WEGWIJS in de AVG voor Onderwijsinstellingen

Uitgebreide technische brochure…

Doel van dit document

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. De Gegevensbeschermingsautoriteit (GBA) wil met dit document onderwijsinstellingen verder informeren en bijstaan om deze nieuwe wetgeving te implementeren.

Deze brochure is een verdere aanvulling en technische uitwerking van de brochure ‘In 7 stappen naar gegevensbescherming in het onderwijs’ en wil een overzicht geven van de voornaamste rechten en plichten die uit de AVG voortvloeien en waaraan onderwijsinstellingen moeten voldoen. De aangehaalde voorbeelden en toelichtingen bij de AVG hebben als doel om de AVG beter te begrijpen en te implementeren binnen het onderwijsveld maar hebben geen juridische precedentswaarde.

Inhoud

Inleiding

De AVG voert één geharmoniseerde privacywet in die direct van toepassing is binnen heel de Europese Unie. In beginsel is de AVG op dezelfde wijze van toepassing in de publieke en private sector en geldt deze wetgeving voor alle overheden, bedrijven en organisaties die persoonsgegevens verwerken, ook onderwijsinstellingen moeten aan deze wetgeving voldoen. Let op: Op verschillende vlakken kunnen EU-lidstaten specifieke nationale wetgeving aannemen om de AVG verder uit te werken of uitzonderingen te maken. Houd naast de AVG dus ook steeds rekening met specifieke nationale wetgeving. Het gaat hierbij niet uitsluitend om gegevensbeschermingsrecht maar ook om andere rechtsdomeinen, zoals bijv. het arbeidsrecht, onderwijsdecreten… die worden beïnvloed door de AVG.

De nieuwe AVG bouwt verder op de huidige privacywetgeving. De basisconcepten en principes die aan de basis liggen van de verwerking van persoonsgegevens, blijven grotendeels behouden. De AVG voegt hier een aantal nieuwe elementen aan toe om de wetgeving in lijn te brengen met de snelle technologische ontwikkelingen van de afgelopen twintig jaar.
De nieuwe verplichtingen die de AVG met zich meebrengt laten zich samenvatten in drie krachtlijnen: de risico-gebaseerde aanpak, verantwoordingsplicht en transparantie:

• De risico-gebaseerde aanpak betekent dat sommige verplichtingen die voortvloeien uit de AVG variëren in functie van het risico dat verbonden is aan de verwerkingsactiviteit. De AVG creëert dus ruimte om tot een oplossing op maat te komen voor de diverse verwerkingen van persoonsgegevens die in onderwijsinstellingen plaatsvinden.

• De verantwoordingsplicht houdt in dat een verwerkingsverantwoordelijke (het verantwoordelijke schoolbestuur) de naleving van de AVG moet kunnen aantonen. Daarom is het documenteren van keuzes belangrijk zodat een onderwijsinstelling kan verantwoorden waarom het een bepaalde maatregel al dan niet invoerde.

• Transparantie is van cruciaal belang, zowel intern als extern. Intern moet je een duidelijk beeld hebben van alle verwerkingen van persoonsgegevens binnen je onderwijsinstelling en moet je het personeel hierover sensibiliseren. Extern, moet je de personen wiens gegevens je verwerkt (hoofdzakelijk is dit informatie over leerlingen en hun ouders, cursisten, studenten en personeel werkzaam binnen de onderwijsinstelling) helder informeren over hun rechten, de manier waarop zij die rechten kunnen uitoefenen en het hoe en waarom van de verwerkingsactiviteit.

Deze brochure is in de eerste plaats geschreven vanuit het perspectief van de onderwijsinstelling als verwerkingsverantwoordelijke.

Basisbegrippen van de AVG

*"Iedere onderwijsinstelling **verwerkt persoonsgegevens"**.*

Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4.1 AVG). Gegevens die toelaten om een natuurlijke persoon rechtstreeks of onrechtstreeks te identificeren vallen hier ook onder. Wanneer het koppelen van puzzelstukjes van informatie (leeftijd, geslacht, postcode…) kan leiden tot de unieke identificatie van een persoon ('singling out'), is elk puzzelstukje ook een persoonsgegeven.

