaststellen. Hierdoor krijgen belanghebbenden inzicht over de aard en hoogte van sancties die zij kunnen verwachten bij overtreding van de wet.

**17. Hoe zit het met versleutelde gegevens?**

Als de instelling passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn hoeft de instelling de inbreuk niet te melden aan de betrokkenen. De formulering 'onbegrijpelijk en ontoegankelijk' dekt niet alleen versleuteling maar ook technieken die persoonsgegevens ontoegankelijk kunnen maken als een datalek zich voordoet.

**18. Wat moet een instelling doen als deze de betrokkenen wil informeren maar deze niet weet wie precies betrokkenen zijn of hoe deze te bereiken zijn?**

Dit is afhankelijk van de situatie, maar een instelling zou bijvoorbeeld via berichten in de media aan betrokkenen kunnen laten weten dat er sprake is geweest van een datalek. Het is aan te raden dit in overleg met de afdeling communicatie of P&O te doen.

**19. Moet een instelling de betrokkenen ook laten weten wat ze het beste kunnen doen om de schade te beperken?**

De instelling moet betrokkenen verschillende zaken laten weten:

- 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.

**20. Wat zijn passende maatregelen in het geval van een datalek?**

In geval van een datalek moet de instelling haar interne procedures volgen, het actieplan uitvoeren en het datalek dichten. Hiertoe moet de instelling de omvang van het datalek en de benodigde maatregelen inventariseren. Alle acties en beslissingen moeten gedocumenteerd worden.

**Bijlage:**
**Voorbeeld DIRECTIEMAIL**

Aan....,
In het Directieberaad van ..... is het protocol besproken “Meldplicht Datalekken”. Mat name gericht op toenemend gebruik van digitale leermiddelen, gegevensdragers en digitale registraties en administraties. Maar ook op niet ICT gerelateerde processen en registraties (denk aan papieren lijsten met persoonsgegevens). De belangrijkste vraag is: “Wat te doen, als gegevens kwijtraken? “Het protocol is geaccordeerd.

Wat het protocol verder concretiseert, is een instructie / procedure, die we binnen de scholen en het College van bestuur moeten (en zelfs door onze samenwerkingspartners laten) volgen. De instructie / procedure is zeer beknopt en wordt gecoördineerd vanuit het bestuurskantoor en beleidsgroep Financiën, beheer en ICT.

**Bijlage:**
**DE PROCEDURE**

Samenvatting en werkinstructie meldplicht datalekken Inbreuk op de privacy van persoonsgegevens? Meld dit bij het bestuurskantoor!

Sinds 1 januari 2016 wordt door de overheid strenger toegezien op de privacy van persoonsgegevens binnen bedrijven en instellingen. Stichting SKO West-Friesland is als onderwijsorganisatie verplicht verlies, diefstal en onrechtmatige verwerking van persoonsgegevens – bijvoorbeeld gegevens van leerlingen – te melden aan de Autoriteit Persoonsgegevens (AP). Dit is geregeld in de meldplicht datalekken (zie ook intranet). Voor deze meldplicht is door de overheid een speciaal loket ingesteld. De meldplicht datalekken valt onder de Wet bescherming persoonsgegevens.

Wat is een datalek?

Als persoonsgegevens van jouw school of het bestuurskantoor in handen vallen van derden die geen toegang tot die gegevens mogen hebben, is sprake van een datalek. Voorbeelden van datalekken zijn: inbraak in een school waarbij laptops zijn gestolen, een kwijtgeraakte USB-stick met leerlinggegevens, een personeelsdossier en het hacken van een databestand. Onder een datalek valt niet alleen het vrijkomen van gegevens – door diefstal, verlies of lekken – maar ook onrechtmatige verwerking van gegevens. De getroffen beveiligingsmaatregelen op jouw school of het bestuurskantoor hebben dan niet gewerkt.

Het risico op datalekken is de laatste jaren groter geworden, omdat persoonsgegevens in steeds meer databanken worden opgeslagen. Om persoonsgegevens zo goed mogelijk te beveiligen, gelden binnen Stichting SKO West-Friesland specifieke procedures. Deze zijn beschreven in ons *privacyreglement* .

Werkinstructie: volg de interne procedure

Om aan de meldplicht van de overheid te voldoen, hanteert Stichting SKO West-Friesland een interne procedure. In deze procedure is opgenomen dat je als medewerker van Stichting SKO West-Friesland een datalek intern meldt. Per incident wordt een Taskforce geformeerd die bepaalt welke maatregelen noodzakelijk zijn.

Wanneer meld je een datalek?

De volgende drie vragen helpen je te beoordelen of je een datalek moet melden:
1- Is er sprake van inbreuk op een beveiligingsmaatregel?

2- Zijn persoonsgegevens gestolen, kwijtgeraakt of onrechtmatig verwerkt?
3- Kan dit leiden tot ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens of de privacy van de betrokkene(n)?
Als alle drie vragen met 'Ja' worden beantwoord, moet je het datalek melden. Dit doe je via dit formulier. Wanneer je twijfelt, overleg dan eerst met een collega of je directeur. Blijft de twijfel bestaan, dan altijd melden!

Vragen?

Wil je meer weten en kan je directeur of leidinggevende je niet verder helpen, neem dan contact op met het bestuurskantoor.