Bijlage XIII Handboek Datalekken

Calvijn College

Inwerkingtreding: 02-06-2021

Inhoudsopgave

1. Inleiding

Sinds 1 januari 2016 is een verwerkingsverantwoordelijke (in dit verband: de school) verplicht om een datalek te melden aan de Autoriteit persoonsgegevens (AP) en mogelijk ook aan de betrokkenen. Per 25 mei 2018 volgt deze meldingsplicht niet langer uit nationale wetgeving, maar uit de Europese Algemene Verordening Gegevensbescherming (AVG).In dit handboek wordt geregeld hoe het bevoegd gezag dient te handelen indien er (mogelijk) sprake is van een beveiligingsincident aangaande de beveiliging van persoonsgegevens waarvoor de school als verwerkingsverantwoordelijke dient te worden aangemerkt en welke afwegingen zij dient te maken om vast te stellen of daadwerkelijk sprake is van een datalek dat moet worden gemeld aan de AP en/of de betrokkene.

Dit handboek is gebaseerd op het bepaalde in artikel 33 en artikel 34 van de AVG, welke bepalingen als volgt luiden:

Artikel 33 Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

1. *Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.*

2. *De verwerker informeert de verwerkingsverwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.*

3. *In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:*

   a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
   b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
   c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
   d) de maatregelen die de verwerkingsverwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4. *Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.*

5. *De verwerkingsverwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.*

Artikel 34 Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

1. *Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.*

2. *De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.*

3. *De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:*

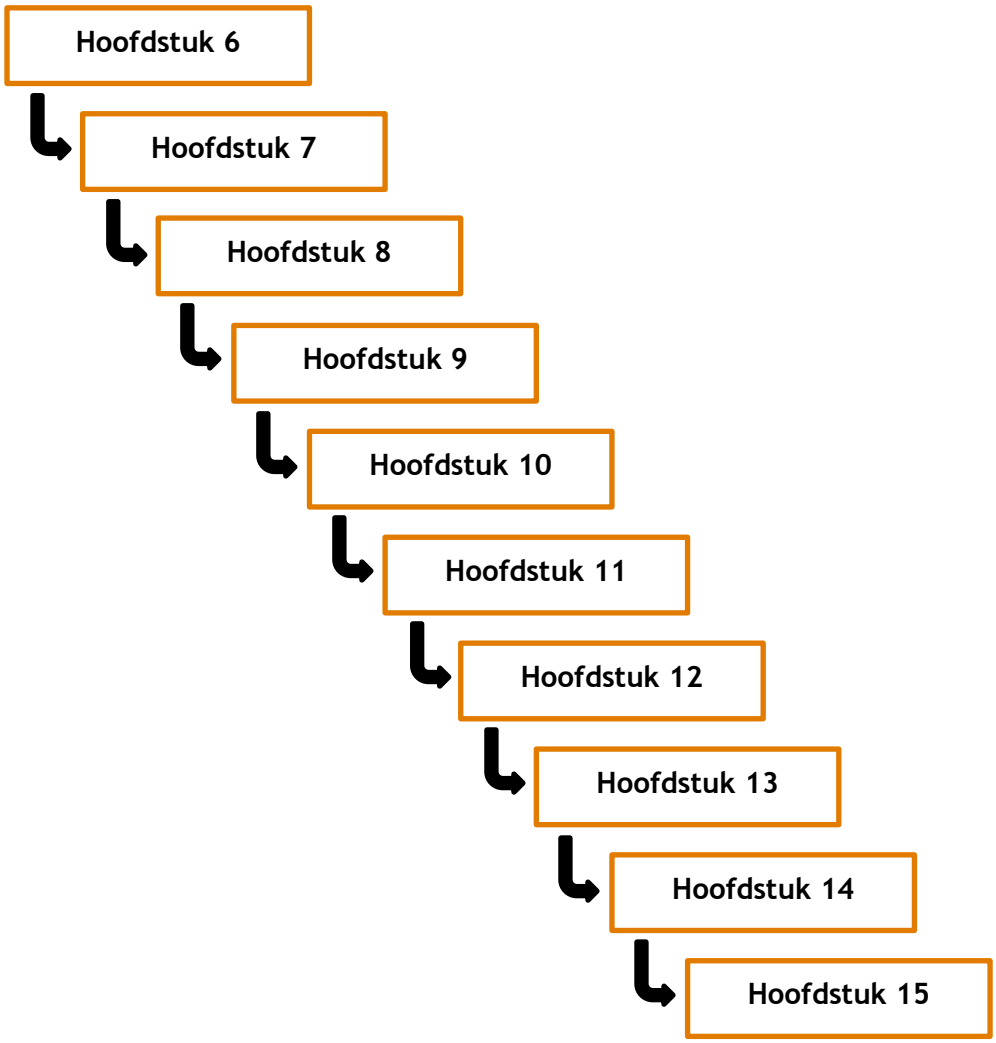
a) de verwerkingsverwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
b) de verwerkingsverwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer voordoen;
c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. *Indien de verwerkingsverwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.*

De inhoud van dit handboek is mede gebaseerd op de nationale Uitvoeringswet AVG en Richtlijnen (guidelines) zoals gepubliceerd door de AP. Tevens is bij dit handboek betrokken hetgeen opgenomen in de Kamerstukken bij wetsvoorstel 33 662, de 'Beleidsregels voor toepassing van artikel 34a van de Wbp' d.d. 8 december 2015. Deze beleidsregels zijn ook na inwerkingtreding van de AVG onverminderd relevant voor de praktische uitwerking van de verplichtingen volgend uit de Verordening.

2. Werkwijze

Dit handboek beschrijft welke stappen de school dient te doorlopen om te kunnen voldoen aan de wettelijke verplichting een datalek – indien noodzakelijk - op de juiste wijze en aan de juiste instanties te melden. Hiertoe is van belang dat indien bij de school een signaal binnenkomt dat er mogelijk sprake is van een beveiligingsincident steeds stap voor stap de hoofstukken 6 tot en met 15 doorlopen. Het beginpunt is daarbij steeds hoofdstuk 6 en vervolgens zal op basis van de opvolgende hoofdstukken opgenomen schema's moeten worden vastgesteld of de school ook toekomt aan het bepaalde in de opvolgende hoofdstukken.



Van belang is voor een goede werkwijze dat alle besluiten die de school neemt op basis van de overwegingen die zij moet maken in het kader van dit handboek schriftelijk en deugdelijk onderbouwd en gemotiveerd vastlegt en bewaard. Dit is onder andere van belang om intern te kunnen monitoren op welke wijze en op basis van welke overwegingen de besluiten zijn genomen.

3. Definities

De onderstaande termen hebben in dit handboek de volgende betekenis:

het bestuur:	vertegenwoordiger van de Stichting;
FG:	de functionaris gegevensbescherming van de school (Data Protection Officer) en wiens gegevens zijn opgenomen in bijlage 2;
leerlingen:	de (oud- en/of aspirant)leerlingen van de school;
personeel:	a) de bij de verwerkingsverantwoordelijke benoemde, directeur, teamleider of leraar, en overige medewerkers benoemd in een andere functie dan het geven van onderwijs, waaronder begrepen de leden van het bestuur van die scholen die zijn benoemd door een toezichthoudend orgaan als bedoeld in artikel 24e1, derde lid van de Wet op het Voortgezet Onderwijs, voor zover die leden mede zijn benoemd op basis van een akte van aanstelling; en b) de onder a bedoelde medewerker die zonder benoeming is tewerkgesteld, tenzij het betreft de toepassing van de artikelen 38a tot en met 39a, 40a, 43a, eerste en tweede lid, 51, eerste tot en met derde lid, 53b en 96o van de wet op het voortgezet onderwijs, voor zover niet anders is bepaald, en de toepassing van daarmee verband houdende wettelijke bepalingen;
persoonsgegevens:	elk gegeven betreffende een geïdentificeerd of identificeerbare natuurlijke persoon (‘de betrokkene’), waaronder in ieder geval uitdrukkelijk begrepen (de ouder(s) en/of verzorger(s)) van de leerlingen en Medewerkers;
school:	de Stichting Calvijn College vertegenwoordigd door het bestuur;
verwerker:	een partij die (als verwerker) in opdracht – en ten behoeve - van de school persoonsgegevens verwerkt, dan wel een partij die (als subverwerker) op zijn beurt in opdracht van de verwerker voornoemde persoonsgegevens verwerkt;

4. Signaleren van een beveiligingsincident

Medewerkers worden onder andere door middel van het protocol Beveiligingsincidenten (bijlage 1) bewust gemaakt onder welke omstandigheden en voorwaarden sprake kan zijn van een beveiligingsincident waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking.

Indien een Medewerker een beveiligingsincident signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de Medewerker dit per omgaande aan de FG ongeacht het tijdstip van de dag.

De FG meldt vervolgens op zijn beurt per omgaande het beveiligingsincident telefonisch aan de voorzitter van het bestuur en het hoofd van de ICT-afdeling en bevestigt dit hen per e-mail, tenzij er gegronde redenen zijn om het beveiligingsincident niet per e-mail te bevestigen (bijvoorbeeld indien daarmee duidelijk zou (kunnen) worden voor hackers dat hun hack is ontdekt).

Iedere Medewerker is te allen tijde bevoegd zelfstandig een melding te doen bij de voorzitter van het bestuur (telefoonnummer/e-mailadres), dus ook bij het ontbreken van een voorafgaande melding aan de FG.

Door middel van de melding aan de FG en/of de voorzitter van het bestuur wordt de procedure als verwoord in dit handboek daadwerkelijk gestart.

5. Incident Response Team

Nadat de voorzitter van het bestuur over een (mogelijk) datalek is geïnformeerd, informeert hij op de kortst mogelijke termijn het IRT. De informatie die de voorzitter van het bestuur daarbij verstrekt is de feiten en omstandigheden ten aanzien van het beveiligingsincident en het verzoek paraat te blijven, tenzij de voorzitter van het bestuur van oordeel is dat gegeven de ernst en aard van het beveiligingsincident het IRT direct in overleg dient te treden, in welk geval hij de leden van IRT kenbaar maakt hoe laat het overleg zal plaatsvinden.

IRT bestaat uit de volgende vaste leden:

1) de voorzitter van het bestuur;
2) de FG; en
3) het hoofd van de ICT-afdeling.

Zo nodig wordt het IRT – na een afweging daartoe van de voorzitter van het bestuur - aangevuld met:

4) de forensisch IT-deskundige;
5) de juridisch adviseur; en/of
6) de communicatieadviseur.

De voorzitter van het bestuur is tevens de voorzitter van het IRT en heeft de plicht er voor zorg te dragen dat er steeds een forensisch IT-deskundige, juridisch adviseur en communicatieadviseur beschikbaar zijn en die op de hoogte zijn van hun (mogelijke) rol binnen het IRT. Voorkomen dient derhalve te worden dat de juridisch adviseur en de communicatieadviseur eerst na de melding van een beveiligingsincident dienen te worden aangezocht en aangesteld.

IRT zal opereren vanuit [adres].

De leden van IRT committeren zich om indien zich een beveiligingsincident zich voordoet en zodra zij zijn geïnformeerd door de voorzitter van het IRT om volledig beschikbaar te zijn ten behoeve van het IRT. Besprekingen, overleg en events die een lid van het IRT heeft gepland binnen een tijdsbestek van 96 uur na door de voorzitter van het IRT op de hoogte te zijn gesteld zal het lid annuleren en/of verplaatsen naar een latere datum en tijdstip. Het lid zal zich ook inspannen om zoveel als mogelijk fysiek aanwezig te zijn.

Binnen het IRT hebben slechts de vaste leden stemrecht. Ieder van de vaste leden heeft één stem. Alle besluiten die het IRT neemt worden schriftelijk vastgelegd en voorzien van de afweging die daaraan vooraf is gegaan.

Besluitvorming door het IRT zal plaatsvinden op basis van volledige en juiste informatie aangaande het beveiligingsincident, tenzij gezien de feiten en omstandigheden een besluit – mede met in acht-neming van de op basis van de AVG geldende termijnen – niet langer kan worden uitgesteld.

6. Verzamelen volledige en juiste informatie

Nadat de voorzitter van het bestuur over een (mogelijk) beveiligingsincident is geïnformeerd, gaat hij – samen met de FG - tevens direct over tot het verzamelen van de volledige en juiste informatie met betrekking tot het (mogelijke) datalek. Bij het verzamelen van die informatie wordt gebruik gemaakt van het Formulier Gegevens Datalek (bijlage 3).

