Informatie over de Algemene Verordening Gegevensbescherming (AVG)

Jan Stuijver, adviseur AVS

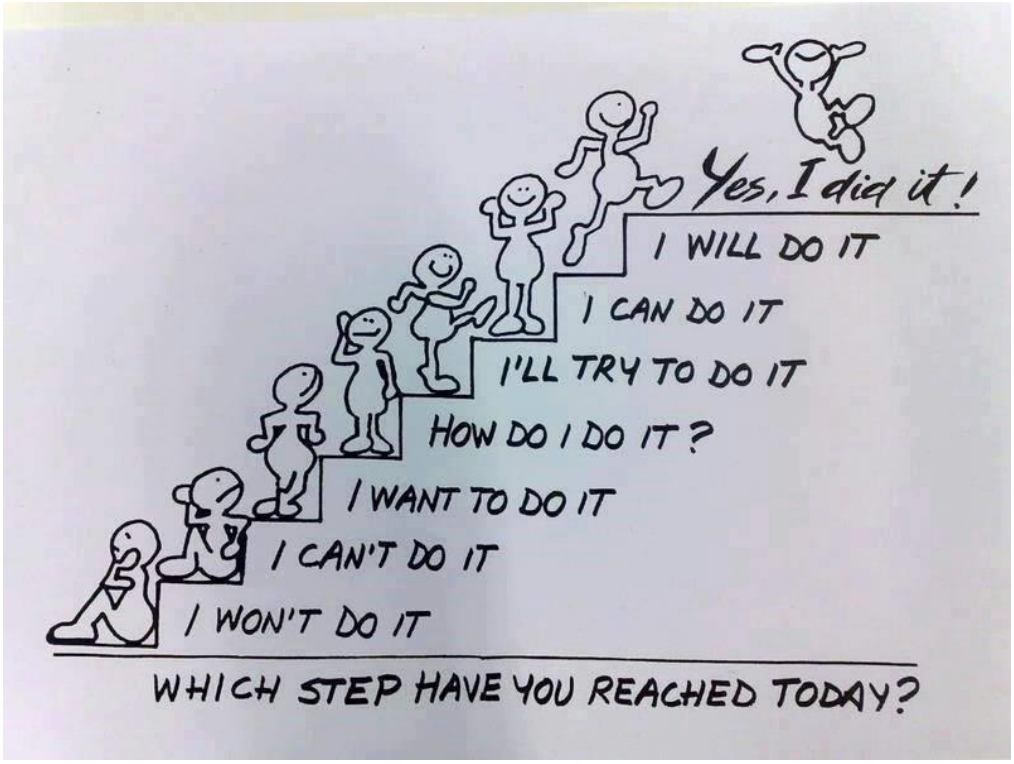
Januari 2017

Inhoud

In deze notitie schrijven we over de zaken die van belang zijn bij privacy. De Wet Bescherming Persoonsgegevens (WBP) en per mei 2018 de Algemene Verordening Gegevensbescherming (AVG) vraagt om e.e.a. in school goed te regelen. In deze notitie lichten we de belangrijkste zaken toe. Aan de orde komt de AVG en de zaken die daarbij horen (2). U kunt lezen over de zaken die u op school moet regelen en hoe om moet gaan met dossiervorming, leerlingvolgsysteem, beeldmateriaal, internet, toestemming gegevens delen, bewaartermijnen (3). In de notitie vindt u ook een voorbeeld van een vacaturetekst 4), en een voorbeeld van de werkwijze op school door de Functionaris Gegevensbescherming (5). Het laatste hoofdstukje (6) geeft u een voorbeeld van een privacyverklaring die u kunt gebruiken bij het privacyreglement.

1. Stappenplan

Dit stappenplan geeft u inzicht in de stappen die u kunt zetten om te komen tot goed beleid ten aanzien van privacy en de eisen die de AVG stelt.



1. Lees je in in de achtergrond van de AVG (zie hoofdstuk 2, 3).
2. Een bespreking met het team. Hierbij gaat het om bewustwording.
3. Check het privacyreglement en pas die daar waar nodig aan.
4. Check je emailverkeer en je emailserver.
5. Maak een lijstje met wie je als organisatie contacten hebt waarbij gegevensuitwisseling plaatsvindt.
6. Maak afspraken over beveiliging met aanbieders van programma's.
7. Maak een privacyverklaring gerelateerd aan het privacyreglement.
8. Kijk hoe je aan de verplichte Functionaris Gegevensbescherming (FG) wilt komen. Inhuren, via een stichting in de buurt met meerdere scholen (samenwerkingsafspraak), samen met andere eenpitters? Kijk naar inhoud en wat je van de persoon kunt vragen qua competenties (zie hoofdstuk 4, 5).
9. Kijk naar de inhoud van de schoolgids en pas aan wat nodig is.
10. Maak een Excelbestand voor vastleggen datalekken.
11. Betrek de MR bij de stappen > informeren en bij wijzigingen instemming ouders vragen voor gewijzigd beleid (zie WMS 13i).

2. Uitgebreide toelichting op de AVG

In de Wet bescherming persoonsgegevens (Wbp) zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd. Per 25 mei 2018 wordt de Wbp vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG) die in heel Europa van toepassing wordt. Deze nieuwe wetgeving stelt hogere en aanvullende eisen aan privacy.

De AVG stelt tal van uiteenlopende eisen aan organisaties die persoonsgegevens verzamelen of verwerken, inclusief de eis om aan de volgende **zes basisbeginselen** te voldoen:

-Transparantie, behoorlijkheid en rechtmatigheid bij de omgang met en het gebruik van persoonsgegevens. Je moet personen duidelijkheid bieden over de manier waarop je persoonsgegevens gebruikt en je hebt ook een 'rechtmatige basis' nodig om die gegevens te verwerken.

-De verwerking van persoonsgegevens moet beperkt blijven tot welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het is niet toegestaan om persoonsgegevens te hergebruiken of openbaar te maken voor doeleinden die niet 'verenigbaar' zijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld.

-Minimaliseren van de verzameling en opslag van persoonsgegevens tot wat toereikend en ter zake dienend is gezien de beoogde doelstelling.

-Waarborgen van de juistheid van persoonsgegevens met de mogelijkheid om deze te wissen of te rectificeren. Je dient maatregelen te nemen om te waarborgen dat de persoonsgegevens die je bewaart, juist zijn en dat deze bij fouten gecorrigeerd kunnen worden.

-Beperken van de opslag van persoonsgegevens. Je dient te waarborgen dat je persoonsgegevens uitsluitend bewaart gedurende de periode die nodig is om de doeleinden waarvoor de gegevens zijn verzameld, te realiseren.

-Waarborgen van de veiligheid, integriteit en vertrouwelijkheid van persoonsgegevens. Jouw organisatie moet er door middel van technische en organisatorische veiligheidsmaatregelen voor zorgen dat persoonsgegevens beveiligd zijn.

Artikel 4 van de AVG bevat een lijst met definities van de begrippen en termen zoals die in de verordening worden gebruikt. De volgende begrippen zijn daarbij met name van belang:

-*'Verwerkingsverantwoordelijke'*: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

-*'Verwerker'*: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

-*'Persoonsgegevens'*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

-*'Verwerking'*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

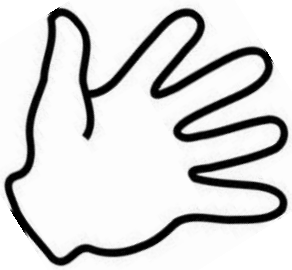
-*'Pseudonimisering'*: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

-*'Rechtsgrond'*: Op basis van de AVG mag je geen persoonsgegevens verwerken met als enige reden dat je dat graag wilt. Je moet concreet kunnen aantonen dat je een 'rechtsgrond' voor die verwerking heeft. De AVG voorziet in een aantal redenen wanneer dat verwerken is toegestaan, bijvoorbeeld wanneer de verwerking noodzakelijk is om een contract uit te voeren, wanneer personen toestemming hebben gegeven voor de

verwerking van hun gegevens of wanneer die verwerking in het 'gerechtvaardigde belang' is van de organisatie (mits dat belang niet ten koste gaat van de rechten van de betreffende personen).

