



NORMEN KADER IBP

Meldplicht datalekken

Colofon

Versie Versie 1.0, december 2025

Normen **IM.01** Incidentmanagement
IM.02 Incidentescalatie
IM.03 Incidentrespons op (cyber)beveiligingsincidenten
GB.01 Datalekken detectie, classificatie en afhandeling
GB.02 Melding datalekken

Auteurs Dit document is voor VRtL opgesteld door Bert Wolthuis (manager IBP) en Teun de Heer (kwartiermaker PO).

VRtL Van Reest tot Linde (VRtL) is een samenwerking tussen Simant en VOMEQ. Van Reest tot Linde werd als vereniging in het leven geroepen met als doelstelling om meer kwaliteit en besparingen te realiseren. Dit met in gedachte een verwachte krimp en het steeds zoeken naar mogelijkheden om middelen zo veel mogelijk direct voor het onderwijs in te zetten. Tegelijkertijd kan daarmee de kwetsbaarheid bij afnemende formatie worden tegengegaan en de uitwisseling van kennis en deskundigheid worden bevorderd waardoor ook verbreding en verdieping van taken ontstaat. We trekken in VRtL verband samen op om het normenkader IBP in te voeren om zo digitaal veilige scholen te realiseren.

Document historie

<i>Versie</i>	<i>Datum</i>	<i>Auteur</i>	<i>Wijzigingen/opmerkingen</i>
0.1	03-07-2025	Bert Wolthuis Teun de Heer	Vaststellen procedure van melden datalekken door bestuurder.
0.2	31-10-2025	Bert Wolthuis	Concept beleidsplan
	02-12-2025	Kernteam VRtL	Tekstuele aanpassingen
<i>Versie</i>	<i>Datum</i>	<i>Distributielijst</i>	<i>Autorisatie</i>
1.0	11-12-2025		Voorzitter CvB
<i>Versie</i>	<i>Datum</i>	<i>Recht</i>	<i>Medezeggenschap</i>
1.0	30-03-2026	Instemming	Voorzitter GMR

Inhoudsopgave

Inleiding.....	4
Hoofdstuk 1: Datalekken.....	5
1.1 Wat is een datalek.....	5
1.2 Bescherming van persoonsgegevens.....	5
1.3 Herkennen en snel handelen.....	6
1.4 Meldplicht voor medewerkers.....	6
1.5 Meldplicht aan de Autoriteit Persoonsgegevens.....	6
1.6 Meldplicht aan betrokkenen.....	7
1.7 Registratie en rapportage.....	7
1.8 Bewaartermijn.....	7
1.9 Sancties van de Autoriteit Persoonsgegevens.....	7
Hoofdstuk 2: Procedure melden van datalekken.....	8
2.1 Rollen.....	8
2.2 Meldproces.....	8
Hoofdstuk 3: Maatregelen preventie datalekken.....	10
3.1 Preventieve maatregelen.....	10
3.2 Kwaliteitscontrole.....	10

Inleiding

Vanaf 1 januari 2016 moet ieder bedrijf of instelling een beleid hebben inzake datalekken van persoonlijke gegevens. Het doel is om gegevens beter te beveiligen en eventuele betrokkenen zo snel mogelijk in staat te stellen om maatregelen te nemen. Beveiligen van persoonlijke gegevens valt onder de bestuurlijke verantwoordelijkheid. Bij ernstige overtredingen van de wet kunnen boetes worden opgelegd.

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door ontwikkelingen binnen zowel de automatisering, het onderwijs als de regelgeving. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan.

In dit document beschrijven we de voor de school belangrijkste zaken rondom datalekken. In hoofdstuk 1 beschrijven we de uitgangspunten die we hanteren. Deze zijn getoetst aan de Autoriteit Persoonsgegevens en sluiten op ons IBP beleid. In hoofdstuk 2 beschrijven we de procedure die gevolgd wordt bij het constateren van een datalek. Hoofdstuk 3 beschrijft organisatorische- en technische maatregelen ter voorkoming van datalekken.

Dit beleidsplan maakt deel uit van de PDCA-cyclus rondom het normenkader en wordt elke drie jaar getoetst en bijgesteld.

Hoofdstuk 1: Datalekken

In dit hoofdstuk beschrijven we de uitgangspunten. Deze zijn niet vrijblijvend, maar vrij strikt omschreven: dit is waar we ons aan moeten houden. De uitgangspunten zijn getoetst aan de Autoriteit Persoonsgegevens.