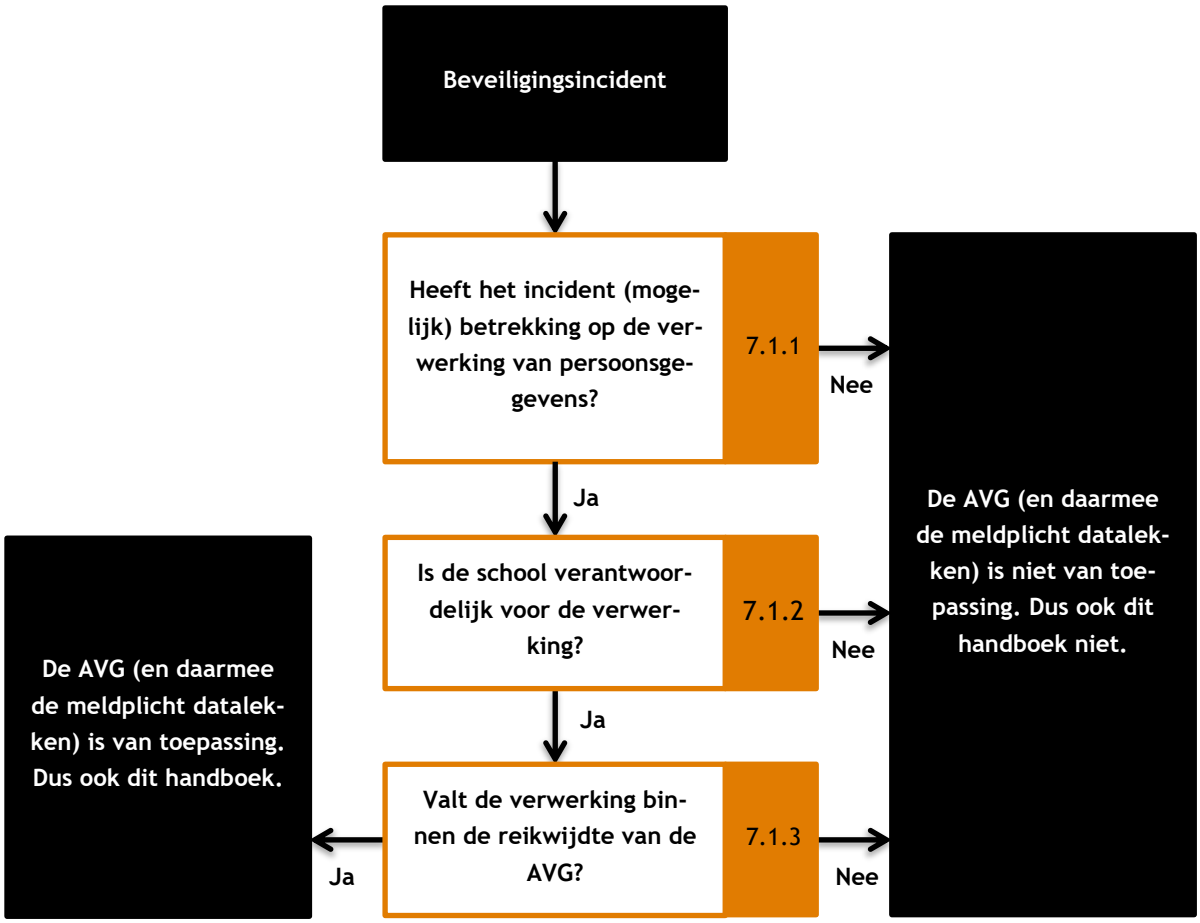
Bij het verzamelen van de benodigde informatie hebben de voorzitter van het bestuur en de FG, althans door hun aangewezen derden - toegang tot alle plekken en ruimtes binnen de school, zijn zij gerechtigd tot inzage in alle informatie, bestanden en/of data die hen geraden voorkomt en kunnen zij met iedereen spreken. Verzoeken tot het verschaffen van informatie die in dit kader (intern) worden gedaan en gegevens die op basis daarvan worden verstrekt, worden schriftelijk gedocumenteerd en liggen ter inzage voor alle leden van het IRT.

7. Is er sprake van een datalek?

Op basis van de verkregen informatie wordt zo snel als mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek. In dit verband dienen feitelijk twee beoordelingen plaats te vinden.

7.1. Eerste beoordeling: is de AVG van toepassing?

De beoordeling of de AVG van toepassing is, vindt plaats op basis van onderstaand schema.



7.1.1. Ziet de melding (mogelijk) op verwerking van persoonsgegevens?

Als er geen sprake is van verwerking van persoonsgegevens, dan zijn de AVG en dit handboek niet van toepassing.

Voorbeeld 1
Indien de school per ongeluk een e-mail verstuurt aan verkeerde personen en in die e-mail enkel melding wordt gemaakt van een toneelstuk dat binnenkort zal worden opgevoerd op school, dan is er geen sprake van verwerking van persoonsgegevens.

Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene') (artikel 4 lid 1 AVG). Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd.

Er bestaat een onderscheid tussen direct en indirect identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam, eventueel in combinatie met het adres en de geboortedatum. Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon (bijvoorbeeld: postcode/huisnummer, e-mailadres, kenteken of een leerlingnummer).

Een gegeven is geen persoonsgegeven, indien doeltreffende technische en organisatorische maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten (anonimisering).

Voorbeeld 2
Er is geen sprake van verwerking van persoonsgegevens indien een Medewerker een USB-stick verliest met daarop enkel een overzicht van de (gemiddelde) resultaten van een toetsperiode (voor statistieke doeleinden bijvoorbeeld) zonder dat deze resultaten zijn gekoppeld aan een enig ander (direct of indirect) gegeven van de leerling, dan wel leerlingnummer.

Het toepassen van cryptografische bewerkingen zoals encryptie[1] of hashing[2] op identificerende gegevens leidt tot pseudonimisering (het vervangen van een identificerend gegeven door een ander identificerend gegeven) maar niet tot anonimisering. De school is, ook na de encryptie of hashing, nog steeds in staat om de leerling te identificeren (door bestanden met elkaar te koppelen). Er is dus dan nog steeds sprake van persoonsgegevens. Wel is pseudonimisering een waardevolle beveiligingsmaatregel die bij een datalek de kans op daadwerkelijk misbruik van de gelekte persoonsgegevens aanzienlijk kan verlagen.

Het verwijderen van de direct identificerende gegevens biedt verder niet altijd voldoende garantie dat er geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit een andere bron, kan immers desondanks, soms zonder bijzondere inspanning, identificatie tot stand worden gebracht.

Voorbeeld 3
Indien een Medewerker in de trein een geordende dossiermap laat liggen met daarin de salarisgegevens van de Medewerkers, welke salarisgegevens zijn gekoppeld aan de postcode en huisnummer, is er sprake van verwerking van persoonsgegevens. Zonder bijzondere inspanningen kan via het (digitale) telefoonboek de identiteit van die Medewerkers worden achterhaald.

Verder moet bij anonimisering rekening worden gehouden met de stand van de techniek. Wat bij een bepaalde stand van de techniek als anoniem kan worden beschouwd, aangezien het gegeven niet redelijkerwijs tot een persoon te herleiden is, kan door technische ontwikkelingen alsnog een persoonsgegeven worden als gevolg van de toegenomen mogelijkheden tot herleiding.

[1] Zie hoofdstuk 11.1
[2] Zie hoofdstuk 11.1

‘Verwerking van persoonsgegevens’ betreft elke bewerking of elk geheel van bewerkingen, al dan niet uitgevoerd via geautomatiseerde procedés, met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, structureren, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen, verliezen of vernietigen van gegevens (artikel 4 lid 2 AVG).

7.1.2. Ziet de melding op verwerking van persoonsgegevens waarvoor de school verantwoordelijk is?

De meldplicht datalekken geeft verplichtingen voor de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens. Dit handboek vindt dan ook alleen toepassing indien de school als verwerkingsverantwoordelijke is aan te merken voor de verwerking van de persoonsgegevens (met andere woorden als verwerkingsverantwoordelijke voor het gemelde beveiligingsincident).

De verwerkingsverantwoordelijke is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 lid 7 AVG). Het gaat hierbij om de vraag wie uiteindelijk bepaalt welke verwerking er plaatsvindt van welke persoonsgegevens en voor welk doel. Ook is van belang wie er beslist over de middelen voor die verwerking: de vraag op welke manier de gegevensverwerking zal plaatsvinden. Deze bevoegdheden kunnen soms in verschillende handen liggen. In dat geval is er sprake van gezamenlijke verantwoordelijkheid.

De school is in ieder geval als verwerkingsverantwoordelijke aan te merken als het de verwerking van persoonsgegevens betreft aangaande:

- de (ouder(s) en/of verzorger(s)) van de leerlingen van de school; en
- de Medewerkers, en de school ten aanzien van die persoonsgegevens heeft bepaald welke verwerking plaatsvindt en voor welk doel.

Voorbeeld 4
De school is geen verwerkingsverantwoordelijke in het geval een Medewerker een USB-stick zou verliezen met daarop enkel persoonsgegevens van de leden van een sportvereniging (ook al zouden daar leerlingen bij zitten) waarvan de Medewerker bestuurslid is.

Voorbeeld 5
De school is wel verwerkingsverantwoordelijke in het geval een Medewerker een USB-stick zou verliezen met daarop alle voornamen en geboortedatum van de leerlingen op school die de Medewerker hobbymatig bijhoudt om te zien hoe voornamen door de tijd heen veranderen.

7.1.3. Valt de verwerking binnen de reikwijdte van de AVG?

De meldplicht datalekken uit de AVG (en daarmee dit handboek) is uitsluitend van toepassing op verwerkingen waarop de AVG van toepassing is verklaard.

Voor de vraag of de AVG van toepassing is op een verwerking van persoonsgegevens, zijn voor de school feitelijk twee elementen van belang:

- de aard en de doelstelling van de verwerking (artikel 2 AVG)
  Bepaalde verwerkingen vallen door hun aard of hun doelstelling buiten de reikwijdte van de AVG en op deze verwerkingen is de meldplicht datalekken niet van toepassing;
- territoriale reikwijdte: waar vinden de activiteiten plaats waarvoor de persoonsgegevens worden verwerkt, en waar bevinden zich de al dan niet geautomatiseerde middelen die bij de verwerking worden gebruikt (artikel 3 AVG)

Mogelijk is de privacywetgeving van een ander land van toepassing op de verwerking. Ook in deze situaties is de meldplicht datalekken uit de AVG niet van toepassing.

Aard en doelstelling

Voor de school kunnen feitelijk zich maar drie situaties voordoen dat de AVG geen toepassing vindt (en daarmee ook dit handboek niet):

- het betreft persoonsgegevens die door de school niet (geheel of gedeeltelijk) geautomatiseerd zijn verwerkt en die ook niet in een fysiek bestand zijn opgenomen of bedoeld zijn om in een fysiek bestand te worden opgenomen;

> Voorbeeld 6
> *Op school wordt een doos bij het grofvuil gezet met allerhande ongeordende oude brieven en documenten met daarin ook documenten met daarin persoonsgegevens van leerlingen en Medewerkers. Deze fysieke documenten kunnen niet als een bestand worden aangemerkt.*

- het betreft persoonsgegevens die worden verwerkt ten behoeve van activiteiten met uitsluitend persoonlijke doeleinden;

> Voorbeeld 7
> *Een leraar houdt een eigen lijstje bij met de namen van de leerlingen en hun gemiddelde cijfers. Dit lijstje heeft het karakter van persoonlijke aantekeningen, dienend als geheugensteun bij het lesgeven. Dit soort aantekeningen zijn uitgezonderd van de werking van de AVG. Zodra echter beoogd is dit lijstje te worden gebruikt door meerdere personen (bijvoorbeeld: vervangende leraar) is de AVG wel van toepassing.*

- het betreft de verwerking van persoonsgegevens door de school voor uitsluitend journalistieke, artistieke of literaire doeleinden.

> Voorbeeld 8
> *De school verwerkt de vingerafdrukken van een aantal leerlingen met het uitsluitende doel deze te gaan gebruiken voor een kunstwerk dat in de school zal komen te hangen. In dit geval is op deze verwerking de AVG niet van toepassing (en dus ook dit handboek niet).*

7.2. Tweede beoordeling: is er een datalek?

Beveiligingsincident: een inbreuk op de beveiliging die *niet* leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

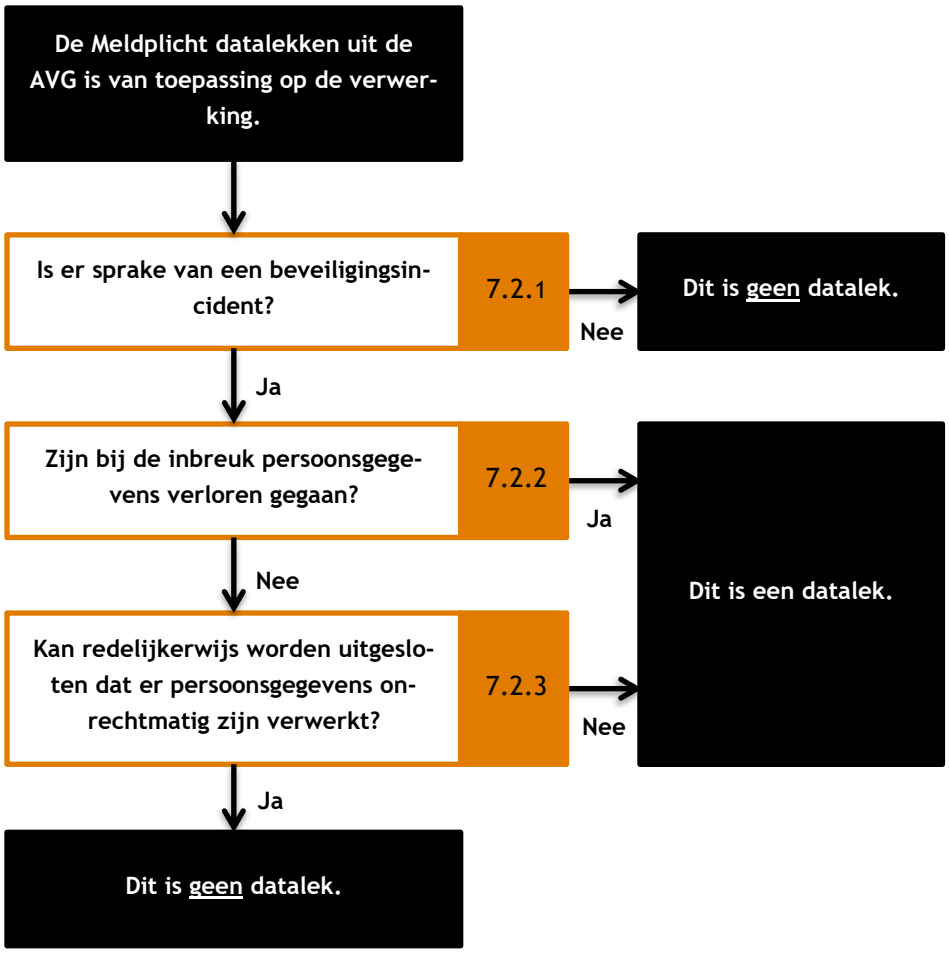
Datalek: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verwerking van persoonsgegevens.