In de **5 vuistregels** worden de belangrijkste (nieuwe) uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat.

1. Doelbepaling en doelbinding;
2. Grondslag
3. Dataminimalisatie
4. Transparantie (recht betrokkene)
5. Data-integriteit



Doelbepaling en doelbinding:
Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld en concreet doel. Deze persoonsgegevens mogen alleen worden verwerkt om dat vastgestelde doel te bereiken (doelbinding).
Let op: als een school gegevens verzamelt, die niet vallen onder het vrijstellingsbesluit, dan eist de Wbp van de school deze gegevensverzameling apart wordt aangemeld bij het Autoriteit Persoonsgegevens (AP) In de praktijk zal dit niet vaak voorkomen.
Met ingang van 25 mei 2018 is de Wbp niet meer van toepassing en gelden de regels vanuit de Algemene Verordening Gegevensbescherming (AVG). Scholen hoeven dan geen melding meer te doen, maar ze zijn verplicht zelf bij te houden welke gegevens waarvoor gebruikt worden: scholen moeten op hoofdlijnen weten welke gegevens voor welk doel worden gebruikt.

Grondslag:
Is er minimaal een wettelijke grond voor de verwerking?
Verwerking van persoonsgegevens is gebaseerd op een van de volgende wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.

Dataminimalisatie:
De persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel ('proportioneel') en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt ('subsidiair').
Het gaat er dus om dat scholen uitsluitend gegevens verzamelen die écht nodig zijn om het doel te bereiken. Niet: zo min mogelijk gegevens, wel: alleen relevante gegevens.

Dataminimalisatie heeft ook te maken met bewaartermijnen en nog meer met het vernietigen van data als de bewaartermijn is verstreken.

Transparantie:
De betrokkene (dus: de leerling en/of zijn ouders) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. De leerling en zijn ouders zijn op de hoogte van hun rechten als het gaat om de verwerking van persoonsgegevens door de school.

Data-integriteit:
De school zorgt er voor dat bij verwerkingen, die door of namens de school of schoolbestuur worden uitgevoerd, de juiste persoonsgegevens op het juiste moment op de juiste plaats beschikbaar zijn. Onjuiste gegevens worden op tijd gerectificeerd of gewist.
Voorbeeld: als iemand van buitenaf zomaar de persoonsgegevens kan wijzigen, dan zijn die gegevens niet meer 'integer'. De kwaliteit van de gegevens wordt allereerst bepaald door de medewerkers die gegevens invoeren. Zij moeten de juiste instructies krijgen om verantwoordelijk met persoonsgegevens om te kunnen gaan. Ook de programma's die gebruikt worden om de gegevens in op te slaan moeten integer zijn. Door het nemen van passende technische of organisatorische maatregelen zorgt de school er voor dat persoonsgegevens op een passende wijze zijn beveiligd en zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Waar komt de AVG in het kort op neer?
1. U moet exact weten welke bestanden met persoonsgegevens u beheert en in bezit heeft.
2. U moet weten welke rechten de personen hebben van wie u gegevens in bezit heeft.
3. Wanneer u een product of dienst ontwikkelt, dan moet er 'security by design' worden toegepast, oftewel: u moet gelijk nadenken hoe u de beveiliging van gegevens waarborgt en inbouwt.
4. Projecten met hoge risico's op lekken moeten vooraf een inschatting van privacy risico's krijgen, een zogenaamde Privacy Impact Analyse (PIA).
5. U mag persoonsgegevens alleen maar gebruiken voor het doel waar de informatie oorspronkelijk voor verzameld is.
6. Wie persoonsgegevens behandelt, is verplicht aan de strengere regelgeving te voldoen die de Algemene Verordening Gegevensbescherming (AVG) voorschrijft.
7. Artikel 4 van de AVG beschrijft twee rollen, die van de controller en van de processor.

Wanneer uw bedrijf persoonsgegevens opvraagt of verwerkt, wordt u gezien als de controller, ongeacht of u zelf direct data verzamelt.

8. U bent als controller volgens de AVG verantwoordelijk voor:

a. Het verzamelen van de gegevens en het toestemming hebben/verkrijgen van de persoon van wie de gegevens zijn.

b. Het zorgen dat deze gegevens alleen voor het doel worden verwerkt waarvoor ze zijn verkregen, en dat ze adequaat worden beveiligd.

c. Het verwijderen van data op verzoek van de persoon van wie de data is.

d. Het aangeven welk niveau van beveiliging vereist is.

Waar te beginnen?

De volgende vier belangrijke stappen om te komen tot AVG-proof zijn:

1. Traceren – het in kaart brengen van alle persoonsgegevens binnen jouw organisatie met de locaties waar ze zich bevinden.
Welke typen persoonsgegevens worden er binnen onze organisatie verwerkt?
Wat is het doel hiervan?

2. Beheren – het managen van de wijze waarop persoonsgegevens worden gebruikt en van de manier waarop ze toegankelijk zijn.
Van welke betrokkenen verwerken wij eigenlijk persoonsgegevens? Om wie gaat het eigenlijk? Waar moet u zeker op letten bij de bescherming van persoonsgegevens binnen uw organisatie per 25 mei 2018.

3 .Beveiligen – het nemen van veiligheidsmaatregelen om kwetsbaarheden en gegevensinbreuken te voorkomen, te traceren en aan te pakken.

4. Rapporteren – reageren op verzoeken omtrent gegevens, rapporteren van gegevensinbreuken en beschikbaarheid van de vereiste documentatie
Het eenvoudigst is om te beginnen met een inventarisatie van de gegevens die u nu binnen uw bedrijf heeft. U moet een antwoord te formuleren op de volgende vragen:

Welke valkuilen zijn er?

1. Er valt binnen de AVG meer onder persoonsgegevens dan u misschien denkt.

Onder persoonsgegevens vallen niet alleen gegevens die iemand direct identificeren, maar ook gegevens die gebruikt worden om mensen te individualiseren binnen een groep.
Het is dus van belang dat u zicht heeft op alle gegevens die verzameld worden en dat u goed weet welke gegevens allemaal onder persoonsgegevens vallen.

2. Een privacy-statement dat alleen u/de organisatie begrijpt.

Het is inmiddels gebruikelijk om in een privacy-statement aan te geven wat u als bedrijf

doet met persoonsgegevens. De AVG schrijft voor dat 'Informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk moeten zijn. Er moet duidelijke en eenvoudige taal worden gebruikt.' Als u eens kritisch naar uw eigen privacy-statement kijkt, hoe begrijpelijk is die tekst dan?

3. Enkel registreren van datalekken met nadelige gevolgen.
De huidige Wet bescherming persoonsgegevens verplicht bedrijven om een administratie bij te houden van iedere inbreuk die leidt tot een aanzienlijke kans op, dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.
De AVG breidt de eisen aan deze administratie uit. Per 25 mei 2018 bent u verplicht om alle inbreuken in verband met persoonsgegevens te documenteren en binnen 72 uur te melden aan de Autoriteit Persoonsgegevens. In deze administratie moeten per geval de feiten, de gevolgen en de maatregelen vastgelegd worden. Opmerkelijk is dat er sprake is van 'alle inbreuken', dus ook de inbreuken waarvoor geen meldingsplicht geldt.
Onder de AVG bent u dus verplicht een veel omvangrijkere administratie bij te houden dan nu het geval is. Ieder incident waarbij iemand "per ongeluk" toegang krijgt tot gegevens moet u strikt genomen registreren. Voor het onderwijs is wellicht een Functionaris Gegevensbescherming dan ook noodzakelijk.