1.1 Wat is een datalek

Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is, waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Er zijn 3 soorten datalekken, een datalek kan in meer dan één van deze categorieën vallen:

1. Inbreuk op de vertrouwelijkheid: persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
2. Inbreuk op de integriteit: persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
3. Inbreuk op de beschikbaarheid: de organisatie waar het datalek is (geweest) kan niet meer bij de persoonsgegevens komen. Of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

Voorbeelden van een datalek zijn:

1. Verlies van een USB-stick of laptop met persoonsgegevens.
2. Sturen van mailing met de adressen in het CC-veld (in plaats van BCC-veld). Hierdoor worden alle mailadressen onbedoeld zichtbaar.
3. Documenten met persoonsgegevens blijven onbeheerd achter bij een kopieerapparaat of worden niet versnipperd weggegooid.
4. Het verlies van systeemintegriteit door virussen, malware of cryptolockers.

1.2 Bescherming van persoonsgegevens

In de Algemene verordening gegevensbescherming (AVG) staat dat een organisatie 'passende technische en organisatorische maatregelen' moet nemen om persoonsgegevens te beveiligen. Daarvoor is het noodzakelijk dat de door ons verzamelde, verwerkte en gepubliceerde gegevens te allen tijde beschikbaar, correct en beschermd zijn.

We hebben dit beschreven in ons IBP-beleidsplan, relevante punten in dit kader zijn:

1. We nemen de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. De bestuurder is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is de bestuurder de verwerkingsverantwoordelijke.
2. Binnen de school is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
3. We nemen passende organisatorische- en technische maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
4. We handelen beveiligingsincidenten en datalekken af volgens een vast protocol en in voorkomende gevallen melden we bij de Autoriteit Persoonsgegevens en aan de betrokkenen.

1.3 Herkennen en snel handelen

Snel handelen begint bij het herkennen van een mogelijk datalek. Bewustwording is daarom zeer belangrijk. Medewerkers moeten weten wat een datalek is en waar ze een datalek kunnen melden. Het bewustwordingsprogramma voor medewerkers zal hier jaarlijks aandacht aan besteden.

Het melden van beveiligingsincidenten en datalekken volgt een gestructureerd proces, dat voorziet in de juiste stappen rondom de meldplicht datalekken. Dit proces wordt uitgewerkt in Hoofdstuk 2.

Medewerkers hoeven niet terughoudend te zijn om een datalek intern te melden. Een datalek kan iedereen overkomen. Het is juist professioneel om meteen in actie te komen.

1.4 Meldplicht voor medewerkers

Alle medewerkers, die een beveiligingsincident of datalek vermoeden, dienen dit onverwijld (zo snel mogelijk) te melden volgens de daartoe afgesproken route.

Elke school beschikt over een digitaal formulier dat ingevuld dient te worden bij een (vermoeden van een) beveiligingsincident of datalek.

1.5 Meldplicht aan de Autoriteit Persoonsgegevens

Een melding aan de Autoriteit Persoonsgegevens moet gedaan worden zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek. Melding wordt gedaan bij: <https://datalekken.autoriteitpersoonsgegevens.nl/>.

Volgens de wet moet een melding gedaan worden als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

Niet ieder datalek hoeft gemeld te worden aan de Autoriteit Persoonsgegevens. Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelek, dan is een melding noodzakelijk.

Voorbeelden van gegevens waarbij melding aan de AP noodzakelijk is:

1. Bijzondere persoonsgegevens zoals, gegevens over iemands godsdienst, ras, gezondheid of strafrechtelijke persoonsgegevens.
2. De financiële of economische situatie van de betrokkene, waaronder gegevens over (problematiese) schulden, salaris- en betalingsgegevens.
3. (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
4. 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.
5. Gegevens die kunnen worden misbruikt voor (identiteits-)fraude, zoals kopieën van identiteitsbewijzen en het Burgerservicenummer.

Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelek, 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.

1.6 Meldplicht aan betrokkenen

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

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. Als er persoonsgegevens van gevoelige aard zijn geëkt, dan is het waarschijnlijk dat dit ook gemeld moet worden aan de betrokkene(n).