Anonieme gegevens en gegevens over overleden personen of rechtspersonen zijn geen persoonsgegevens.

Voorbeelden van persoonsgegevens:

- naam, voornaam en contactgegevens van leerlingen en ouders, cursisten, personeel;
- openstaande facturen, betalingsinformatie (voor zover zij betrekking hebben op natuurlijke personen);
- personeelsevaluaties;
- aanwezigheden en ziektebriefjes;
- IP-adres van diegene die je website bezoekt;
- lijst van de personeelsnummers die halftijds werken;
- camerabeelden.

Een algemeen contactmailadres of telefoonnummer van de school – bijv. info@school.be is geen persoonsgegeven;

Je mag niet zomaar alle persoonsgegevens verwerken. Bepaalde persoonsgegevens zijn gevoeliger dan andere. Deze **gevoelige gegevens** zijn persoonsgegevens die een **hoger beschermingsniveau** verdienen omdat hun verwerking significante risico's met zich mee kan brengen. De verwerking van gevoelige gegevens is in beginsel verboden, tenzij je aan één van de uitzonderingsgronden van artikel 9 of 10 van de AVG voldoet. Ook gewone persoonsgegevens waaruit je gevoelige informatie kan afleiden zijn gevoelige gegevens.

Tot de bijzondere categorieën van persoonsgegevens (artikel 9 en 10 AVG) behoren:

- gezondheidsgegevens;
- genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een persoon;
- ras of etnische afkomst;
- seksuele gerichtheid en gedrag;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond.
- gerechtelijke gegevens over strafrechtelijke veroordelingen en strafbare feiten.

Het is duidelijk dat onderwijsinstellingen ook gevoelige gegevens verwerken: oa gezondheidsgegevens van leerlingen en/of personeel en het een uittreksel van het strafregister dat je nodig hebt bij je eerste aanstelling van onderwijspersoneel zijn hier een voorbeeld van.

Verwerken is een breed begrip en bevat iedere bewerking die je doet met persoonsgegevens vanaf het moment dat je de persoonsgegevens gaat opvragen tot en met de vernietiging van deze persoonsgegevens.

Deze bewerkingen kunnen al dan niet geautomatiseerd zijn. De AVG is ook niet te omzeilen door alle persoonsgegevens op papieren dragers te bewaren. Het bijhouden van systematisch geordende bestanden op papier is ook een verwerking in de zin van de AVG.

"Onze school maakt gebruik van het digitaal pakket XYZ. Leerlingen kunnen er op aanmelden, oefeningen maken en de klasleerkrachten kan dit volgen."

De AVG is van toepassing op verschillende **actoren**. Indien de onderwijsinstelling inderdaad beslist om met het digitaal pakket XYZ te werken, en doel en middelen voor deze verwerking bepaalt, wordt het bestuur van deze onderwijsinstelling volgens de AVG als "**verwerkingsverantwoordelijke**" beschouwd. De onderneming die het digitaal pakket XYZ ter beschikking stelt en in opdracht van de onderwijsinstelling persoonsgegevens verwerkt, wordt de "**verwerker**" genoemd. De personen van wie de gegevens verwerkt worden- in dit geval de leerlingen en de klasleerkracht- worden in de AVG aangeduid met de term "**betrokkene**".

Waar moeten onderwijsinstellingen rekening houden als ze persoonsgegevens verwerken?

De AVG is van toepassing op iedere verwerking van persoonsgegevens en maakt hier in principe geen uitzonderingen op voor onderwijsinstellingen. Een onderwijsinstelling moet dus steeds de basisprincipes respecteren die aan de grondslag liggen van elke rechtmatige verwerking van persoonsgegevens. Sterker nog de AVG verplicht verwerkingsverantwoordelijken (ic schoolbesturen) dat ze kunnen **aantonen** dat ze persoonsgegevens volgens de AVG verwerken.