4. Onvoldoende afspraken met uw IT-bedrijf.
De AVG bepaalt dat er afspraken gemaakt moeten worden over de melding van datalekken. Er staat niets vermeld over de inhoud van deze afspraken of de verantwoordelijkheden. Het is daarom verstandig om duidelijke afspraken met uw IT-bedrijf te maken over de informatie die nodig is om een goede en volledige administratie bij te houden. Op welke manier waarborgt uw IT-bedrijf dat de informatie die u nodig hebt bij een eventuele melding beschikbaar is? Verantwoordelijken kunnen anders met lege handen staan als de toezichthouder aanklopt en inzage vraagt in de (wettelijk verplichte) administratie. Ook belangrijk: kan uw IT-bedrijf aantonen dat u alles hebt gedaan om een lek te voorkomen? Dit laatste punt kan uw kans op een eventuele boete bij een inbreuk verkleinen.

Als alles op orde is wat dan?
De regels binnen de AVG staan genoteerd, u weet wat u moet doen om de persoonsgegevens binnen uw organisatie te beschermen, de valkuilen zijn bekend en een actieplan - inclusief een verdeling van verantwoordelijkheden - ligt klaar als er dan toch een datalek ontstaat. U bent al goed op weg als u deze voorbereidingen heeft getroffen. Maar hoe staat u op tijd paraat? Hoe signaleert en herkent u een datalek, zodat u op tijd een melding kunt maken?
Ten eerste is het belangrijk om in beeld te hebben welke persoonsgegevens u allemaal

opslaat. Welke kroonjuwelen heeft u onder uw hoede, wie heeft er toegang tot die gegevens en hoelang blijven deze bewaard? Samen met collega's zijn er van tevoren verschillende scenario's te bedenken waar het mis kan gaan.
Schakel daarom ook met uw IT-partners, zij weten precies welke aanvallen van buitenaf mogelijk zijn, kunnen systemen voor u monitoren en weten vanuit hun ervaring met andere klanten ook waar de pijnpunten binnen een organisatie zitten. Zodra u hier een goed overzicht van hebt, weet u precies waar een datalek kan ontstaan en dus ook waar u alert op moet zijn.
Bij organisaties van een redelijk formaat is het echter onvoldoende om alleen alert te zijn. Nóg belangrijker is het dat álle medewerkers die met persoonsgegevens omgaan bewust zijn van de privacygevoeligheid, dat zij volledig geïnformeerd zijn over de nieuwe regelgeving en hier samen met u alert op zijn. Ook is het belangrijk dat u een cultuur creëert waarbij medewerkers zich veilig voelen om een datalek te melden. Het is bekend dat menselijke fouten of slordigheden het merendeel van de datalekken veroorzaken. Uw IT-processen kunnen dan wel spic en span zijn, maar vergeet niet dat een verkeerd geadresseerd mailtje of het achterlaten van een usb stick ook zorgen voor een datalek.

Datalek voorkomen. Wat is dan van belang?

- Het opstellen van strakke richtlijnen binnen een organisatie is een belangrijke eerste stap.

Bewustwording speelt hierin een centrale rol; zorg ervoor dat medewerkers zich bewust zijn van hun gedrag wanneer ze omgaan met persoonsgegevens. Een niet-versleutelde PC kan onbewust een kwaadwillend persoon toegang verschaffen tot persoonsgegevens. Medewerkers die in de fout gaan moeten ook weten bij wie ze zich kunnen melden. Hoe langer zij wachten met melden, hoe groter de gevolgen voor alle betrokken partijen. Eventueel volgt ook nog een boete als het datalek niet binnen 72 uur gemeld is bij de Autoriteit Persoonsgegevens.
Gelukkig zijn er allerlei hulpmiddelen om de bewustwording van medewerkers te vergroten. In Microsoft Exchange vindt u bijvoorbeeld opties die alarm slaan wanneer mensen per ongeluk documenten met woorden als 'vertrouwelijk' of 'intern' versturen. Moderne firewalls hebben 'data leakage prevention', wat het lekken van data tegen gaat. Het is ook aan te raden uw netwerk te (laten) monitoren op afwijkend gedrag. U krijgt dan direct een seintje wanneer er bijvoorbeeld sprake is van een enorme toename van dataverkeer van binnen naar buiten. Verder zijn er diverse (goedkope) tools - waaronder de Canary - die waarschuwen wanneer er een hacker in uw netwerk zit.

- Denk niet alleen digitaal

Tegenwoordig gebeurt bijna alles online. Ook persoonsgegevens worden inmiddels bijna alleen nog maar online verwerkt. Toch zijn er ook zat voorbeelden van papieren datalekken. Denk bijvoorbeeld aan een verkeerd bezorgde brief met gevoelige

patiëntinformatie of een map met persoonsgegevens die uit een auto gestolen wordt. Ook hier gaat het om datalekken.
- Maak goede afspraken met het personeel.
- Zorg dus voor duidelijke afspraken met andere partijen.
Misschien maakt u gebruik van externe partijen die namens u persoonsgegevens verwerken. Die partijen moeten passende beveiligingsmaatregelen treffen en u in het geval van een datalek tijdig informeren. Zorg dus voor duidelijke afspraken met deze partijen, en dat zij bijvoorbeeld weten aan wie zij een eventueel datalek moeten melden.

Waar rekening mee houden?
De AVG voorziet in een aantal belangrijke aspecten die niet vergeten mogen worden.
Alle betrokkenen hebben uitgebreide rechten:
a. Zij mogen gegevens corrigeren als de verzamelde persoonsgegevens onjuist blijken te zijn (artikel 16).
b. Zij hebben ook het recht om 'vergeten te worden'; op verzoek dient u gegevens zo spoedig mogelijk ('zonder onredelijke vertraging') te wissen (artikel 17).
c. Zij hebben ook het recht om de eigen gegevens in een gestandaardiseerd formaat te ontvangen. Dan is het eenvoudiger om gegevens door te geven aan een andere leverancier van een vergelijkbare dienst, bijvoorbeeld wanneer zij overstappen (artikel 20).
d. En uiteraard hebben zij het recht om de eigen gegevens in te zien (artikel 15). U heeft ook een Registerplicht (artikel 30). Dat betekent dat u schriftelijk de belangrijkste aspecten van de persoonsgegevens die u verwerkt, moet vastleggen. Dit geldt niet voor organisaties met minder dan 250 medewerkers, tenzij:
-U stelselmatig en op grote schaal (bijzondere) persoonsgegevens verwerkt.
-De gegevensverwerking een groot risico voor de betrokkenen inhoudt.

Waar nog meer rekening mee houden?
U heeft nog steeds een meldplicht bij datalekken, net als in de huidige Wbp, maar:
1. De drempel wanneer u moet melden is lager geworden. U dient nu elk datalek te melden, mits er geen enkel risico is voor de 'vrijheden en rechten van individuen' (artikel 33).
2. Het datalek moet gemeld worden 'zonder onnodige vertraging' en binnen 72 uur nadat u deze heeft geconstateerd.
3. Bij een hoog risico voor de rechten en vrijheden van individuen moet u ook alle betrokkenen op de hoogte stellen (art. 34). Wat 'hoog' is dient u zelf in te schatten.
4. Wanneer u overheidsinstantie bent of een bedrijf dat het observeren van personen als (kern)activiteit heeft, dan moet u een Functionaris Gegevensbescherming (FG) aanstellen. Dit geldt ook wanneer u grote hoeveelheden gegevens verzamelt.

Incidenten en datalekken

Een *beveiligingsincident* is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.