In afwijking van hetgeen bepaald is onder hoofdstuk 5 aangaande de besluitvorming zijn de voorzitter van het IRT en de FG gerechtigd gezamenlijk een oordeel te vellen of een melding is aan te merken als een beveiligingsincident of een datalek indien die beoordeling eenvoudig is te maken. Staken in dit kader de stemmen, dan is de stem van de voorzitter van het IRT doorslaggevend. Indien een beoordeling niet eenvoudig lijkt te maken zal het oordeel na overleg met het volledige IRT worden geveld.

De beoordeling of er sprake is van een beveiligingsincident of datalek vindt plaats op basis van onderstaand schema. Het uiteindelijk oordeel wordt altijd schriftelijk onderbouwd, opgeslagen en bewaard.

Ieder datalek moet worden gedocumenteerd, inclusief de feiten omtrent de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. De AP kan deze documentatie opvragen om te controleren of datalekken daadwerkelijk worden gemonitord en opgevolgd.

Om te beschikken over documentatie van ieder datalek dient de school tevens doorlopend goede afspraken te maken met de verwerkers, zodat de school ook over documentatie beschikt van beveiligingsincidenten die hebben plaatsgevonden bij verwerkers. Deze afspraken worden vastgelegd in de verwerkersovereenkomsten die tussen de school en de verwerker worden gesloten. De FG dient zich er steeds van te vergewissen dat bij totstandkoming van een verwerkersovereenkomst afspraken zijn gemaakt over de invulling van de documentatieplicht conform artikel 33 lid 5 AVG, die ook voor de verwerkers geldt


De Meldplicht datalekken uit de AVG is van toepassing op de verwerking.
Is er sprake van een beveiligingsincident?
7.2.1
Nee
Dit is geen datalek.
Ja
Zijn bij de inbreuk persoonsgegevens verloren gegaan?
7.2.2
Ja
Dit is een datalek.
Nee
Kan redelijkerwijs worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt?
7.2.3
Nee
Ja
Dit is geen datalek.

7.2.1. Is er sprake van een beveiligingsincident?

De school is als verwerkingsverantwoordelijke verplicht om op grond van artikel 32 AVG passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Een beveiligingsincident moet ruim worden uitgelegd. Het betreft alle beveiligingsincidenten waardoor de bescherming van de persoonsgegevens op enig moment (tijdelijk) is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan mogelijk:

- verlies; of
- onrechtmatige verwerking (inzien, onbevoegde kennisname, wijzigen, verwijderen, doorsturen, etc.).

Het is niet van belang of de school in dit kader al dan niet passende technische of organisatorische maatregelen heeft getroffen (bijv. encryptie). Dat is bij de vaststelling of er sprake is van een inbreuk op de beveiliging niet van belang.

In ieder geval is sprake van een beveiligingsincident waarbij een inbreuk op de beveiliging van de persoonsgegevens plaatsvindt, bij:

- een kwijtgeraakte USB-stick door een Medewerker (al dan niet encrypted);
- een gestolen laptop/mobiele telefoon van een Medewerker (al dan niet encrypted);
- een inbraak door een hacker op het netwerk van de school of van een verwerker;
- een malware-besmetting op het Netwerk van de school of van een verwerker;
- een calamiteit zoals een brand in het datacentrum van de school of van een verwerker;
- het bewust of onbewust prijsgeven door een Medewerker van zijn gebruiksnaam en wachtwoord aan een derde, althans een daartoe onbevoegde derde;
- een toegangsdeur naar een ruimte met personeels- en/of leerlingdossiers die (tijdelijk) niet deugdelijk afgesloten is geweest en daarmee toegankelijk is geweest voor daartoe onbevoegde derden.

7.2.2. Zijn bij het incident persoonsgegevens vernietigd/verloren gegaan?

Verlies van persoonsgegevens houdt in dat de school (of de verwerkers) de persoonsgegevens niet meer hebben; ze zijn weg en niet meer reproduceerbaar. Als gevolg van het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan en de school beschikt niet meer over een complete en actuele reservekopie van de persoonsgegevens. Als er sprake is van vernietiging of verloren gaan van persoonsgegevens is er sprake van een datalek. De aard van het beveiligingsincident is daarbij niet van belang voor het antwoord op de vraag of er sprake is van een datalek. Indien persoonsgegevens verloren gaan als gevolg van bijvoorbeeld brand dan is er sprake van een datalek.

Van vernietiging en het verloren gaan van de persoonsgegevens is in ieder geval sprake indien:

- persoonsgegevens definitief worden verwijderd van de systemen van school en verwerkers als gevolg van een fout van een Medewerker;
- persoonsgegevens vernietigd worden als gevolg van brand in het datacenter van school of verwerker;
- de smartphone of laptop van een Medewerker wordt gestolen en er geen actuele reservekopie beschikbaar is van de gegevens op de smartphone of laptop;
- een Medewerker zijn smartphone of laptop in het water laat vallen en persoonsgegevens op de smartphone of laptop niet meer beschikbaar zijn of kunnen worden gemaakt.

Bovengenoemde omstandigheden kwalificeren echter niet direct als datalek indien van de vernietigde en/of verloren gegane gegevens een actuele reservekopie beschikbaar is voor de school en/of verwerkers.

7.2.3. Valt uit te sluiten dat persoonsgegevens onrechtmatig zijn verwerkt?

Van onrechtmatige verwerking van persoonsgegevens kan in meerdere situaties sprake zijn. Het kan gaan om:

- onbevoegde aantasting van persoonsgegevens;
- onbevoegde wijziging van persoonsgegevens;
- onbevoegde kennisneming van persoonsgegevens;
- onbevoegde doorzending/verstrekking van persoonsgegevens.

Indien de school redelijkerwijs *niet* kan uitsluiten dat de inbreuk op de beveiliging heeft geleid tot een onrechtmatige verwerking, dan moet de school de inbreuk beschouwen als een datalek. Slechts indien uitgesloten kan worden dat de inbreuk op de beveiliging niet heeft geleid tot een onrechtmatige verwerking (en de gegevens zijn niet verloren gegaan), kan de breuk als louter een beveiligingsincident worden aangemerkt.

In geval van een malware-besmetting op het systeem van de school of verwerker moet de school er in ieder geval van uitgaan dat er sprake is van een datalek. Immers, in dat geval kan niet redelijkerwijs worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt.

Voorbeeld 9

Een Medewerker laat zijn laptop onbeheerd achter (in de klas) met daarbij een memo-sticker met daarop zijn inlognaam en wachtwoord. Op de laptop staan alle studieresultaten en leerlingdossiers van een groot aantal leerlingen. Na ontdekking van dit beveiligingsincident past de school/Medewerker direct het wachtwoord van dit account aan. Daarna onderzoekt de school of een derde daadwerkelijk toegang heeft gezocht tot de persoonsgegevens op de laptop. Bij dit onderzoek blijkt uit de logbestanden, waarin per inlognaam is vastgesteld welke acties er op welk tijdstip zijn uitgevoerd met welke gegevens. Uit de loggegevens volgt dat kan worden uitgesloten dat er met de inlognaam toegang is gekregen tot de persoonsgegevens op de laptop gedurende de periode dat het beveiligingsincident zich voordeed. In dat geval is er enkel sprake van een beveiligingsincident en niet van een datalek.

Voorbeeld 10

Een verwerker - ingeschakeld door de school ten behoeve van de salarisadministratie - zendt per ongeluk een bestand met loonstroken van een aantal Medewerkers naar een verkeerd e-mailadres. Zelfs indien de verwerker de ontvanger verzoekt om het bestand (ongelezen) te verwijderen/vernietigen kan de school niet redelijkerwijs uitsluiten dat deze inbreuk heeft geleid tot de situatie dat een onbevoegde kennis heeft genomen van de persoonsgegevens. In dit geval is er sprake van een datalek.

Voorbeeld 11

De toegangsdeur tot een afgesloten ruimte in het schoolgebouw met daarin fysieke leerlingdossiers (die gestructureerd en op alfabet staan opgeslagen) heeft gedurende een bepaalde periode niet op slot gezeten, dan wel heeft zelfs tijdelijk opengestaan. Gedurende deze periode hebben onbevoegden, waaronder leerlingen, de mogelijkheid gehad de leerlingdossiers in te zien. Of dat ook daadwerkelijk het geval is, is niet duidelijk. De school kan echter niet redelijkerwijs uitsluiten dat deze inbreuk heeft geleid tot de situatie dat een onbevoegde kennis heeft genomen van de persoonsgegevens van de leerlingen. In dit geval is er sprake van een datalek.
Als op basis van camerabeelden die op de gang van het schoolgebouw hangen echter kan worden uitgesloten dat gedurende de periode dat het beveiligingsincident zich voordeed er onbevoegden zijn geweest die zich toegang tot de ruimte hebben verschaft, dan kan worden uitgesloten dat er deze inbreuk heeft geleid tot de situatie dat een onbevoegde kennis heeft genomen van de persoonsgegevens van de leerlingen. In dat geval is er geen sprake van een datalek.

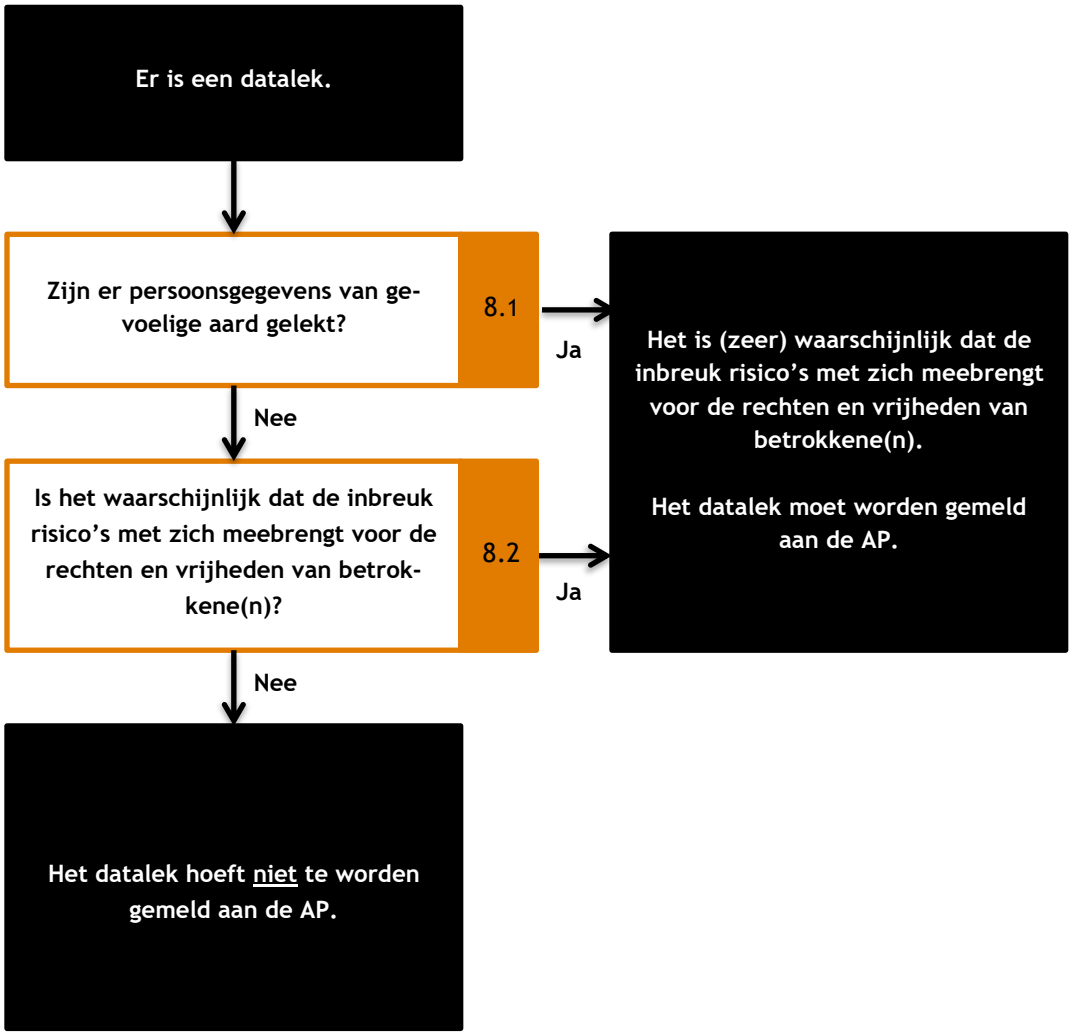
Voorbeeld 12

De adequaat versleutelde laptop van een Medewerker is uit de auto gestolen. Studieresultaten van 1000 leerlingen waren betrokken. Het wachtwoord van de laptop is niet gecompromitteerd en er was een back-up voorhanden, zodat er geen sprake is van een datalek, maar beveiligingsincident.