Basisprincipes

Gegevens mogen volgens artikel 5 van de AVG enkel verwerkt worden als ze voldoen aan de basisprincipes die de AVG oplegt. Deze principes zijn rechtmatigheid, doelbinding, transparantie, juistheid, minimale gegevensverwerking, opslagbeperking, integriteit en vertrouwelijkheid (of beveiliging).

Rechtmatigheid

Als de onderwijsinstelling persoonsgegevens gaat verwerken moet ze zich baseren op één van de rechtmatigheden die artikel 6 van de AVG opsomt. De AVG kent zes verschillende rechtmatigheden waarop we ons kunnen baseren indien we persoonsgegevens verwerken.
Deze rechtmatigheden zijn:

1. voldoen aan een wettelijk verplichting;
2. overeenkomst;
3. toestemming;
4. het behartigen van een vitaal belang;
5. vervullen van een taak van openbaar belang of openbaar gezag;
6. voor het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.

Onderwijsinstellingen zullen zich meestal beroepen op de eerste 3 rechtmatigheden.

Enkel *“de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen”* zal door onderwijsinstellingen niet kunnen ingeroepen worden.

De wettelijke verplichting

De AVG bepaalt dat een onderwijsinstelling persoonsgegevens mag verwerken als ze wettelijke verplichtingen moet naleven.

Welke onderwijswetgeving is van toepassing voor onderwijs?

Voor personeel is er het decreet rechtspositie personeelsleden van 27 maart 1991 (decreet voor sommige personeelsleden van het gesubsidieerd onderwijs, en een decreet voor sommige personeelsleden van het gemeenschapsonderwijs) . Daarnaast zijn er nog een heleboel andere wetgevingen waardoor je als onderwijsinstelling persoonsgegevens moet verwerken. Oa regelgeving in functie van sociale zekerheid, preventie en welzijn op het werk en fiscaliteit.

Voor leerlingen: is er afhankelijk van het onderwijsniveau het Decreet basisonderwijs (25/02/1997) en het Besluit van de Vlaamse Regering houdende de codificatie betreffende het secundair onderwijs

(codex secundair 17/12/2010). Daarnaast is er ook het Decreet leerlingenbegeleiding dat vanaf 1 september 2018 van kracht wordt.

De overeenkomst

Een onderwijsinstelling zal bij het ondertekenen van het schoolreglement (=een overeenkomst tussen ouders van de minderjarige leerling, de meerderjarige leerling, cursist en onderwijsinstelling) de persoonsgegevens van deze leerling (en ouders) verwerken die noodzakelijk zijn voor de uitvoering van deze overeenkomst. Deze rechtsgrond dekt ook precontractuele maatregelen voor zover die op verzoek van de betrokkene worden uitgevoerd. Het initiatief moet dus bij de betrokkene liggen. Een voorbeeld van dit laatste is dat leerlingen zich aanmelden bij een centraal aanmeldsysteem. Je moet daar een aantal noodzakelijke gegevens van de leerling doorgeven zodanig dat de onderwijsinstelling je terug kan contacteren voor het effectief inschrijven van de leerling.

Een andere overeenkomst is dat de onderwijsinstelling persoonsgegevens van haar personeel (leerkrachten, ondersteunend en onderhoudspersoneel...) moet verwerken om het loon uit te betalen. Deze verwerking is noodzakelijk om de arbeidsovereenkomst uit te voeren;

De toestemming

Een onderwijsinstelling mag persoonsgegevens verwerken indien de betrokkene hierin toestemt. Wees echter gewaarschuwd: de toestemming is geen mirakeloplossing die samenvalt met het ondertekenen van het schoolreglement! Bovendien mag de betrokkene zijn of haar toestemming altijd en zonder enige motivering intrekken.