Een *datalek* is een beveiligingsincident, waarbij gegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden enz.).

Let op: Alle datalekken zijn beveiligingsincidenten, maar niet ieder beveiligingsincident is een datalek.

Een school is verplicht binnen 72 uur een datalek te melden bij de Autoriteit Persoonsgegevens (AP).

Tip

Maak een centraal meldpunt met een standaard proces om datalekken *en* incidenten te melden en om vragen te stellen (zie voorbeeld hoofdstuk 6).

- ✓ Spreek af waar informatie en afspraken over AVG te vinden zijn:
  Bijvoorbeeld: incidenten@schoolX.nl
  - Eén adres om te communiceren
  - Eén proces voor de duidelijkheid
  - Eén register voor het overzicht
- ✓ De Functionaris Gegevensbescherming ziet zo alles voorbij komen en kan als een 'spin in het web' bijsturen waar nodig.

Van belang om te weten over publicatie beeldmateriaal

De Autoriteit Persoonsgegevens wijst in haar berichtgeving op het feit dat het voor scholen en ouders vaak onduidelijk is wat wel en niet mag bij publicatie van beeldmateriaal van leerlingen. De Autoriteit wijst op twee regels:

1. Scholen moeten expliciete toestemming hebben voor het publiceren van foto's of video's van leerlingen. Aandachtspunten hierbij:

a. Het gaat om toestemming van elke leerling die herkenbaar op de foto staat.

b. De toestemming moet ondubbelzinnig zijn. Dat betekent dat een school niet uit mag gaan van het principe 'wie zwijgt, stemt toe'.

c. Duidelijk moet zijn voor welke specifieke verwerking en doel de toestemming geldt. Toestemming voor het publiceren van foto's van een schoolreisje binnen een afgeschermde omgeving is dus nog geen toestemming voor publicatie van één van die foto's op de schoolsite.

2. Scholen moeten passende technische en organisatorische maatregelen treffen om beeldmateriaal van leerlingen, dat zij verzamelen en gebruiken, te beschermen.

De rol van de Medezeggenschap

Alle huidige privacyreglementen voor het verwerken van de personeels-en leerlinggegevens moeten worden aangepast aan de AVG. Dit houdt in dat besturen gewijzigde concepten aan de (G)MR voor moeten leggen. De personeelsgeleding heeft een instemmingsbevoegheid waar het gaat om het wijzigen van een regeling over het verwerken van en de bescherming van persoonsgegevens van het personeel (art. 12 lid 1 onder m WMS).De oudergeleding van de (G)MR heeft in het primair onderwijs een instemmingsbevoegheid met betrekking tot het wijzigen van ene regeling over het verwerken en de bescherming van persoonsgegevens van ouders en leerlingen (art. 13 lid 1 onder i Wms). In het voortgezet onderwijs komt die bevoegdheid toe aan de leerlinggeleding (art. 14 lid 3 onder de Wms).

Zie wet: Verordening (EU) 2016/679 Algemene Verordening Gegevensbescherming

3. AVG op school – vragen en antwoorden

Moet ik ieder jaar akkoord vragen voor het verwerken van de gegevens?
Volgens de AVG en tevens de website Autoriteit Persoonsgegevens (AP) moet je eerst of je de gegevens mag verwerken (grondslag) en volgens welk doel. Er staan geen bewaartermijnen in de AVG benoemd anders dan dat dit in overeenstemming moet zijn met het doel en als het doel voorbij is de gegevens vernietigd moeten worden. (Of gearchiveerd maar dat is een andere casus). De bewaartermijnen moeten dus door de organisatie zelf worden gedefinieerd in overeenstemming met het doel tenzij andere wetgeving verplicht tot bewaren. Er is nergens in de AVG beschreven dat dit jaarlijks moet worden vernieuwd.

Moeten we een Functionaris Gegevensverwerking aanstellen?
De Autoriteit Persoonsgegevens is van mening dat op basis van de huidige uitleg van de AVG dit van toepassing is voor onderwijsinstellingen. Daarnaast adviseren de PO-Raad, VO-raad en Kennisnet schoolbesturen om een FG aan te wijzen.
Met de komst van de AVG krijgt u als school meer verantwoordelijkheden om de persoonsgegevens van uw leerlingen goed te beschermen.

Digitalisering
Innovatieve, digitale systemen bieden interessante mogelijkheden om de kwaliteit van het onderwijs en de interne werkprocessen te verbeteren. Bijvoorbeeld met digitale toetsingsprogramma's, leerlingvolgsystemen en het gebruik van sociale media & apps. Maar deze nieuwe mogelijkheden om persoonsgegevens te verwerken, brengen ook de verantwoordelijkheid met zich mee om dat zorgvuldig en veilig te doen.
Onder de AVG moet u vooraf goed nadenken over de systemen waarmee u werkt of wilt gaan werken en hoe u die inricht (privacy by design). De standaardinstellingen moeten bovendien privacy vriendelijk zijn (privacy by default).

Verantwoordingsplicht
Nieuw onder de AVG is ook de verantwoordingsplicht. De verantwoordingsplicht houdt onder meer in dat u aan moet kunnen tonen welke technische en organisatorische maatregelen u hebt genomen om de persoonsgegevens van uw leerlingen te beschermen.
U moet aan de toezichthouder goed kunnen onderbouwen waarom u het recht hebt om bepaalde persoonsgegevens te verwerken. In sommige gevallen heeft u bijvoorbeeld toestemming nodig van leerlingen of hun ouders om persoonsgegevens te verwerken. Zoals voor het publiceren van foto's op uw website waarop leerlingen herkenbaar in beeld zijn. U moet dan kunnen laten zien dat u die toestemming heeft.

De AP stelt wel additionele voorwaarden aan beeldmateriaal (bijvoorbeeld bij scholen) dat het gebruik hiervan aan doelen moet worden gekoppeld en dat als dit doel voorbij je bij een nieuw doel opnieuw akkoord moet vragen.

Vragen over informeren en toestemming

Wanneer moet u leerlingen en ouders informeren over de persoonsgegevens die u verwerkt?

Net als onder de huidige Wet bescherming persoonsgegevens (Wbp) geldt onder de AVG de informatieplicht. Voor u als school betekent dat dat u verplicht bent om leerlingen en ouders te informeren over het verwerken van persoonsgegevens. Zodat zij weten welke gegevens u over hen verzamelt en wat u er mee doet.
Wanneer het gaat om kinderen onder de 16 jaar, dan moet u de ouders om toestemming vragen. Gaat het leerlingen ouder dan 16 jaar? Dan moet u de leerlingen zelf om toestemming vragen.

Direct en indirect verzamelen

U moet ouders en leerlingen informeren over de persoonsgegevens die u:

- direct via de ouderen en/of leerlingen ontvangt; of
- indirect, via andere kanalen verzamelt. Bijvoorbeeld via andere personen of via openbare informatie op internet.

Wanneer hoeft u ouders en leerlingen niet te informeren?

Als u de informatie direct bij ouders en leerlingen verzamelt dan hoeft u hen niet te informeren als:

- de betrokken persoon al over de informatie beschikt;
- het informeren onmogelijk blijkt of onevenredig veel inspanning zou vergen;
- het verkrijgen of verstrekken van deze gegevens uitdrukkelijk is voorgeschreven bij unie of lidstatelijk recht;
- de persoonsgegevens vertrouwelijk moeten blijven vanwege beroepsgeheim of statutaire geheimhoudingsplicht.

Welke informatie moet u leerlingen en/of ouders geven over de persoonsgegevens die u verwerkt?

Net als onder de huidige Wet bescherming persoonsgegevens (Wbp) geldt onder de AVG de informatieplicht. Welke informatie u ouders en leerlingen moet geven, hangt af van of

u de persoonsgegevens ‘direct’ of ‘indirect’ bij de betrokken leerlingen en/of ouders verzamelt.