8. Melding datalek aan Autoriteit persoonsgegevens

Indien wordt geoordeeld door de voorzitter van het IRT en de FG, dan wel het IRT, dat er sprake is van een datalek, dient vervolgens door het IRT bepaald te worden of het datalek aan de AP dient te worden gemeld. De meldingsplicht aan de AP bestaat voor de school alleen indien het datalek leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens.

De beoordeling of melding moet worden gedaan aan de AP en dat het derhalve waarschijnlijk is dat het datalek risico's voor de rechten en vrijheden van natuurlijke personen (betrokkenen) met zich mee heeft gebracht vindt plaats op basis van onderstaand schema.



8.1. Zijn er persoonsgegevens van gevoelige aard gelekt?

Allereerst moet worden gekeken naar de aard van de gegevens die als gevolg van het datalek gelekt zijn. Is er bijvoorbeeld sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderszins van gevoelige aard zijn?

Bij een aantal categorieën van persoonsgegevens, in dit kader aangeduid als persoonsgegevens van gevoelige aard, kunnen verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot persoonsgegevens van gevoelige aard moeten in ieder geval worden gerekend:

- *Bijzondere persoonsgegevens zoals bedoeld in artikelen 9 en 10 AVG*
  Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras of etnische afkomst, politieke opvattingen, gezondheid, seksuele leven (gedrag en gerichtheid), lidmaatschap van een vakbond, genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een persoon, strafrechtelijke persoonsgegevens en persoonsgegevens over veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.
- *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 prestaties op school, (ontwikkeling van) leergedrag, werk- of relatieproblemen of gokverslaving.[3]
- *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).
- *Gegevens die onder een beroepsgeheim vallen*
  Het gaat hier bijvoorbeeld om het medisch beroepsgeheim.

Indien derhalve ten aanzien van één of meerdere (ouder(s) en/of verzorger(s) van) leerlingen en/of Medewerkers één of meerdere gegevens van gevoelige aard zijn gelekt, dan dient hoe dan ook gemeld te worden aan de AP.

[3] De AP heeft geoordeeld dat het bij verwerking van persoonsgegevens in het kader van vastlegging van leergedrag kan gaan om zeer gedetailleerde gegevens over de individuele onderwijsvorderingen van een leerling, waaraan allerhande conclusies worden verbonden die mogelijk gevolgen hebben voor het latere maatschappelijke leven van de leerlingen.

Voorbeeld 13
Als gevolg van een brand in het datacenter van de verwerker gaan alle studieresultaten van de leerlingen verloren. Er is geen back-up beschikbaar. Er is sprake van het verloren gaan van persoonsgegevens van gevoelige aard.

Voorbeeld 14
Een hacker weet op de website van de school door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een aantal Medewerkers. Normaal gesproken gaat het hier niet om persoonsgegevens van gevoelige aard. Dit wordt anders als deze Medewerkers onderdeel uitmaken van een club binnen de school die zich richt op bijvoorbeeld een specifieke levensovertuiging, politieke voorkeur of seksuele geaardheid.

8.2. Is het waarschijnlijk dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n)?

De aard en omvang van het datalek dient in ogenschouw te worden genomen bij de beantwoording van de vraag of het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

Een datalek bij grote instellingen zoals de Belastingdienst, de Sociale Verzekeringsbank (SVB), een bank of een verzekeraar kan leiden tot financieel nadeel voor de betrokkene of tot de compromittering van gegevens die beschermd worden door een geheimhoudingsplicht. Datalekken in de omvangrijke verwerkingen van persoonsgegevens waarover de overheid beschikt kunnen ook zeer grote gevolgen hebben voor de betrokkenen.

Verder is het volgende relevant:

- De omvang van de hierboven beschreven verwerkingen betekent dat het bij een datalek kan gaan om veel persoonsgegevens per persoon, en om gegevens van grote groepen betrokkenen. Deze beide factoren maken een grote hoeveelheid gelekte data aantrekkelijk voor misbruik in het criminele circuit. De kans dat de gelekte data dan wordt doorverkocht wordt daardoor ook groter, met als gevolg dat de betrokkenen langer last houden van het datalek.
- Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als de school de gegevens gebruikt om het studieadvies van een leerling te bepalen zijn de gevolgen van verlies en onbevoegde wijziging van die gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor het vaststellen van een tussentijdsrapport.
- Bij omvangrijke verwerkingen van de overheid is vaak sprake van persoonsgegevens die binnen ketens worden gedeeld. Dit betekent dat de gevolgen van verlies en onbevoegde wijziging van persoonsgegevens door de hele keten heen kunnen optreden. Voor de betrokkenen wordt het hierdoor moeilijker om de mogelijke gevolgen van een datalek te overzien en om zich daar waar mogelijk aan te onttrekken.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet de school ervan uitgaan dat het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

Daarnaast kan voor betrokkenen in kwetsbare groepen verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen. De gevolgen van onbevoegde toegang tot NAW-gegevens zullen bijvoorbeeld voor de meeste betrokkenen beperkt zijn, maar dit ligt anders voor betrokkenen die te maken hebben met bijvoorbeeld stalking of die in een blijf-van-mijn-lijfhuis verblijven. Voor bepaalde categorieën van betrokkenen, zoals kinderen en mensen met een verstandelijke handicap, kan het moeilijker zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk eerder ingaan op pogingen tot phishing of oplichting.

Indien duidelijk is dat gegevens worden verwerkt van betrokkenen in kwetsbare groepen, bijvoorbeeld omdat de verwerking zich specifiek richt op betrokkenen die hiertoe behoren, dan moet ervan worden uitgegaan dat het waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van betrokkene(n).

Dit brengt met zich dat steeds indien er door het datalek persoonsgegevens van leerlingen zijn betrokken (gevoelig van aard of niet) de school ervan uit moet gaan dat het mogelijk waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van deze leerlingen.

Voorbeeld 15
Een hacker weet op de website van de school door middel van SQL-injectie, een veel voorkomende vorm van hacking, een bestand te bemachtigen met daarin de namen en e-mailadressen van een twintigtal Medewerkers die een nieuwsbrief ontvangen. De nieuwsbrief richt zich op personen die een cursus volgen om vertrouwd te raken met het gebruik van computers en het internet. De aard van de doelgroep leidt hier tot extra risico's voor de betrokkenen. Gezien de onervarenheid van de betrokkenen met digitale communicatie bestaat er een aanzienlijk risico dat zij in zullen gaan op pogingen tot phishing of oplichting.

Bij een datalek als gevolg van een hack, is van belang wat de aard van de gelekte persoonsgegevens is, en wat de risico’s van misbruik van deze persoonsgegevens voor de betrokkene zijn. De intentie bij een hack is veelal kwaadwillend. Bij een hack zal melding dan ook al snel gepast zijn gelet op de risico’s van misbruik van persoonsgegevens. Bij een hack ligt ook aangifte bij de politie in de rede in verband met opsporing van de daders.

Indien moet worden vastgesteld dat er geen sprake is van een datalek dat aan de AP dient te worden gemeld, is het ter vrije afweging van het IRT om desondanks de betrokkenen te informeren over het datalek en welke gegevens van hen daar zijn gelekt.

9. Onverwijlde melding aan Autoriteit persoonsgegevens

Indien melding van het datalek aan de AP zal moeten plaatsvinden op grond van de gevoelige aard van de gegevens, dan wel de aard en de omvang daarvan, althans het IRT na zorgvuldige afweging zekerheidshalve tot melding over wenst te gaan aan de AP, dan dient het IRT deze melding *onverwijld* te doen aan de AP.

Het 'onverwijld melden' houdt in dat de school, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. Het betreft hier de tijd benodigd met de stappen als genoemd onder hoofdstukken 6 tot en met 8 van dit handboek. Wat als 'onverwijld' moet worden aangemerkt hangt verder af van de omstandigheden van het geval. Bij een klein en overzichtelijk datalek mag verwacht worden dat sneller na de ontdekking wordt gemeld dan in geval van een omvangrijke hack waarbij langdurig grote hoeveelheden data vanuit verschillende bestanden en servers is gekopieerd.

Onderstaand worden de uitgangspunten opgesomd die de AP met het oog op zijn toezichthoudende en handhavende bevoegdheden hanteert:

- de termijn voor het melden van het datalek begint te lopen op het moment dat de school (als verwerkingsverantwoordelijke), op de hoogte raakt van een beveiligingsincident dat mogelijk onder de meldplicht datalekken valt;
- zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, moet (door de FG) een melding bij de AP worden gedaan, tenzij op dat moment inmiddels al uit het onderzoek van het IRT is gebleken dat het incident niet onder de meldplicht datalekken valt;
- indien het incident later dan 72 uur na ontdekking aan de AP wordt gemeld, dan dient desgevraagd te kunnen worden gemotiveerd aan de AP waarom de melding later heeft plaatsgevonden;
- mogelijk is er 72 uur na de ontdekking van het incident nog niet volledig zicht op wat er gebeurd is en om welke persoonsgegevens het gaat. In dat geval wordt de melding gedaan op basis van de gegevens waarover op dat moment wordt beschikt. Eventueel kan de melding naderhand nog worden aangevuld of ingetrokken.

Om een datalek tijdig te kunnen melden dient de school steeds doorlopend goede afspraken te maken met de verwerkers, zodat deze de school tijdig en adequaat informeren over alle relevante beveiligingsincidenten en de school ook de juiste en volledige informatie verschaffen om tijdig de beoordelingen te kunnen maken in het kader van dit handboek. Deze afspraken worden vastgelegd in de verwerkersovereenkomsten die tussen de school en de verwerker worden gesloten. De FG dient zich er steeds van te vergewissen dat bij totstandkoming van een verwerkersovereenkomst is gewaarborgd dat de verwerker verplicht is tijdig een beveiligingsincident te melden en school daarbij te voorzien van de relevante en juiste informatie.

De voorzitter van het IRT is eindverantwoordelijk voor een onverwijlde en tijdige melding aan de AP.

10. Wijze van melding aan Autoriteit persoonsgegevens

Het datalek zal door het IRT worden gemeld bij het AP door middel van het online webformulier zoals dat op de website van de AP (www.autoriteitpersoonsgegevens.nl) beschikbaar is. Een overzicht van de vragen die in dit webformulier zijn opgenomen zijn als bijlage 4 aan dit handboek gehecht.