Een 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 geëkt wachtwoord te vervangen. Hoe eerder de betrokkene daarover is 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. Per geval moet worden bepaald of de maatregelen die zijn genomen voldoende bescherming bieden om de melding aan de betrokkene achterwege te kunnen laten.

1.7 Registratie en rapportage

Alle meldingen van datalekken worden vastgelegd in het incidentenregister van YourSafety-net. Een rapportage over het aantal datalekken maakt onderdeel uit van het jaarverslag van de FG.

Het is van belang om van elkaar te leren. In elk geval zullen alle datalekken die gemeld worden aan de AP, worden besproken in de directieraad/strategische driehoek en de driehoek Simant-Vomeo-VRtL (Bestuur VRtL en kernteam Normenkader).

1.8 Bewaartermijn

Er is geen wettelijke termijn voor bewaarplicht voor de gegevens van datalekken. De gegevens van datalekken die onder de meldplicht vallen zullen door ons minimaal 3 jaar bewaard worden. Hiermee nemen we het advies van de Autoriteit Persoonsgegevens over. De gegevens worden na 1 jaar geanonimiseerd.

1.9 Sancties van de Autoriteit Persoonsgegevens

Zowel het niet melden van een datalek als het ontbreken van adequate beveiliging van de persoonsgegevens kan leiden tot een bestuurlijke boete.

Bij het opleggen van een boete houdt de Autoriteit Persoonsgegevens rekening met alle omstandigheden per datalek. Het feit of de persoonsgegevens wel of niet door derden zijn ingezien is daarbij belangrijk. Voorbeelden van gevallen waarbij een boete opgelegd wordt:

1. Het niet melden van een datalek terwijl dat wel moet.
2. Het niet op orde hebben van de beveiliging.
3. Het verwerken van persoonsgegevens zonder toestemming.
4. Export van persoonsgegevens naar landen buiten de EU zonder dat goed geregeld te hebben.

Hoofdstuk 2: Procedure melden van datalekken

In dit hoofdstuk beschrijven we de manier waarop een beveiligingsincident en/of een mogelijk datalek door de ontdekker kan worden gemeld en hoe het daaropvolgende onderzoek verloopt.

Er kan gemeld worden met behulp van een publiek meldformulier. Dit formulier is beschikbaar in de werkomgeving van alle medewerkers, bijvoorbeeld via TopDesk, het Digiplein of via het medewerkersportaal.

2.1 Rollen

Verschillende medewerkers hebben een rol in de meldprocedure. Dit betreft rollen op schools- en bovenschools niveau. Er is een autorisatiematrix vastgesteld voor de betrokkenen binnen deze procedure.

1. Privacy Officer (Incident Analyst)

Eerstelijns contactpersoon voor incidenten voor een locatie.

Kan incidenten aanmaken, gerapporteerde incidenten beoordelen en eventueel doorzetten naar contactpersoon/analist van de Master-organisatie.

2. Manager IBP (Incident Analyst)

Contactpersoon en analist voor incidenten binnen de gehele Master-organisatie. Kan incidenten aanmaken, gerapporteerde incidenten beoordelen en zo nodig de FG en het IRT alarmeren.

3. Functionaris Gegevensbescherming - FG

Toegang tot incidentenregister: kan incidenten beoordelen en advies geven over aanpak van een incident. Daarnaast ook toegang tot alle beleidszaken, RVV en bibliotheek.

4. Incident Response Team - IRT

Het Incident Response Team wordt op de hoogte gebracht als er een nieuw (potentieel) datalek is gemeld. Het IRT zal het incident onderzoeken en vervolgstappen nemen (lek dichten, melden aan autoriteit/betrokken, oorzaak onderzoeken, etc.).

5. Directie

Voor het doen van een melding bij de Autoriteit Persoonsgegevens en/of aan de betrokkenen moet toestemming worden gegeven door de directie. Bij bovenschoolse incidenten moet het bestuur toestemming geven.