Informatieplicht bij ‘direct’ verzamelde informatie

Verwerkt u persoonsgegevens die u rechtstreeks via de ouders en/of leerlingen verzamelt? Dan moet u hen gelijktijdig informeren over het volgende:

a. de identiteit en de contactgegevens van uw organisatie, of de vertegenwoordiger van uw organisatie;
b. indien van toepassing, de contactgegevens van de functionaris gegevensbescherming;
c. voor welk doel u de persoonsgegevens verwerkt en de rechtsgrond;
d. indien de grondslag van de gegevensverwerking gebaseerd is op gerechtvaardigd belang, op basis van welke grondslag u de persoonsgegevens verwerkt;
e. indien van toepassing: aan wie u de persoonsgegevens (mogelijk) verstrekt;
f. indien van toepassing: of u van plan bent om de persoonsgegevens te verstrekken aan een derde land of internationale organisatie. En zo ja, om welk land of internationale organisatie het dan zou gaan;
g. hoe lang u de persoonsgegevens zult bewaren;
h. wat de rechten van ouders en/of leerlingen zijn;
i. indien van toepassing, of u de persoonsgegevens gebruikt bij het opstellen van profielen van leerlingen en wat hiervan de gevolgen zijn.

Let op: geef bij het verzamelen van de persoonsgegevens duidelijk aan welke informatie ouders en/of leerlingen verplicht aan u moet geven. En ook wat de gevolgen zijn als zij dat niet doen.

Informatieplicht bij ‘indirect’ verzamelde informatie

Verzamelt u persoonsgegevens van ouders en/of leerlingen via andere kanalen? Bijvoorbeeld via andere personen of via openbare informatie op internet. Dan moet u ouders en leerlingen de volgende informatie over uw gegevensverwerkingen geven:

j. de identiteit en de contactgegevens van uw organisatie, of de vertegenwoordiger van uw organisatie;
k. indien van toepassing: de contactgegevens van de functionaris gegevensbescherming;
l. welke (categorieën van) persoonsgegevens u heeft verkregen;

m. van wie/wat u de persoonsgegevens heeft verkregen;
n. voor welk doel u de persoonsgegevens verwerkt;
o. als de grondslag van de gegevensverwerking gebaseerd is op gerechtvaardigd belang, op basis van welke grondslag u de persoonsgegevens verwerkt aan wie u de persoonsgegevens (mogelijk)verstrekt;
p. of u van plan bent de persoonsgegevens te verstrekken aan een derde land of internationale organisatie. En zo ja, om welk land of internationale organisatie het dan zou gaan;
q. hoe lang u de persoonsgegevens zult bewaren;
r. wat de rechten van ouders en/of leerlingen zijn;
s. indien van toepassing, of de persoonsgegevens gebruikt worden bij het opstellen van profielen van leerlingen en wat hier de gevolgen van zijn.

Waar moet u als school op letten als u ouders/leerlingen informeert over de gegevens die u verwerkt?

Informeert u ouders en/of leerlingen over de verwerking van persoonsgegevens binnen uw school? Dan moet u volgens de Algemene verordening gegevensbescherming (AVG) aan een aantal eisen voldoen.

Duidelijke taal

De informatie moet beknopt, eenvoudig, toegankelijk en begrijpelijk zijn. Het moet voor ouders en/of leerlingen duidelijk zijn wat u bedoelt als het over de verwerking van persoonsgegevens gaat.
U moet het taalgebruik dus aanpassen aan de betreffende doelgroep. Dit laatste geldt in het bijzonder wanneer u leerlingen informeert.

Schriftelijk

U moet de informatie schriftelijke geven. Hieronder valt volgens de AVG ook de elektronische vorm. Dat betekent dat u de informatie bijvoorbeeld via uw website of per e-mail mag geven.

Hoe vraagt u onder de AVG toestemming voor het publiceren van beeldmateriaal van leerlingen?

Net als onder de huidige Wet bescherming persoonsgegevens (WBP) heeft u ook onder de AVG toestemming nodig voor het publiceren van beeldmateriaal van leerlingen. Nieuw onder de AVG is dat u als school moet kunnen aantonen dat u toestemming heeft van de leerlingen of hun ouders/voogd.

Toestemming van leerling of ouder

Wilt u beeldmateriaal publiceren van een leerling van 16 jaar of ouder? Bijvoorbeeld online of in een papieren schoolkrant? Dan moet de leerling daarvoor zelf toestemming geven. Is de leerling jonger dan 16 jaar? Dan heeft u toestemming nodig van zijn of haar ouder. Het moet voor leerlingen en ouders net zo makkelijk zijn om de toestemming weer in te trekken als om de toestemming te geven.

Waar moet de toestemming aan voldoen?

Bij geldige toestemming moet elke twijfel zijn uitgesloten. De toestemming moet aan drie voorwaarden voldoen:

t. de toestemming moet vrij en niet onder druk gegeven zijn. De leerling of ouder mag bijvoorbeeld niet benadeeld worden als hij of zij geen toestemming geeft;
u. de toestemming moet ondubbelzinnig zijn. Het moet dus volstrekt helder zijn dát er toestemming is verleend. U mag niet uit gaan van het principe 'wie zwijgt, stemt toe';
v. u hebt toestemming gevraagd voor een specifieke verwerking en een specifiek doel. Bijvoorbeeld om via foto's en video's op uw website verslag te doen van een schoolreisje aan alle ouders.

Tip: u kunt ervoor kiezen om in een keer toestemming te vragen voor de publicatie van beeldmateriaal voor meerdere activiteiten gedurende het schooljaar. Maar let op: dit mag alleen als per activiteit aan bovenstaande drie voorwaarden (t,u,v) is voldaan.

Hoe zit het met privacy en leerlingvolgsysteem?

Bestaande regels

Net als onder de Wbp geldt onder de AVG voor leerlingvolgsystemen dat:

- U alleen gegevens mag verwerken als dat noodzakelijk is voor het doel;
- De gegevens die u verwerkt juist moeten zijn;
- U de beveiliging van en de toegang tot het systeem goed regelt. Dit houdt bijvoorbeeld in dat er niet meer mensen toegang mogen hebben tot de persoonsgegevens van leerlingen dan noodzakelijk is voor het doel. Ook moet u de gebruikersactiviteiten van het systeem bijhouden (loggen).

Nieuwe regels

Belangrijke nieuwe regels onder de AVG die ook relevant zijn voor leerlingvolgsystemen zijn:

- Onder de AVG moet u als school kunnen aantonen dat u bij het gebruik van het leerlingvolgsysteem de regels van de AVG naleeft. Dit heet de verantwoordingsplicht.
- U moet de gegevensverwerking van het leerlingvolgsysteem opnemen in het zogenoemde register van verwerkingsactiviteiten.
- Ook schrijft de AVG voor dat voor bepaalde verwerkingen het doen van een Data protection impact assessment (DPIA) verplicht is. Gebruikt u een leerlingvolgsysteem op uw school? Dan kunt u verplicht zijn een DPIA uit te voeren. Ook als u op dit moment al een leerlingvolgsysteem gebruikt.
- Onder de AVG geldt het recht op dataportabiliteit. Dat is het recht van mensen om gegevens over te dragen. Bijvoorbeeld naar een andere school.

Het belang van privacy bij leerlingvolgsystemen

Als school bent u verplicht om te werken met een leerlingvolgsysteem. Een leerlingvolgsysteem houdt vorderingen en resultaten bij van leerlingen, groepen en van de school als geheel. Als onderwijsinstelling brengt u daarmee de leerprestaties en ontwikkeling van uw leerlingen dus systematisch in beeld. Ook andere gegevens, zoals verzuimgegevens en gezondheidsgegevens, kunnen in het leerlingvolgsysteem zijn opgenomen.