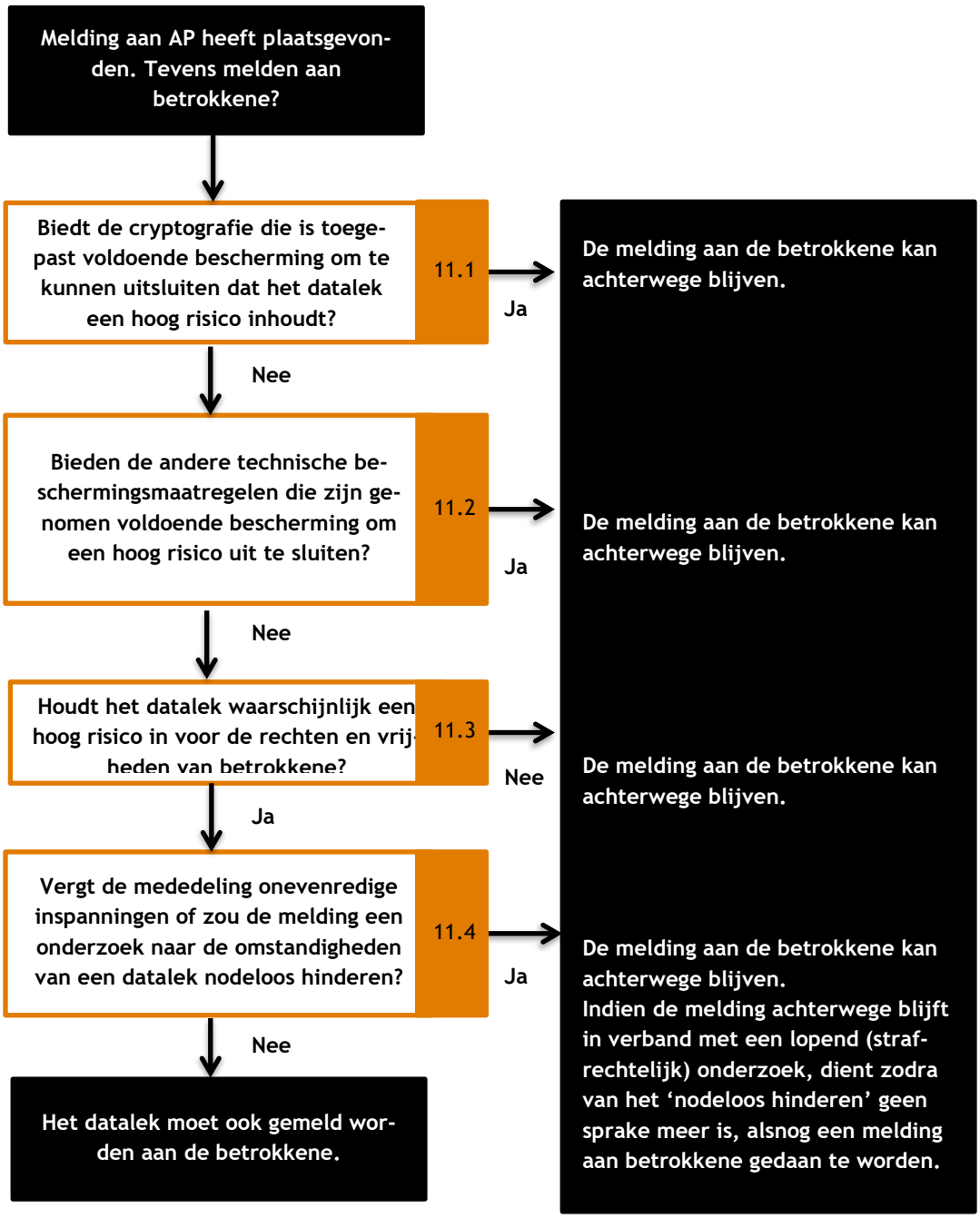
Indien onder omstandigheden – bijvoorbeeld als gevolg van een hack of brand – geen gebruik gemaakt kan worden van het webformulier, dan kan het IRT de gevraagde gegevens per fax (070 - 88 88 501) toezenden aan de AP. Het IRT zorgt daarbij dat kan worden aangetoond dat datum en tijdstip van de melding kan worden aangetoond.

De voorzitter van het IRT is eindverantwoordelijk voor de inhoud van de melding.

In geval een melding aanleiding geeft tot nadere actie door de AP, zal het IRT als contactpersoon functioneren.

11. Melden datalek aan betrokkene?

Na de melding aan de AP dient het IRT te beoordelen of tevens melding dient te worden gedaan bij de betrokkenen bij het datalek. Deze beoordeling maakt het IRT op basis van onderstaand schema.



11.1. Biedt de cryptografie die is toegepast voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?

Indien passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de persoonsgegevens, dan kan de school de melding aan de betrokkene achterwege laten (artikel 34 lid 3 a AVG).

Cryptografie komt vaak naar voren als het voornaamste voorbeeld van een technische beschermingsmaatregel. Dit onderdeel gaat in op het gebruik van cryptografie als technische beschermingsmaatregel om persoonsgegevens onbegrijpelijk of ontoegankelijk te maken voor onbevoegden. Andere technische beschermingsmaatregelen worden behandeld in hoofdstuk 11.2.

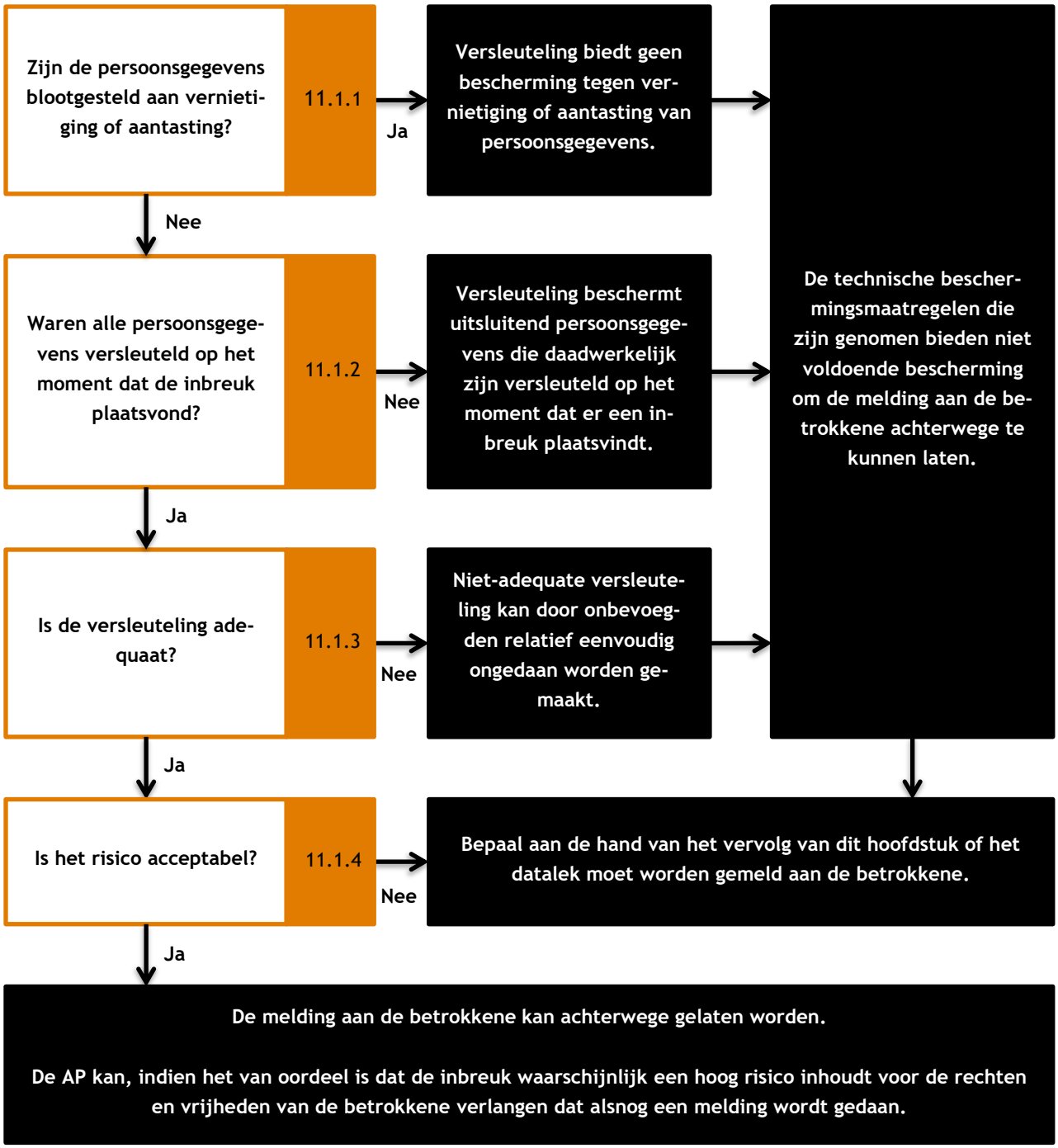
In dit kader zijn er twee cryptografische bewerkingen:

1) encryptie (versleuteling); en
2) hashing (het omzetten van gegevens in een unieke code).

Encryptie
Kenmerkend voor encryptie is dat deze bewerking omkeerbaar is: door gebruik van de juiste sleutel kan de oorspronkelijke informatie worden (terug)verkregen (decryptie). Encryptie wordt onder andere toegepast op draagbare hardware (laptops, smartphones) en op verwijderbare media (zoals onder andere USB-sticks) om de gegevens die daarop zijn opgeslagen te beveiligen.

Hashing
Kenmerkend voor hashing is dat het een bewerking betreft die van informatie, ongeacht de lengte, een unieke hashcode maakt die altijd even lang is (de lengte is afhankelijk van de gebruikte hashingmethode). Hashing wordt onder meer gebruikt bij de opslag en verwerking van wachtwoorden: op het moment dat de gebruiker een (nieuw) wachtwoord kiest, wordt de bijbehorende hashcode opgeslagen. Wanneer de gebruiker vervolgens inlogt, wordt de hashcode van het ingevoerde wachtwoord vergeleken met de opgeslagen hashcode en krijgt de gebruiker toegang tot het informatiesysteem als de codes overeenkomen.

Als door de cryptografische bewerkingen die zijn toegepast de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding aan de betrokkene achterwege worden gelaten. Dit is een strenge norm, die van geval tot geval moet worden toegepast op basis van de actuele stand van de techniek. Als er twijfel bestaat over de adequaatheid van de technische beschermingsmaatregelen die zijn getroffen, dan moet het datalek gemeld worden aan de betrokkene. In onderstaand schema zijn de beoordelingsgronden opgenomen om tot deze afweging te kunnen komen.



11.1.1. Zijn de persoonsgegevens blootgesteld aan vernietiging of aantasting?

Persoonsgegevens die adequaat zijn versleuteld kunnen bij een datalek nog steeds worden vernietigd, en ook aantasting of onbevoegde wijziging is nog steeds mogelijk (bijvoorbeeld door zogenoemde 'cryptoware', die de reeds versleutelde gegevens nogmaals versleutelt met een sleutel die de school dan uitsluitend tegen betaling in zijn bezit kan krijgen).

Een datalek waarbij adequaat versleutelde persoonsgegevens niet alleen zijn blootgesteld aan onbevoegde kennisname, maar ook aan verlies of aan andere vormen van onrechtmatige verwerking, kan

ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk aan de betrokkene worden gemeld.

Voorbeeld 16
De versleutelde laptop van een Medewerker is gestolen uit de kofferbak van zijn auto. Op de laptop staan de bankrekeningnummers van 200 betrokkenen. Door de diefstal zijn deze gegevens blootgesteld aan onbevoegde kennisname. De school komt tot de conclusie dat alle gegevens op de harde schijf adequaat versleuteld zijn (11.1.3), en dat het restrisico acceptabel is (11.1.4). In principe zou de school de melding aan de betrokkene dus achterwege kunnen laten.
Echter: de school beschikt niet over een back-up (reserve-kopie) van de bankrekeningnummers op de harde schijf. Dat betekent dat er in dit geval niet alleen sprake is van blootstelling aan onbevoegde kennisname, maar ook van het verlies van de getroffen persoonsgegevens. Aangezien de school de gegevens niet meer heeft, zal de school deze opnieuw bij de betrokkenen op moeten vragen. De vertraging die hierdoor ontstaat in de salarisbetalingen, kan tot financiële problemen leiden bij de Medewerkers. In dit geval ligt het, ondanks de genomen technische beschermingsmaatregelen, voor de hand om het datalek te melden aan de betrokkenen. De melding omvat in ieder geval het verzoek om de bankrekeningnummers opnieuw aan te verstrekken en een uitleg van de potentiële consequenties en negatieve gevolgen van de inbreuk.

11.1.2. Waren de persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?

Versleuteling beschermt uitsluitend persoonsgegevens die daadwerkelijk versleuteld zijn op het moment dat er een inbreuk plaatsvindt. Een datalek waarbij (ook) niet versleutelde persoonsgegevens zijn gelekt, kan ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene en moet daarom mogelijk worden gemeld.

Voorbeeld 17
Op de harde schijf van een laptop staat een bestand met persoonsgegevens. Het bestand zelf is niet versleuteld. De laptop wordt automatisch vergrendeld als deze enige tijd niet wordt gebruikt, en bij de automatische vergrendeling wordt de inhoud van de harde schijf versleuteld. De laptop is in handen gekomen van een aanvaller die met technische middelen gebruik van het toetsenbord simuleert, en daardoor voorkomt dat de automatische vergrendeling in werking treedt en de gegevens op de harde schijf worden versleuteld. Er is hier dus geen sprake van een adequate versleuteling en zal gemeld moeten worden aan betrokkenen.

Voorbeeld 18
Een Medewerker geeft aan een derde de gebruikersnaam en het wachtwoord dat toegang geeft tot bepaalde gegevens van alle Medewerkers van de school. Het gaat onder meer om namen, adressen, e-mailadressen, telefoonnummers, toegangs- en andere identificatiegegevens (gebruikersnamen, gehashte wachtwoorden en personeelsnummers) en versleutelde betaalgegevens (waaronder rekeningnummers). Om twee redenen moet de school dit datalek melden aan de betrokkene:
- *slechts een deel van de persoonsgegevens is versleuteld (de wachtwoorden en de betaalgegevens);*
- *de betaalgegevens zijn weliswaar versleuteld opgeslagen, maar als de derde met de verstrekte gegevens inlogt krijgt hij via de gebruikersinterface toegang tot de onversleutelde gegevens.*

11.1.3. Is de versleuteling adequaat?

Het is in eerste instantie aan het IRT om te beoordelen of de versleuteling sterk genoeg is, en op de juiste wijze wordt uitgevoerd.