2.2 Meldproces

De volgende stappen worden gevolgd bij het melden en behandelen van een incident:

1. De ontdekker meldt het incident via het vastgestelde meldingsformulier
2. De Privacy Officer (incidentanalist) neemt het incident zo spoedig mogelijk in behandeling.
3. De Privacy Officer verzamelt indien nodig aanvullende informatie en voegt deze toe aan het meldingsformulier.
4. De Privacy Officer maakt een inschatting van de risico's:
 - als het gaat om aanzienlijke risico's, als het een complex incident betreft en/of als het incident betrekking heeft op beide stichtingen, draagt de Privacy Officer de afhandeling over aan de manager IBP.
 - bij twijfel overlegt de Privacy Officer met de manager IBP.
5. De Incident Analyst (PO of manager IBP) beschrijft de risico's en bepaalt welke correctieve maatregelen moeten worden getroffen. Hierbij kan advies worden gevraagd aan:
 - de FG.
 - het IRT.
6. De Incident Analyst maakt een inschatting of de Autoriteit Persoonsgegevens (AP) en/of de betrokkenen moeten worden geïnformeerd. Als dit (mogelijk) het geval is, overlegt de Incident Analyst met:
 - de manager IBP

- de directie (bij bovenschoolse incidenten: het bestuur)
 - een melding wordt alleen gedaan na toestemming van de directie of het bestuur
 - ten aanzien van de wijze van communiceren wordt advies gevraagd bij afdeling communicatie
7. De manager IBP en de FG worden geïnformeerd over de bevindingen, zodat deze in de gelegenheid worden gesteld om zich een oordeel te vormen over de voorgestelde aanpak.
 8. Verdere afhandeling van het incident door (of: onder aansturing van) de Incident Analist.
 - Indien nodig: het incident wordt gemeld aan de Autoriteit Persoonsgegevens (AP), na toestemming van de directie. Een melding moet binnen 72 uur na ontdekking worden gedaan. Als nog niet alle relevante informatie beschikbaar is kan een voorlopige melding worden gedaan.
 - Indien nodig wordt het incident gemeld aan betrokkene, na advies van afdeling communicatie en na toestemming van de directie.
 - Het uitvoeren van de correctieve maatregelen om de gevolgen van het incident zoveel mogelijk te beperken.
 - Aanvullen van het meldingsformulier en/of van de informatie in het incidentregister.
 9. Opvolging van het incident door de Incident Analist om herhaling te voorkomen.
 - Voorstellen preventieve maatregelen.
 - Implementeren preventieve maatregelen.
 - Preventieve maatregelen toevoegen aan het incidentmeldingsformulier.
 10. Het afsluiten van het incidentmeldingsformulier.

Hoofdstuk 3: Maatregelen preventie datalekken

3.1 Preventieve maatregelen

De volgende organisatorische – en technische maatregelen worden genomen om datalekken tegen te gaan.

Organisatorische maatregelen:

1. Een bewustwordingsprogramma voor de medewerkers over hoe veilig om te gaan met persoonsgegevens.
2. Richtlijnen of gedragscodes waarin is vastgelegd wat het gewenste gedrag is voor de betrokkenen van de school.
3. Aandacht voor privacy op bestuurlijk niveau.
4. Toewijzen van verantwoordelijkheden voor informatiebeveiliging.
5. Een standaard afhandeling van datalekken en beveiligingsincidenten.
6. Het opstellen en bijhouden van een register van verwerkingen.
7. Het uitvoeren van een data protection impact assessment (DPIA) voor risicovolle verwerkingen.
8. Procedures om op gezette tijdstippen de beveiligingsmaatregelen te testen, te beoordelen en te evalueren.

Technische maatregelen:

1. Logische en fysieke (toegangs-)beveiliging van apparatuur.
2. Technisch beheer van de autorisaties en bijhouden van logbestanden.
3. Patchbeleid om software, zoals browsers, virusscanners en operating systems up-to-date te houden.
4. Een adequate back-up om de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te kunnen herstellen.
5. Automatisch verwijderen van verouderde gegevens.
6. Versleuteling van gegevens.
7. Pseudonimiseren van persoonsgegevens.

3.2 Kwaliteitscontrole

Het is van belang om de preventieve maatregelen continu te evalueren en daarbij verbetering te realiseren.

Minimaal jaarlijks wordt beoordeeld of de procedure en de uitvoering nog met elkaar in overeenstemming zijn. Indien deze niet met elkaar overeenkomen wordt beoordeeld of de procedure moet worden geactualiseerd of dat medewerkers moeten worden geïnstrueerd op een juiste toepassing van de procedure.

Jaarlijks wordt bekeken of cases die niet aan betrokkenen gemeld zijn, alsnog gemeld moeten worden. Bijvoorbeeld vanwege nieuwe technische ontwikkelingen.