Gelet op de aard van de persoonsgegevens in een leerlingvolgsysteem en het feit dat kinderen extra kwetsbaar zijn, moet u als onderwijsinstelling dus zorgvuldig omgaan met de privacy bij leerlingvolgsystemen.

Voor een deel gelden onder de Algemene Verordening Gegevensbescherming (AVG) dezelfde regels voor leerlingdossiers als onder de huidige Wet bescherming persoonsgegevens (Wbp). Maar u moet zich straks ook aan een aantal nieuwe regels houden.

Over de leerlingdossiers

Als basisschool mag u verschillende gegevens over een leerling bewaren in het zogeheten leerlingdossier. Dit dossier bestaat uit administratieve gegevens en informatie die nodig is voor het onderwijs aan en de begeleiding van de leerling. Het leerlingdossier kan de volgende gegevens over een leerling bevatten:

- gegevens over in- en uitschrijving;
- gegevens over afwezigheid;
- adresgegevens;
- gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt;
- het onderwijskundig rapport;

- gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen;
- gegevens over de vorderingen en de resultaten van de leerling;
- verslagen van gesprekken met de ouders;
- de resultaten van eventueel psychologisch onderzoek.

Het belang van privacy bij leerlingdossiers

Een leerlingdossier maakt het dus mogelijk om de ontwikkeling, het gedrag en leerprestaties van een leerling systematisch in beeld te brengen en te volgen. Ook kan een leerlingdossier bijzondere persoonsgegevens bevatten (gegevens over de gezondheid van de leerling). Gelet op de aard van de verwerking van persoonsgegevens in een leerlingdossier en het feit dat kinderen extra kwetsbaar zijn, moet u als onderwijsinstelling dus zorgvuldig omgaan met persoonsgegevens

De regels voor bewaartermijnen die nu onder de Wet bescherming persoonsgegevens (Wbp) gelden, veranderen niet onder de AVG. Dat betekent dat u als school het leerlingdossier 2 jaar mag bewaren nadat de leerling van school is gegaan. Net als nu geldt onder de AVG in sommige situaties een langere bewaartermijn.

Situaties met langere bewaartermijnen

De AVG-regels voor bewaartermijnen gaan naast een aantal huidige regels voor langere bewaartermijnen bestaan, zoals:

- In het lager en voortgezet onderwijs geldt dat u gegevens over verzuim en afwezigheid en in- en uitschrijving 5 jaar moet bewaren nadat de leerling is uitgeschreven;
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen, moet u als school 3 jaar na het vertrek van de leerling bewaren;

Adresgegevens voor reünies

U mag als school adresgegevens van oud-leerlingen bewaren voor het organiseren van reünies. Let er wel op dat u hiervoor eerst toestemming vraagt aan de oud-leerlingen en u de gegevens dan alleen voor dat doel mag gebruiken.

Hoe omgaan met persoonsgegevens op internet?

Veel mensen publiceren gegevens over zichzelf of over anderen op internet, zoals foto's op Facebook. Ook organisaties plaatsen persoonsgegevens op internet. De gevolgen hiervan kunnen groot zijn voor de mensen om wie het gaat. Onder meer omdat eenmaal

op internet geplaatste gegevens jaren later nog vindbaar zijn. Dit kan bijvoorbeeld bij een sollicitatie nadelige gevolgen hebben.

Toestemming nodig
Niemand mag zomaar persoonsgegevens van een ander op internet publiceren. Dit mag in principe alleen als deze persoon hiervoor toestemming geeft. Mensen hebben ook het recht om hun toestemming later in te trekken.

Uitzondering voor persoonlijk gebruik
Is een website of profiel op een sociale netwerksite alleen toegankelijk voor een beperkte kring mensen? En wordt de website of het profiel niet voor professionele of commerciële doeleinden gebruikt? Dan mag iemand daarop informatie over anderen publiceren zonder hun toestemming.

Uitzondering voor journalistiek
Ook voor journalistieke publicaties, zoals een nieuwsartikel op internet, geldt een uitzondering. Journalisten mogen zonder toestemming persoonsgegevens op internet plaatsen. De publicatie moet dan wel aan bepaalde voorwaarden voldoen.

Persoonsgegevens verwijderen
Staan iemands gegevens op internet, dan heeft diegene het recht om deze gegevens te laten verwijderen. Bijvoorbeeld omdat ze onjuist, onvolledig of verouderd zijn of omdat ze niet ter zake doen.

Mag klassenfoto op website van school?
Mede door de opkomst en de toename van de digitale middelen wordt het steeds gemakkelijker om informatie snel onder een grote doelgroep te verspreiden. Ook scholen hebben hiermee te maken. De mogelijkheden lijken tegenwoordig eindeloos. Echter, de praktijk leert dat scholen hierbij nog wel eens vergeten rekening te houden met de wettelijke kaders die hiervoor gelden.

Een aantal praktijkvoorbeelden
In de praktijkvoorbeelden gaat het met name op leerlinggegevens, maar de uitgangspunten zijn ook van toepassing op personeelsgegevens.

We hebben de website van onze school vernieuwd. Mogen we daarop ook de klassenfoto's en de namen van leerlingen vermelden?
In dit voorbeeld wordt gesproken over klassenfoto's en namen van leerlingen. De naam van een leerling betreft altijd een persoonsgegeven. Een klassenfoto kan ook persoonsgegevens bevatten als kinderen herkenbaar in beeld zijn gebracht. Als dit het

geval is, betreffen dit dus ook persoonsgegevens. Verwerking (plaatsing op de website) is dus enkel toegestaan als daar een grondslag (a t/m f van artikel 8) uit de Wbp voor bestaat. Met andere woorden: als er geen toestemming is gegeven door de ouders van de leerling (of de leerling zelf als hij/zij 16 jaar of ouder is), zal vastgesteld moeten worden of sprake is van een gerechtvaardigd belang (de andere grondslagen bieden immers in deze situatie geen grondslag om de gegevens te mogen verwerken). Of sprake is van een gerechtvaardigd belang, zal afhangen van de vraag of het belang van de school bij plaatsing van de foto's en de namen groter is dan het privacybelang van de leerling. Dit zal naar alle waarschijnlijkheid in de meeste situaties niet het geval zijn. Plaatsing van de foto's en de namen is dan dus zonder toestemming niet toegestaan.

Jeugdzorg/Veilig Thuis vraagt informatie op over een leerling. Ben ik verplicht om mee te werken?
Ook voor deze casus geldt dat er een grondslag moet zijn uit de Wbp. Geven de ouders toestemming, dan is het geen probleem om de gevraagde informatie te verstrekken. Toestemming is echter niet altijd noodzakelijk. Als er serieuze zorgen zijn over de leerling, kan de school zowel gevraagd als ongevraagd informatie over de leerling verstrekken aan Jeugdzorg/Veilig Thuis voor zover dit noodzakelijk wordt geacht voor de behartiging van het gerechtvaardigd belang van de leerling, ook zonder toestemming van de ouders. In beginsel moet de school ouders hiervan wel vooraf op de hoogte stellen. Echter, als de veiligheid van het kind of van een ander in het geding is of er haast geboden is, kan hierop een uitzondering worden gemaakt. Op het moment dat het specifiek om (een redelijk vermoeden van) kindermishandeling gaat, biedt artikel 5.2.6 van de Wet Maatschappelijke Ondersteuning 2015 (WMO) zelfs een wettelijke basis voor de gegevensverstrekking. Dit artikel bepaalt namelijk dat een school informatie aan Veilig Thuis mag geven om de kindermishandeling te laten stoppen of een redelijk vermoeden van kindermishandeling te laten onderzoeken.