Zowel encryptie als hashing zijn in principe te 'kraken', wat inhoudt dat onbevoegden toegang kunnen krijgen tot de oorspronkelijke gegevens.[4] Dit terrein ontwikkelt zich voortdurend en het is zeer goed mogelijk dat een cryptografische bewerking die in de huidige situatie veilig genoeg is dat over enige tijd niet meer is. Bij gebruik van cryptografische bewerkingen beoordeelt het IRT daarom periodiek of deze nog steeds voldoende bescherming bieden.

De Europese verordening 611/2013 geeft een nadere invulling aan ‘adequate versleuteling’. Volgens deze verordening mogen gegevens als onbegrijpelijk beschouwd worden als ze:

- op veilige wijze zijn versleuteld met een standaardalgoritme, de sleutel voor decryptie door geen enkele inbreuk gevaar heeft gelopen en de sleutel voor decryptie zodanig werd gegenereerd dat personen zonder geautoriseerde toegang de sleutel met de beschikbare technologische middelen niet kunnen vinden; of
- zijn vervangen door een met een cryptografisch versleutelde hashfunctie berekende hashwaarde, de sleutel die hiervoor werd gebruikt door geen enkele inbreuk gevaar heeft gelopen en deze voor datahashing gebruikte sleutel zodanig is gegenereerd dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Aandachtspunten bij de beoordeling zijn:

- Het algoritme zelf, of de wijze waarop deze wordt toegepast, kunnen kwetsbaarheden vertonen waardoor de encryptie of de hashing niet de bescherming biedt die daarvan verwacht mag worden.
- Encryptie is omkeerbaar. Een onbevoegde die over de juiste sleutel beschikt, of deze zonder al te veel moeite kan vinden, kan de gelekte gegevens ontsleutelen.
- Hashing is herhaalbaar. Als bij hashing geen ‘salt’ is toegepast, of als een onbevoegde over de gebruikte ‘salt’ beschikt of deze zonder al te veel moeite kan vinden, kan de gebruikte hashingmethode toegepast worden op een lijst met veelgebruikte waarden en daardoor bijvoorbeeld gestolen wachtwoorden worden achterhaald.[5]

Behalve het gebruikte algoritme zelf, is voor adequate versleuteling ook van belang dat dit op de juiste wijze wordt toegepast. Een beoordeling door een deskundige kan hier uitsluitsel over bieden. Bij voorkeur vindt deze beoordeling plaats voordat er een datalek heeft plaatsgevonden zodat, op het moment dat zich een datalek voordoet, gemakkelijk bepaald kan worden of de encryptie of de hashing die is toegepast voldoende bescherming biedt.

---

[4] Kraken wordt tegengegaan door het gebruik van (combinaties van) moderne cryptografische technieken en door toepassing van zogenoemde salts (extra informatie die bij hashing wordt toegevoegd aan het oorspronkelijke gegeven om het kraken van de hashcode te bemoeilijken).

[5] Algemene informatie over algoritmen en toepassingen daarvan zijn te vinden in de publicaties van het European Union Agency for Network and Information Security (ENISA) en het Nationaal Cyber Security Centrum (NCSC). Bij het opstellen van deze beleidsregels was de meest recente publicatie van ENISA op dit gebied het 'Algoritms, key sizes and parameters report – 2014' dat werd gepubliceerd in november 2014.

Als laatste is van belang dat de gebruikte sleutel c.q. ‘salt’ niet is gelekt. Dit zal van geval tot geval moeten worden vastgesteld.

11.1.4. Is het restrisico acceptabel?

Door de beantwoording van de voorgaande vragen heeft het IRT, als het goed is, een beeld gekregen van de mate waarin de technische beschermingsmaatregelen die zijn genomen de gelekte persoonsgegevens beschermen tegen daadwerkelijke onbevoegde kennisname. Per concreet geval zal moeten worden beoordeeld of de geboden bescherming voldoende is om de kennisgeving aan de betrokkene achterwege te kunnen laten omdat het restrisico beperkt is.

Behalve met wat hierboven is aangegeven, moet het IRT daarbij ook meewegen welke gevolgen het voor de persoonlijke levenssfeer van de betrokkene kan hebben als een aanvaller/onbevoegde er nu of in de toekomst alsnog in slaagt om kennis te nemen van de betrokken persoonsgegevens.

Voorbeeld 19
Een laptop, met op de harde schijf een bestand met persoonsgegevens, is gestolen bij een verwerker. De school als verwerkingsverantwoordelijke onderzoekt het incident, en komt tot de conclusie dat zij op grond van het zesde lid van artikel 34a Wbp af mag zien van de melding aan de betrokkene. Haar overwegingen daarbij zijn:

- *bij de versleuteling van het bestand is gebruik gemaakt van combinatie van algoritme en sleutellengte die door het ENISA in een actuele (niet door een recentere publicatie achterhaalde) handreiking wordt beoordeeld als 'toekomst-vast voor de komende 10 tot 50 jaar;*
- *met betrekking tot het gebruikte algoritme en de implementatie daarvan zijn geen kwetsbaarheden bekend;*
- *de implementatie is met goed gevolg beoordeeld door een deskundige;*
- *het bestand zelf was versleuteld, dus de versleuteling was niet afhankelijk van automatische vergrendeling die in het specifieke geval mogelijk niet heeft gewerkt;*
- *de sleutel is niet gelekt;*
- *gezien de aard van het datalek, de verwerking en de gelekte gegevens is het restrisico acceptabel.*

11.2. Bieden de andere technische beschermingsmaatregelen die zijn genomen voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?

Remote wipe
Naast encryptie wordt er aangenomen dat er nog een technische beschermingsmaatregel is waarmee persoonsgegevens kunnen worden beschermd tegen onbevoegde kennisname. Het betreft: het op afstand wissen van de gegevens die op hardware staan (*remote wiping*).

Door de gegevens op afstand te wissen zijn deze niet langer beschikbaar voor onbevoegden, aangezien na een geslaagde ‘*remote wipe*’ een onbevoegde nog wel de beschikking heeft over de hardware waarop de gegevens stonden, maar niet meer over de (persoons)gegevens zelf. Een ‘*remote wipe*’ heeft echter uitsluitend kans van slagen als er aan een aantal randvoorwaarden wordt voldaan. Deze luiden als volgt:

- de '*remote wipe*' is tijdig in gang gezet, zodat een onbevoegde nog geen kans heeft gehad om kennis te nemen van de persoonsgegevens;
- de hardware waar het om gaat moet nog intact zijn en werken, zodat het in staat is om de *remote wipe* uit te voeren en de gegevens te wissen;
- de toepassing die voor het wissen van de gegevens wordt gebruikt moet correct werken, zodat alle gegevens waar het om gaat daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waaruit de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Als gebruik gemaakt wordt van '*remote wiping*', dan zal op basis van de specifieke omstandigheden van het geval vastgesteld moeten worden of er wordt voldaan aan de strenge norm van artikel 34 lid 3 a AVG. De voorgaande paragrafen kunnen daarbij gebruikt worden als leidraad bij die vaststelling. Op voorhand kan wel worden vastgesteld dat de randvoorwaarden zoals gesteld voor een toereikende 'remote wipe' niet altijd met zekerheid zullen kunnen worden vastgesteld door het IRT.

Pseudonimisering
Daarnaast kan er sprake zijn van pseudonimisering. Pseudonimisering wil zeggen dat technische maatregelen zijn genomen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene. Geslaagde pseudonimisering maakt de persoonsgegevens waarover het gaat tot op zekere hoogte onbegrijpelijk voor onbevoegden en de kans dat een datalek daarmee ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene wordt verlaagd. Onvolkomenheden in de wijze waarop de persoonsgegevens zijn gepseudonimiseerd kunnen er echter toe leiden dat onbevoegden de oorspronkelijke identiteit van de betrokkenen alsnog kunnen achterhalen, eventueel met gebruikmaking van andere gegevens die ze reeds in hun bezit hadden of alsnog in hun bezit krijgen.

Ook als de gelekte persoonsgegevens gepseudonimiseerd zijn zal op basis van de specifieke omstandigheden van het geval moeten worden vastgesteld of er aan de norm van artikel 34 lid 3a AVG wordt voldaan.

Net als bij een '*remote wipe*' zult u dus ook bij blootstelling van gepseudonimiseerde gegevens aan onbevoegde kennisname op basis van de specifieke omstandigheden van het geval moeten vaststellen of er wordt voldaan aan de strenge norm van artikel 34a lid 6 Wbp. De onderstaande paragrafen kunt u daarbij gebruiken als leidraad. Verder is aan te bevelen om bij de beoordeling gebruik te maken van het advies over anonimiseringstechnieken dat de samenwerkende Europese toezichthouders in 2014 hebben uitgebracht.

11.3. Houdt het datalek waarschijnlijk een hoog risico in voor de rechten en vrijheden van betrokkene?

Het datalek moet aan de betrokkene worden gemeld indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene (artikel 34 lid 1 AVG).

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van persoonsgegevens in hun belangen worden geschaad. Verlies of onrechtmatige verwerking van dergelijke gegevens kunnen namelijk onder meer leiden tot onrechtmatige publicatie, aantasting in eer en goede naam, stigmatisering of uitsluiting van de betrokkene, tot schade aan de gezondheid, discriminatie, financiële schade of (identiteits)fraude. De schade kan derhalve van materiële en/of van immateriële aard zijn. Het vorenstaande is onder te verdelen in drie onderdelen:

- schending van de vertrouwelijkheid (financiële schade, reputatieschade, chantage, fysieke schade, identiteitsschade, misbruik van inloggegevens);
- beschikbaarheid (bepaalde diensten kunnen niet meer worden verleend, er kan niet (tijdig) betaald worden, betrokkene kan bepaalde activiteiten niet uitoefenen, rechten zoals het recht op verwijdering of rectificatie kunnen niet meer worden uitgeoefend);
- integriteit: (niet langer in overeenstemming met de werkelijkheid: onterechte beslissingen, financiële schade, fysieke schade).

Het is aan het IRT om te beoordelen of een datalek aan de betrokkene wordt gemeld. Indien er echter persoonsgegevens van gevoelige aard zijn gelekt (hoofdstuk 8.1), dan moet het IRT ervan uitgaan dat het datalek - niet alleen aan de AP - maar ook aan de betrokkene moet worden gemeld. In alle overige gevallen zal op basis van de omstandigheden van het geval een afweging moeten worden gemaakt door het IRT. Daarbij dient het IRT dan ook de aard en omvang van gelekte persoonsgegevens in ogenschouw te nemen (hoofdstuk 8.2). Het IRT stelt zich in dit verband steeds de volgende drie vragen:

- zijn er gevoelige gegevens gelekt?
- houdt de inbreuk waarschijnlijk een hoog risico in voor de rechten en vrijheden van betrokkene?
- hoe groot is het risico dat die nadelige gevolgen ook daadwerkelijk optreden?

Op basis van het antwoord op deze vragen kan het IRT de gevolgen/impact van het datalek voor betrokkene vaststellen op grond van onderstaand schema:[6]

Hoe groot is de impact van het datalek?	Geen gevoelige gegevens gelekt		Wel gevoelige gegevens gelekt	
	Beperkte nadelige gevolgen	Grote nadelige gevolgen	Beperkte nadelige gevolgen	Grote nadelige gevolgen
Kleine kans op nadelige gevolgen	Laag	Gemiddeld	Gemiddeld	Hoog
Grote kans op nadelige gevolgen	Gemiddeld	Hoog	Hoog	Hoog

[6] Dit schema kan het IRT ook gebruiken om de impact van het datalek op de eigen organisatie vast te stellen. De vragen worden dan gerelateerd aan de school zelf. Op basis van de antwoorden op de vragen, kan dan ook de impact voor de school worden vastgesteld en kan op basis daarvan worden besloten welke mensen en middelen er worden vrijgemaakt en welke acties worden ondernomen. Het gaat dan onder andere om impact als: reputatieschade, staken van proces, verlies van klanten, aansprakelijkheid, boete, intensivering van toezicht en naleving, concurrentienadeel, chantage en misbruik van inloggegevens.

Het informeren van de betrokkene over een opgetreden datalek is met name noodzakelijk in situaties waarin er voor de betrokkene daadwerkelijk ongunstige gevolgen voor de persoonlijke levenssfeer te duchten zijn (impact: hoog). Door de kennisgeving is de betrokkene alert op de mogelijke gevolgen van het datalek en kan de betrokkene zich, voor zover dat mogelijk is, daartegen beschermen door bijvoorbeeld extra voorzorgsmaatregelen te treffen (zoals vervanging van een wachtwoord) of door bepaalde (software)diensten en/of producten (tijdelijk) niet meer te gebruiken.

De AP kan, indien deze van oordeel is dat de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene, verlangen dat u alsnog een kennisgeving doet (tegen dit besluit staat bezwaar en beroep open).