Een leerling verlaat de basisschool. Ouders zijn het niet eens met het opgestelde onderwijskundig rapport en willen geen toestemming geven om dit rapport te verstrekken aan de vervolgschool. Mag het rapport toch worden doorgegeven?
Ja, dit mag. In de Wet op het primair onderwijs is namelijk opgenomen dat een schooldirecteur van elke leerling die de school verlaat een onderwijskundig rapport moet opstellen ten behoeve van de ontvangende school. Het is dus niet nodig dat ouders toestemming geven voor het verstrekken van het onderwijskundig rapport aan de vervolgschool. Er bestaat in dit geval een wettelijke verplichting om het rapport aan de vervolgschool te overhandigen. De gegevensverwerking kan dus gebaseerd worden op art. 8 sub c Wbp.

De leerkracht van hun kind bepaalde zorgen die er leven met betrekking tot hun kind, bespreekt met collega's. Mogen deze gegevens onderling worden uitgewisseld?
Binnen de school vindt doorgaans veel overleg plaats over leerlingen. Van periodieke klasbesprekingen tot de bespreking van individuele leerlingen met specifieke problematiek. Deze verwerking van persoonsgegevens vindt zijn grondslag in het feit dat verwerking noodzakelijk is om de onderwijsovereenkomst die de school met de ouders heeft na te komen (art. 8 onder b Wbp). Dit is (in het primair en voortgezet onderwijs althans) geen fysieke overeenkomst, maar doordat de ouders hun kind op school hebben ingeschreven, is de school verantwoordelijk voor het geven van goed onderwijs aan en de begeleiding van de betreffende leerling. Onderdeel van het geven van onderwijs aan en het begeleiden van leerlingen binnen de school is dat degenen die belast zijn met deze activiteiten of daarbij noodzakelijk zijn betrokken, periodiek overleggen. Ter uitvoering van hun taak mogen zij de daarvoor noodzakelijke gegevens ontvangen. Een leerkracht mag dus overleg voeren over de leerling met bijvoorbeeld een duo-partner of een intern begeleider, die belast is met de begeleiding van een leerling. Een leerkracht kan echter niet zomaar gegevens over de leerling verstrekken aan een collega van bijvoorbeeld een andere groep die op geen enkele wijze betrokken is bij het onderwijs aan en de begeleiding van de betreffende leerling. Ook derden kunnen belast zijn met onderwijs- en begeleidingsactiviteiten of daarbij noodzakelijk zijn betrokken. Zij zijn door de school ingeschakeld en hebben een taak binnen de reguliere ontwikkeling en begeleiding van leerlingen. Niet van belang is of deze derde, bijvoorbeeld een remedial teacher, in dienst is van de school of niet.

Een leerling van 17 jaar wil niet dat zijn ouders zijn dossier inzien. Dient de school zich hieraan te conformeren?
16 jaar is een belangrijke leeftijdsgrens in de Wbp. De leerling kan alleen een inzageverzoek met betrekking tot de eigen persoonsgegevens indienen als hij/zij 16 jaar of ouder is. Op het moment dat de leerling jonger is dan 16 jaar, kunnen de wettelijk vertegenwoordigers (bijvoorbeeld de ouders) een dergelijk verzoek doen. Een leerling van 17 jaar heeft dus het recht om zijn eigen dossier in te zien. Zijn ouders hebben op grond van de Wbp geen recht meer om het leerlingdossier van hun kind in te zien. Echter, uit de Wet op het primair onderwijs en de Wet op het voortgezet onderwijs vloeit voort dat de school verplicht is om de ouders, voogden of verzorgers te rapporteren over de vorderingen van de leerling zolang de leerling nog minderjarig is. Gelet op deze wettelijke verplichting (art. 8 onder c Wbp) dient de school in deze casus, ondanks het bezwaar van de leerling, de ouders toch inzage te geven in het leerlingdossier. Dit is echter wel beperkt tot informatie omtrent de vorderingen van het kind en geldt enkel zolang de leerling minderjarig is.

Daarnaast geldt dat in de meeste gevallen eventueel ook een beroep kan worden gedaan op het gerechtvaardigd belang (art. 8f). 'De meeste gevallen', omdat uiteraard elke keer een belangenafweging gemaakt dient te worden tussen het belang van de leerling en het belang van de ouders. Ouders dienen op grond van de het Burgerlijk Wetboek voor hun kinderen te zorgen, financieel zelfs tot hun kind 21 jaar is. In dat kader hebben ouders belang bij de informatie die is opgenomen in het leerlingdossier. Dit is dus breder dan enkel de informatie over de vorderingen. Als de ouders echter niet meer betrokken zijn bij de opvoeding van het kind, zal het belang van de leerling hoogstwaarschijnlijk zwaarder wegen en kan een ouder niet met een beroep op het gerechtvaardigd belang om inzage vragen in het leerlingdossier.

4. Voorbeeld vacaturetekst Functionaris Gegevensbescherming (FG)

Deeltijd

Bij de school / scholen …… worden gevoelige persoonsgegevens verwerkt. Om te zorgen voor een goede gegevensbescherming zijn we op zoek naar een enthousiaste Functionaris Gegevensbescherming (FG) voor … uur per week

Wat ga je doen binnen deze functie?

-Je houdt intern toezicht op en je adviseert over de verwerking van persoonsgegevens conform de geldende wet- en regelgeving: Wet Bescherming Persoonsgegevens (WBP) en Algemene Verordening Gegevensbescherming (AVG). Je voert audits gegevensbescherming uit op onze verschillende locaties en monitort de beveiligingsincidenten en datalekken die worden gemeld.

-Je verhoogt het bewustzijn van medewerkers over gegevensbescherming om te voldoen aan privacy wet- en regelgeving. Hiervoor ontwikkel je communicatiemiddelen, bezoek je afdelingen en ben je vraagbaak voor managers en medewerkers.

-Je toont aan dat de school/scholen aan de wettelijke regels voor gegevensbescherming voldoet en bouwt daarvoor verder aan de privacyboekhouding. Hierin staan o.a. beleid en regels voor informatiebeveiliging, het verwerkingenregister (dat houdt je actueel en volledig), auditplanning en -resultaten, alle acties voor awarenessbevordering en het plan om compliant te worden aan de AVG.

-Je ondersteunt de schoolleider(s) bij de totstandkoming en opvolging van bewerkersovereenkomsten met externe bewerkers van persoonsgegevens.

-Je voert waar nodig gegevensbeschermingseffectbeoordelingen uit in samenwerking met betrokkenen in de organisatie, denk aan de ict-er.

De FG heeft een onafhankelijke positie in de organisatie en rapporteert aan het bestuur. Organisatorisch ben je onderdeel van de afdeling ……. Je onderhoudt verder interne contacten met managers en medewerkers van afdelingen die werken met persoonsgegevens en de afdeling Informatievoorziening waar de informatiebeveiliging is belegd. De verantwoordelijkheid van datalekmeldingen bij de Autoriteit Persoonsgegevens ligt bij jou en de bestuurssecretaris. Je standplaats is ……., maar je bent tevens werkzaam op onze andere locaties.

Naar wie zijn we op zoek?

Je hebt een afgeronde HBO- of WO-opleiding en affiniteit met het onderwerp gegevensbescherming;
Je hebt kennis van de Nederlandse en Europese gegevensbeschermings wet en -regelgeving en vereisten;
Je hebt een opleiding op het gebied van gegevensbescherming of bent bereid die op korte termijn te volgen;
Je hebt kennis van de bedrijfssector (de ggz of vergelijkbaar), administratieve organisatie en informatiesystemen;
Je bent zorgvuldig, integer en professioneel en in staat om de boodschap goed over te brengen.