Voorbeeld 20
Een Medewerker verliest een USB-stick met daarop de ledenlijst van het schoolkoor. Die bevat NAW-gegevens en e-mailadressen. Dit zijn geen gevoelige gegevens. Als de gegevens in onbevoegde handen vallen, dan kunnen de NAW-gegevens misschien gebruikt worden door een rivaliserende schoolkoor, of kan er spam worden verzonden aan de gelekte e-mailadressen. Dat zijn beperkte nadelige gevolgen. De kans op spam is klein vanwege het geringe aantal e-mailadressen (niet interessant om door te verkopen aan spammers), terwijl ook het scenario van het rivaliserende schoolkoor vrij onwaarschijnlijk lijkt. De te verwachten impact van het datalek is daarmee laag.

Voorbeeld 21
Hetzelfde voorbeeld, maar nu gaat het om een christelijk koor. In dit geval gaat het om gevoelige persoonsgegevens, omdat ze iets zeggen over de (waarschijnlijke) geloofsovertuiging van de personen op de lijst. Het meest waarschijnlijke nadelige gevolg is dat leden het vervelend vinden dat deze informatie mogelijk naar buiten komt. Dat is een beperkt nadelig gevolg. Bovendien is de kans gering dat het daadwerkelijk optreedt, want waarom zou iemand die deze informatie vindt deze openbaar maken. De te verwachten impact van het datalek is daarmee gemiddeld.

Voorbeeld 22
Hetzelfde voorbeeld, maar nu gaat het niet om een christelijk schoolkoor maar om een schoolvoetbalteam bestaande uit homoseksuele jongens en meisjes. Ook nu gaat het om gevoelige gegevens, en zeker in tijden van homohaat kan het lek grote nadelige gevolgen hebben voor de betrokkenen; denk aan pesterijen of zelfs fysiek geweld. Hoe groot de kans daarop precies is, is dan niet meer relevant: de te verwachten impact van het datalek is hoog.

11.4. Vergt de mededeling onevenredige inspanningen of zou de melding een onderzoek naar de omstandigheden van het datalek nodeloos hinderen?

Onevenredige inspanning
Het IRT mag de melding aan de betrokkene achterwege laten als de mededeling onevenredige inspanningen zou vergen (artikel 34 lid 3c AVG). In dat geval komt in de plaats van de melding aan betrokkene een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd. Van een onevenredige inspanning kan bijvoorbeeld sprake zijn omdat het gaat om een zeer groot aantal betrokkenen of omdat de betrokkenen lastig te contacteren zijn (bijvoorbeeld omdat enkel een IP-adres beschikbaar is). Een openbare mededeling kan bijvoorbeeld zijn een bericht via een regionale of landelijke nieuwswebsite of krant. Een alternatief kan ook meer gerichte

communicatie zijn die met grote waarschijnlijkheid alle betrokkenen bereikt. Bijvoorbeeld door een banner of bericht op de schoolwebsite te plaatsen.

Onderzoek naar toedracht

Tot slot zou een reden kunnen zijn om (nog) niet te melden aan de betrokkenen indien dit het onderzoek naar de toedracht van het datalek in gevaar zou kunnen brengen. Het IRT zal dan wel gedegen moeten kunnen onderbouwen waaruit dat gevaar bestaat dat als gemeld wordt aan de betrokkenen de toedracht van het lek niet, of mogelijk niet, achterhaald zal kunnen worden.

12. Hoe melden aan de betrokkene?

De melding aan de betrokkene is steeds schriftelijk en in duidelijke en eenvoudige taal. In de kennisgeving aan de betrokkene wordt in ieder geval vermeld:

- de aard en waarschijnlijke gevolgen van de inbreuk ('Wat is er aan de hand?');
- de persoon/instantie waar de betrokkene meer informatie over de inbreuk kan krijgen ('Waar kan ik terecht met vragen?');
- de maatregelen die de school heeft voorgesteld of genomen om de inbreuk aan te pakken ('Wat is er al gedaan'); en
- de maatregelen die de betrokkene worden aanbevolen om de negatieve gevolgen van de inbreuk te beperken ('Wat kan ik doen?') (artikel 34 lid 2 AVG).

Bij het beschrijven van de aard van de inbreuk kan de school doorgaans met een algemene omschrijving volstaan. De school neemt de contactgegevens van de FG op zodat de betrokkene hem of haar kan bereiken als de betrokkene vragen heeft over het datalek. Verder geeft de school aan wat de betrokkene zelf kan doen om de negatieve gevolgen van het datalek te beperken. Te denken valt aan het veranderen van gebruikersnamen en wachtwoorden wanneer deze door de inbreuk mogelijk gecompromitteerd zijn. Het staat de school vrij om meer informatie toe te voegen aan de kennisgeving, maar dit is wettelijk niet verplicht.

Voorbeeld 23
De school biedt haar leerlingen een online account aan waarop ze kunnen inloggen om studieresultaten te raadplegen. De school ontdekt dat een derde zich illegaal toegang heeft verschaft tot de database met gebruikersnamen en wachtwoorden van de website. De wachtwoorden zijn niet adequaat versleuteld. De school onderneemt de volgende acties:
- *zij informeert de (ouder(s) en/of verzorger(s)) van de leerlingen over het datalek. De school raadt daarbij aan om, voor alle accounts (ook die buiten schoolverband) waar de leerling hetzelfde wachtwoord gebruikt, dit wachtwoord te wijzigen;*
- *zij reset alle wachtwoorden en dwingt alle leerlingen om een nieuw wachtwoord op te geven. De school doet dit op een veilige manier zodat zij zeker weet dat het haar leerlingen zijn die een nieuw wachtwoord aanmaken, en niet een onbevoegde derde, en zij geeft hierbij ook aan waarom de leerling een nieuw wachtwoord aan moet maken;*
- *zij past haar systemen aan, zodat alle gebruikte wachtwoorden op een adequate manier worden versleuteld.*

Voorbeeld 24
Mogelijke aanpak als gevolg van datalek op school door 'bug' in software van aanbieder digitaal leermiddel:
- *de school stuurt een e-mail naar de betrokkenen waarin kort wordt aangegeven wat er is gebeurd en wat de betrokkene zelf kan doen om de negatieve gevolgen tegen te gaan.*
- *In de e-mail aan de betrokkenen verwijst de school naar meer uitgebreide informatie op de website van de school. Daar licht de school de aard van de inbreuk en de maatregelen die zijn getroffen en maatregelen die de betrokkene zelf kan treffen waar nodig nader toe.*
- *Verder verwijst de school in de e-mail naar de FG (e-mail, telefoonnummer) waar de betrokkene nadere informatie kan verkrijgen.*

Het belangrijkste is, dat de school zo veel mogelijk betrokkenen bereikt met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken. Met enkel een bericht in de media wordt dat doel normaal gesproken niet bereikt. Het IRT dient dan ook zorgvuldig te bepalen via welke kanalen de melding aan de betrokkene wordt gedaan en wat exact

aan de betrokkene wordt gemeld. Het IRT zal daar bij voorkeur gebruik maken van de expertise van de communicatiedeskundige.

13. Wanneer melden aan de betrokkene?

De school moet het datalek *onverwijld* melden aan de betrokkene (artikel 34 lid 1 AVG). Onverwijld betekent in dit verband: zonder onredelijke vertraging oftewel zo snel als redelijkerwijs mogelijk. De termijn hangt vooral af van de aard van het risico; hoe acuter het risico hoe sneller de mededeling moet worden gedaan.

Het onverwijld melden houdt in dat, na het ontdekken van het datalek, enige tijd genomen mag worden voor nader onderzoek of het nemen van passende maatregelen zodat de betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd. Voorkomen moet namelijk ook worden dat te snel en daarmee onjuist wordt geïnformeerd richting de betrokkene of dat er te weinig tijd besteed wordt aan het aanpakken van de inbreuk door het nemen van passende maatregelen. Wel moet er rekening mee worden gehouden 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 school de betrokkene daarover informeert, hoe eerder deze in actie kan komen.

Net als bij de melding aan de AP kan er eventueel voor gekozen worden door het IRT om de betrokkene in eerste instantie te informeren op basis van de informatie waarover op dat moment wordt beschikt, zodat de betrokkene alvast maatregelen kan gaan treffen om zich te beschermen tegen de gevolgen van het datalek, en om deze informatie in tweede instantie op basis van nader onderzoek aan te vullen.

Voorbeeld 25
Indien de school weet dat onbevoegden toegang hebben gehad tot een database met inloggegevens, maar dat de school nog aan het onderzoeken is of de onbevoegden ook andere persoonsgegevens hebben ingezien, kan de school in een dergelijk geval meteen al beginnen met het resetten van de getroffen wachtwoorden en met het informeren van de betrokkenen, waarbij zij aangeeft dat betrokkenen, als zij elders dezelfde inloggegevens gebruiken, deze moeten wijzigen.

In de melding aan de AP moet worden aangeven of het datalek al aan de betrokkenen is gemeld en, zo niet, wanneer dat dan wel plaatsvindt. De termijn die in de melding aan de AP wordt aangegeven, moet ook worden nagekomen. Mocht deze termijn bij nader inzien niet haalbaar blijken te zijn, dan dient dat tijdig aan de AP te worden kenbaar gemaakt door middel van een aanpassing van de melding.

14. Melden aan overige partijen

Melding aan de AP en betrokkene zijn verplicht op basis van artikel 33 en artikel 34 AVG, althans als op basis voor vorenstaande hoofdstukken is geoordeeld dat melding verplicht is. Dat neemt niet weg dat het voor de school noodzakelijk kan zijn om ook andere partijen – binnen en buiten de school – te informeren. Te denken valt aan partijen als:

- de verzekeraar van de school;
- Medewerkers (indien zij geen betrokkenen zijn);
- brancheorganisaties/ketenpartners (verwerkers); en
- media.

Van belang is dat de school probeert de communicatie met betrekking tot het datalek zo veel mogelijk in eigen hand te houden (ook intern). In dat verband is ook het IRT als enige binnen de school gerechtigd naar buiten toe te communiceren over het datalek. Daarmee wordt bereikt dat de school zelf deze derden kan berichten in plaats van dat zij dat van anderen (of zelfs vanuit de media) moeten vernemen. Hierdoor wordt ook bewerkstelligd dat er feitelijke gegevens over het datalek openbaar worden gemaakt in plaats van speculaties en mogelijk 'spookverhalen'.

Melding aan overige partijen wordt niet in de AVG voorgeschreven, maar indien wel besloten wordt te melden aan overige partijen kan het IRT daarbij het meest geschikte moment kiezen. Er zijn immers geen termijnen die in dit kader gelden. Het IRT kan dan ook namens de school communiceren met de overige partijen op het moment – en de wijze – waarop het best uitkomt voor de school. Het IRT zal – indien communicatie aan derden wenselijk/noodzakelijk is - een communicatieplan en actieplan opstellen voor deze eerste communicatie over het datalek, welk plan in ieder geval mede wordt afgestemd op de communicatie aan de betrokkene en AP. Bij het opstellen van een communicatieplan zal dan bij voorkeur de communicatieadviseur een belangrijke rol spelen.

De school zal in haar verwerkersovereenkomsten met verwerkers op voorhand afspraken maken dat de school beslist wie, wanneer en hoe het datalek extern (dus aan andere partijen dan AP en betrokkenen) wordt gecommuniceerd. Op deze wijze heeft de school de externe communicatie met betrekking tot het datalek in de hand en kan zij er ook voor kiezen welke partij (op positieve of negatieve wijze) op de voorgrond treedt. Zo zou een overweging kunnen zijn om de communicatie aan de derden door de verwerker te laten doen waar het datalek is ontstaan om zo de reputatieschade voor de school te beperken.

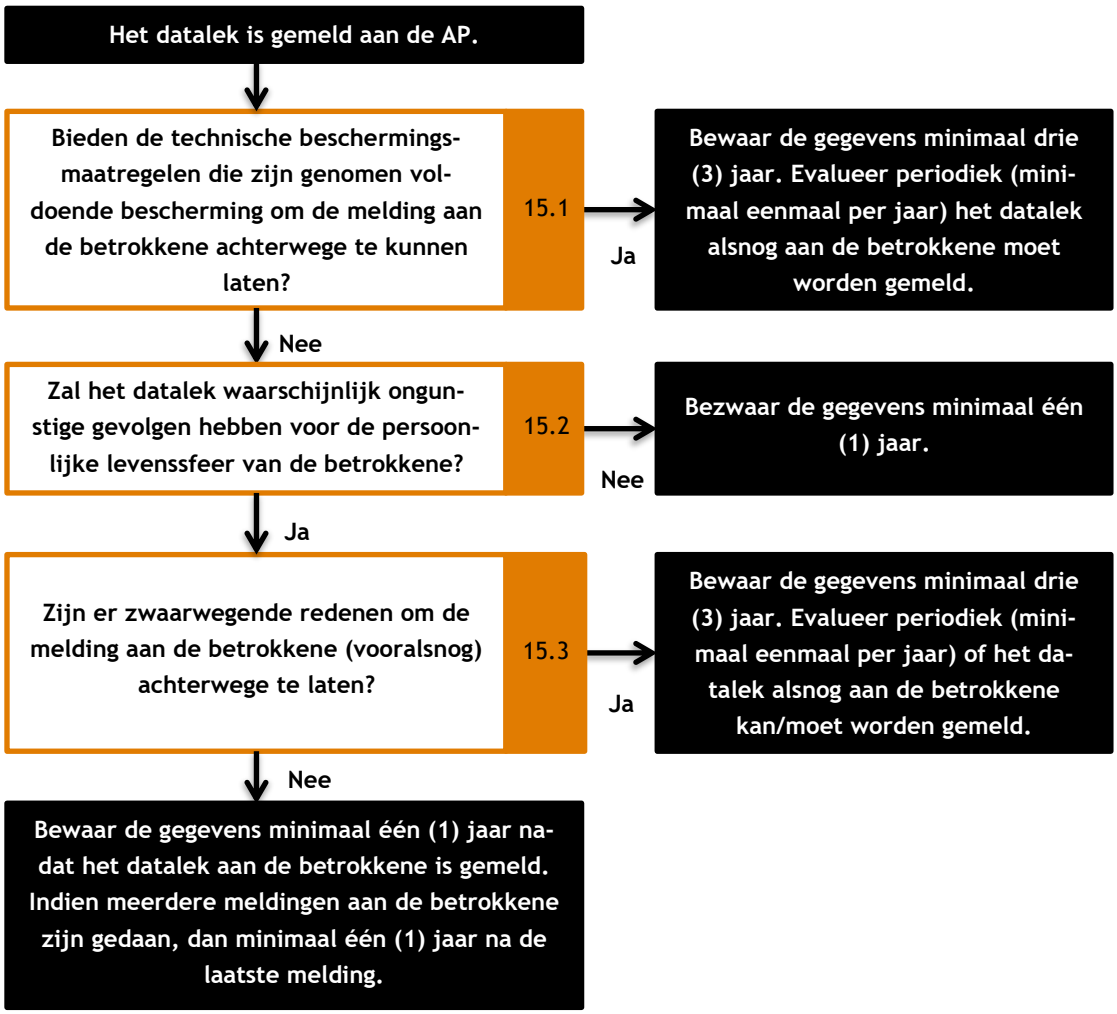
15. Welke gegevens moet de school documenteren?

De school dient ieder beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of ongeoorloofd zijn gewijzigd, verstrekt of ingezien, ongeacht of het moet worden gemeld, te documenteren (art. 33 lid 5 AVG), zie bijlage 5. Het overzicht hoeft niet openbaar te worden gemaakt. Per beveiligingsincident bevat het overzicht in ieder geval:

- de feiten en gegevens omtrent de aard van de inbreuk; en
- een beschrijving van de gevolgen van de inbreuk en de genomen corrigerende maatregelen.

De AP kan toegang verlangen tot deze documentatie en de documentatie moet adequaat zijn om de toezichthouder te laten controleren of beveiligingsincidenten daadwerkelijk worden gemonitord en opgevolgd. Zoals reeds aan bod is gekomen in paragraaf 7.2. betekent deze verplichting dat de school in een verwerkersovereenkomst duidelijke afspraken moet maken met verwerkers over de wijze van documenteren ten aanzien van beveiligingsincidenten die zich (mogelijk) voordoen bij verwerkers.

Wettelijk is niet voorgeschreven voor hoelang het overzicht moet worden bewaard. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren. Het onderstaande schema biedt u een beslismodel voor het vaststellen van de bewaartermijnen van geregistreerde datalekken zoals opgesteld in de beleidsregels van de AP.



Het bovenstaande schema gaat ervan uit dat de school de gegevens voor de volgende doeleinden bewaart:

- lering trekken uit het datalek en uit de wijze waarop het IRT dit heeft afgehandeld;
- antwoord kunnen geven op vragen van betrokkenen en derden;
- alsnog melden van het datalek aan de betrokkenen, indien dit in eerste instantie achterwege is gelaten en de omstandigheden vereisen dat dit alsnog gebeurt.

Voorbeeld 27
Het laatste bullet point kan zich voordoen als de school bij diefstal van een versleutelde USB-stick besluit om de kennisgeving aan de betrokkene achterwege te laten. De school moet zich er in een dergelijke situatie van bewust zijn dat de komst van nieuwe technieken nieuwe risico's kan inhouden, en dat er met grote regelmaat nieuwe kwetsbaarheden in breed gebruikte versleutelingsalgoritmen worden ontdekt. Dit houdt in dat de school, met de diefstal van de versleutelde USB-stick in het achterhoofd, over een langere periode alert moet zijn op deze risico's. Bij signalen van mogelijke 'ontsleuteling' zal de school alsnog de afweging moeten maken of u de betrokken personen moet informeren.

Er dient verder rekening mee gehouden te worden dat een vervolgprocedure na een datalek juridische maatregelen kan omvatten (civiel- of strafrechtelijk), en dat de school waar dat aan de orde is het bewijsmateriaal moet verzamelen, bewaren en presenteren overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Nadat zich binnen de school een datalek heeft voorgedaan dat is gemeld aan de AP, zal de FG ieder half jaar een vergadering beleggen waarbij de vaste leden van het IRT bij aanwezig zullen zijn. Indien daar aanleiding voor is kunnen daarvoor door de FG – in overleg met de voorzitter van het IRT - ook de forensisch IT-deskundige, juridisch adviseur of communicatieadviseur voor worden uitgenodigd. Tijdens deze bespreking stelt het IRT vast of er met betrekking tot reeds plaatsgevonden datalekken alsnog geïnformeerd moet worden aan de betrokkenen (en eventueel derden) als gevolg van (technische) ontwikkelingen.

16. Handelswijze Autoriteit persoonsgegevens na melding en handhaving

Dit hoofdstuk bespreekt wat de AP doet in het geval de school een datalek meldt aan de AP. Ook gaat dit hoofdstuk in op de handhaving bij overtreding van de meldplicht door de school.

16.1. Administratieve afhandeling

Na het melden van een datalek ontvangt de school per omgaande een ontvangstbevestiging. Als de melding de AP aanleiding geeft tot nadere actie, dan zal de AP daarover contact met de school opnemen. In eerste instantie zal het daarbij gaan om verificatie dat de gedane melding daadwerkelijk van de school afkomstig is, en om eventuele inhoudelijke vragen over de melding die op dat moment (reeds) zouden bestaan.

16.2. Inhoudelijke afhandeling

Het is de verantwoordelijkheid van de school om de oorzaak van het datalek op te sporen, en om maatregelen te treffen om herhaling te voorkomen. Het is ook aan de school om te bepalen of zij de betrokkenen informeert en op welke manier zij dit doet. Dit handboek dient om de school in die besluitvorming te ondersteunen. De AP biedt, als toezichthouder, geen ondersteuning bij de afhandeling van een concreet datalek.

De ontvangen datalekmeldingen stellen de AP in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijke raken, of waarvan zij last kunnen ondervinden. Als de school het datalek niet heeft gemeld aan de betrokkene kan de AP, indien deze van oordeel is dat het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene, verlangen dat de school alsnog een kennisgeving doet (artikel 58 lid 2e AVG). Het niet nakomen van dit bevel door de AP levert een overtreding op die is onderworpen aan een administratieve geldboete. Zie voor de hoogte van deze boete paragraaf 16.4.

Ook kan de AP op basis van de ontvangen datalekmeldingen actie ondernemen om de adequate beveiliging van persoonsgegevens (binnen de school) meer in de breedte te bevorderen. Als uit de ontvangen datalekmeldingen blijkt dat de beveiliging van persoonsgegevens mogelijk niet op orde is, dan kan dat voor de AP aanleiding vormen voor nader onderzoek naar de naleving van de beveiligingsverplichtingen uit de AVG binnen de school.

16.3. Register van ontvangen datalekmeldingen

De AP houdt een register bij van de ontvangen datalekmeldingen. Dit register is niet openbaar. Het belang bij het vertrouwelijk blijven van gegevens over de beveiliging van de gegevensverwerking of over gelekte persoonsgegevens staat daaraan in de weg. Wel kan de AP op basis van de gedane

meldingen in jaarverslagen of andere publicaties op geanonimiseerd en geabstraheerd niveau aandacht besteden aan datalekken bij de school.

16.4. Handhaving

De AP heeft een onderzoeksbevoegdheden, corrigerende bevoegdheden en adviserende bevoegdheden (artikel 58 AVG). Daarnaast kan de AP een administratieve geldboete opleggen (artikel 83 AVG). De AVG kent twee categorieën geldboeten. Een relatief lage geldboete van maximaal € 10.000.000,00 of 2% van de jaaromzet wanneer de AP constateert dat administratieve bepalingen zijn overtreden en een hoge geldboete van maximaal € 20.000.000,00 of 4% van de jaaromzet voor meer fundamentele overtredingen of het niet opvolgen van bevelen van de AP.

Onderzoek door de AP

De AP kan en mag:

- van de school (en haar verwerkers) gelasten om informatie te verstrekken die de AP nodig heeft om haar taken uit te kunnen voeren. De school is verplicht hieraan mee te werken;
- onderzoek verrichten in de vorm van gegevensbeschermingscontroles (audit);
- een toetsing verrichten van eventueel conform artikel 42 lid 7 AVG afgegeven certificeringen;
- de school (of verwerker) in kennis stellen van een beweerde inbreuk op de AVG;
- toegang vorderen tot persoonsgegevens en andere noodzakelijke informatie;
- toegang vorderen tot ruimten in de school en hulpmiddelen waarmee persoonsgegevens worden verwerkt (bijvoorbeeld relevante software).

Corrigerende maatregelen door de AP

Naast de onderzoeksbevoegdheden mag de AP ook corrigerende maatregelen nemen, te weten:

- waarschuwen en berispen;
- de school gelasten tot uitvoeren van een specifiek recht van betrokkene (bijvoorbeeld het wissen van gegevens);
- de school gelasten om binnen een bepaalde termijn verwerkingen in overeenstemming te brengen met de AVG;
- de school gelasten om een inbreuk aan de betrokkene mee te delen;
- het opleggen van een tijdelijk of definitief verwerkingsbeperking of -verbod;
- de school gelasten om persoonsgegevens te rectificeren, wissen of verwerkingen te beperking en dit mee te delen aan betrokkene;
- een certificering in te (laten) trekken.

Adviezen door de AP

De AP heeft de bevoegdheid om adviezen te verstrekken (zoals in voorkomend geval het verplichte advies voorafgaand aan bepaalde gegevensbeschermingseffectbeoordelingen of bijvoorbeeld advies aan sectororganisaties over toepassing van de AVG) en om certificeringen en gedagscodes goed te keuren. Adviezen die op basis van deze bevoegdheid worden gegeven kunnen worden aangemerkt als een besluit in de zin van de Algemene wet bestuursrecht (Awb). Hiertegen staat bezwaar en beroep open.

Het opleggen van een geldboete door de AP

De AP kan bij overtreding van de verplichtingen uit de AVG een geldboete opleggen. De AP houdt bij het bepalen van de hoogte van de boete rekening met alle omstandigheden van het geval en dient gemotiveerd aan te geven hoe men aan het betreffende bedrag komt (artikel 83 lid 2 AVG). Hierbij betrekt de AP onder meer de aard, ernst en duur van de inbreuk en het aantal getroffen betrokkenen alsmede de door hen geleden schade.

Daarnaast zijn er boeteverhogende omstandigheden (bijv. recidive of tegenwerking onderzoek AP) en boeteverlagende omstandigheden (bijv. vergaande medewerking met AP of eigener beweging schadeloosstellen gedupeerden) die de AP bij de vaststelling van de boete kan meewegen.

Type schending	Maximale boetebedrag
I. schending van een verplichting van procedurele aard (artikel 84 lid 4 AVG) Toelichting: categorie I. ziet specifiek op schendingen van verplichtingen overeenkomstig de artikelen 8, 11, 25 t/m 39, 41 lid 4, 42 en 43 van de AVG.	€ 10.000.000,00 of 2% van de jaaromzet
II. schending van een meer principiële verplichting of die de privacy van betrokkene directer raakt (artikel 83 lid 5 AVG) en het niet opvolgen van een bevel van de AP (artikel 83 lid 6 AVG) Toelichting: categorie II. ziet specifiek op schendingen van verplichtingen overeenkomstig de artikelen 5, 6, 7, 9, 12 t/m 22, 44 t/m 49, krachtens hoofdstuk IX door Nederland vastgesteld recht en artikel 58 lid 1 en 2 van de AVG.	€ 20.000.000,00 of 4% van de jaaromzet

17. Evaluatie handboek

De FG zal minimaal eenmaal per jaar, of zoveel eerder als noodzakelijk mocht blijken, een vergadering beleggen met de vaste leden van het IRT om dit handboek en bijbehorende bijlagen te evalueren en te bezien of de uitgangspunten van dit handboek aanpassing behoeven in het kader van ontwikkelingen/wijzigingen in de wetgeving, rechtspraak of binnen de (organisatie van de) school zelf.

18. Bijlagen

Bijlage 1	Protocol Beveiligingsincidenten
Bijlage 2	Incident Response Team
Bijlage 3	Formulier gegevens datalek
Bijlage 4	Webformulier
Bijlage 5	Registratie datalekken (door verwerkingsverantwoordelijke)