Wat wij bieden en hoe je kunt reageren

Je krijgt de ruimte om proactief te werken en nieuwe ideeën aan te dragen en uit te voeren. Arbeidsvoorwaarden zijn conform de CAO-PO. Het salaris is afhankelijk van je opleiding en werkervaring. Je begint met een aanstelling voor bepaalde tijd, met de intentie dit bij gebleken geschiktheid om te zetten in een vaste aanstelling. Bij voorkeur voer je deze functie uit in combinatie met een andere functie bij de school/scholen.

Voor meer informatie kun je contact opnemen met……..
Van iedere nieuwe medewerker wordt bij indiensttreding een Verklaring Omtrent Gedrag gevraagd.

5. Voorbeeldtekst over afspraken op school tav de AVG

AVG: waarschijnlijk heb je die afkorting wel ergens voorbij zien of horen komen? Misschien weet je ook al wel dat het iets met Privacy te maken heeft? En dat het moet! Tenminste, je, we of ze moeten er iets mee. En dat klopt! We moeten Privacy goed regelen. Jij, als medewerker, en zij, als leverancier of zorgpartner, ook. 'Het recht om met rust gelaten te worden' is een van de 10 grondrechten van de mens.

De **Algemene Verordening Gegevensbescherming** die vanaf 25 mei 2018 in werking treedt, ziet er op toe dat Privacy serieus wordt genomen. In heel Europa gelden daar dezelfde regels voor, hoewel een uitvoeringswet wat ruimte voor landelijke verschillen laat. Wat betekent dat precies voor ons? Nou dat in ieder geval de adagia 'Zo doen we het altijd' en 'Ja, maar dat is wel makkelijk' niet meer op gaan!

Sinds 2001 kennen we de Wet bescherming persoonsgegevens (Wbp). In eerste instantie zag het College bescherming persoonsgegevens toe op het goed regelen van Privacy. Sinds er ook (fikse) boetes uitgedeeld kunnen worden is de naam aangepast in Autoriteit Persoonsgegevens (AP). De AP ziet toe op naleving van de wet. De AVG is de strengere, Europese opvolger. De belangrijkste verschillen met de Wbp:

- de definitie persoonsgegeven is uitgebreid, IP-adressen, MAC- adressen, cookies vallen er ook onder;
- rechten van de betrokkene zijn uitgebreid, bijvoorbeeld het recht op dataportabiliteit en vergetelheid;
- er zijn geen vrijstellingen meer, maar in plaats daarvan is een Verwerkingsregister verplicht;
- bij verwerking op grote schaal dient er een data protection impact analyse gemaakt te worden;
- overheidsinstanties/publieke organisaties moeten een Functionaris Gegevensbescherming aanstellen.

De Functionaris Gegevensbescherming (FG)

We hebben dus ook een Functionaris Gegevensbescherming (FG) nodig. De FG is een belangrijke functionaris rondom de AVG. De FG is in ieder geval verantwoordelijk voor het houden van onafhankelijk toezicht op, en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens. Dit betekent dat de FG bij alle mogelijke processen waar persoonsgegevens worden gebruikt betrokken zou moeten zijn. Daarnaast loopt de formele communicatielijn van de organisatie naar de Autoriteit Persoonsgegevens met betrekking tot vragen en klachten over de verwerking van

persoonsgegevens via de FG. Dit is tevens de escalatielijn voor de FG als deze een escalatie nodig acht. De Functionaris Gegevensbescherming bij ons is:

Taken en verantwoordelijkheden FG

- toezicht houden;
- inventarisaties van gegevensverwerkingen maken;
- meldingen van gegevensverwerkingen bijhouden;
- vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
- interne regelingen ontwikkelen;
- adviseren over technologie en beveiliging (privacy by design);
- input leveren bij het opstellen of aanpassen van een gedragscode.

[Bron: Website Autoriteit Persoonsgegevens]

Concrete voorbeelden wanneer je de FG kunt raadplegen

- bij een (vermeend) datalek, dus een incident waar mogelijk persoonsgegevens zijn gelekt, bijvoorbeeld wanneer een USB-stick, laptop, tablet of telefoon kwijt of gestolen is;
- bij onduidelijkheid over privacy, bijvoorbeeld bij het delen van persoonsgegevens;
- bij het maken van afspraken met derden/externen over het delen van persoonsgegevens.

Contactgegevens

Naam
Postadres
E-mailadres
Telefoonnummer

Wat moet er wanneer door wie gebeuren in aanloop naar 25 mei 2018?

Een taai, maar zeer belangrijk onderwerp in het belang van onze leerlingen en medewerkers. Ook voor jullie dus. Ik reken op jullie medewerking. Samen kunnen we dit prima regelen en onderhouden!

Status	Wat	Voor wanneer	Afstemming
	Protocol Datalekken - communicatie	28-2-2018	ICT-coördinatoren/Veiligheidscoördinatoren
	Privacyreglement – communicatie	28-2-2018	ICT-coördinatoren/Veiligheidscoördinatoren
	Functionaris gegevensbescherming (FG) - communicatie	28-2-2018	Alle medewerkers
	Toestemming gebruik beeldmateriaal leerlingen	28-2-2018	Schoolleiders/Administraties
	Beveiligingsmaatregelen	28-2-2018	ICT-coördinatoren/Alle medewerkers
	Sluit verwerkersovereenkomsten met leveranciers	24-5-2018	ICT-coördinatoren
	ICT-reglement (+ Internet/sociale media/Bruikleen)	24-5-2018	ICT-coördinatoren
	Verwerkingsregister	24-5-2018	Locatieverantwoordelijken
	Bewustwording	24-5-2018	Alle medewerkers

6. Privacyverklaring

In een privacyverklaring moet in ieder geval het volgende staan.
De bedrijfsnaam vermelden, inclusief de adresgegevens van uw bedrijf en een contactadres voor privacygerelateerde vragen.

1. **Doeleinden**
   Met welk doel worden persoonlijke gegevens verwerkt? Denk dan aan zaken als 'vastleggen leerling en persoonsgevens of 'beveiliging en optimalisering van de website' (bijvoorbeeld het vastleggen van IP-adressen).

2. **Gebruik van cookies**
   Als uw site cookies gebruikt (wat vrijwel altijd zo is), dan bent u verplicht uit te leggen wat cookies zijn en wat u daarmee doet. Al is het maar mensen ingelogd laten.

3. **Nieuwsbrieven**
   Als ouders, collega's, partners op nieuwsbrieven geplaatst worden, moeten ze daar expliciet toestemming voor gegeven hebben. Ook moet er in elke nieuwsbrief staan hoe men er weer vanaf komt.

4. **Inzage en correctie**
   Een ouder of collega heeft altijd recht op inzage in zijn gegevens. Daarbij kan hij verzoeken om correctie of verwijdering van zijn persoonsgegevens. Verwijdering mag echter alleen als de gegevens niet meer relevant zijn.

5. **Beveiliging**
   Licht toe welke technische en organisatorische maatregelen u heeft genomen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bij het plaatsen van bestellingen is het bijvoorbeeld wachtwoorden op de database zelf.

Heeft u nog vragen dan kunt u de website raadplegen van de Autoriteit Persoonsgegevens (AP): www.autoriteitpersoonsgegevens.nl

U kunt ook bellen met de Helpdesk van de AVS. Wij helpen u graag met vragen die u heeft.

Helpdesk AVS
Telefoon, fax en e-mailadres
Telefoon: 030-2361010
Fax: 030-2361036
E-mailadres helpdesk@avs.nl

Aanvullende publicatie
Een publicatie over het personeelsdossier en hoe u daar als leidinggevende werk van kunt maken: 'Het personeelsdossier: een goed begin is het halve werk', Jan Stuijver, AVS Utrecht
Bestellen:
www.avs.nl/vereniging/publicatiesenproducten/hetpersoneelsdossiereengoedbeginishethalvewerk