Volgens de definitie in artikel 4.11 van de AVG moet iedere toestemming:

• vrij zijn. De betrokkenen moeten een echte keuze hebben zonder dat zij onder druk worden gezet met negatieve gevolgen indien zij hun toestemming niet zouden geven. Een toestemming die onlosmakelijk verbonden is aan de aanvaarding van het school- of instellingsreglement, is niet geldig.

• specifiek zijn. Dit betekent dat de betrokkene voor ieder afzonderlijk doeleinde de keuze moet hebben om al dan niet in te stemmen.

• geïnformeerd zijn. Dit betekent dat de onderwijsinstelling vooraf in begrijpelijke taal de betrokkene moet uitleggen wie, welke persoonsgegevens voor welke doeleinden zal gebruiken. Als onderwijsinstelling moet je de betrokkene er ook altijd wijzen op de mogelijkheid om de toestemming in te trekken. Al deze informatie moet duidelijk te onderscheiden zijn van alle andere informatie.

• berusten op een positieve actie.

Daarnaast moet een geldige toestemming ook voldoen aan een aantal bijkomende vereisten. Zo moet de toestemming ook:

• aantoonbaar zijn. De onderwijsinstelling moet steeds een bewijs bewaren van het verkrijgen van de toestemming.

• even gemakkelijk kunnen worden ingetrokken als ze werd gegeven.

Voorbeeld: In een kleuterschool wil men aan de ouders een adreslijst geven van alle kinderen uit de klas. Je hebt hiervoor dus toestemming van de ouder nodig om hun adres te publiceren op de adressenlijst van de klas. De ouders moeten vrij zijn om hun adres te geven en als ze toestemming geven moeten ze duidelijk geïnformeerd zijn dat deze lijst bijvoorbeeld enkel zal gebruikt worden om

uit te delen in de klas (en dus niet op de website van de school zal staan). Om de toestemming te geven moeten de ouders dan bijvoorbeeld een vakje aankruisen op een formulier.

Op basis van toestemming kan je ook gevoelige gegevens verwerken zoals gezondheidsgegevens.

In het belang van de betrokkene (leerling, cursist…) mag je naar medische info vragen. Zo kan je de leerling beter begeleiden of hulp bieden wanneer er zich problemen voordoen. Weet dat de betrokkene hier zelf vrij op moet kunnen antwoorden een zelf kan aangeven welke informatie de onderwijsinstelling toekomt.

Twee andere gronden waarop een onderwijsinstelling zich ook nog op kan baseren om persoonsgegevens te verwerken.

Het gerechtvaardigde belang van de verwerkingsverantwoordelijke

Een onderwijsinstelling mag persoonsgegevens verwerken als dit noodzakelijk is voor een gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en fundamentele vrijheden van de betrokkene zwaarder doorwegen. Dit betekent dat de onderwijsinstelling in de eerste plaats een gerechtvaardigd belang moet nastreven om vervolgens een afweging te maken met de belangen van de betrokkene. Deze rechtsgrond is dus dynamisch en vraagt voor iedere verwerking een bijzondere en gedocumenteerde rechtvaardiging die de noden van de onderwijsinstelling afweegt aan de impact op de betrokkene.

Het behartigen van een vitaal belang

De AVG geeft aan dat je persoonsgegevens rechtmatig mag verwerken indien dat noodzakelijk is voor de bescherming van een belang dat voor het leven van de betrokkene of dat van een andere natuurlijke persoon essentieel is.

Doelbinding

Artikel 5.2 van de AVG bepaalt dat persoonsgegevens *“voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt”;*

Doelen die gerechtvaardigd zijn in het onderwijs en waarvoor je persoonsgegevens mag verwerken zijn:

- leerlingenadministratie;
- leerlingenbegeleiding;
- personeelsadministratie;
- personeelsbeheer;
- schoolorganisatie;
- communicatie;
- beveiliging;

Gegevens die je verkregen hebt voor een bepaald doel kan u niet zomaar voor een ander doel gebruiken. Als onderwijsinstelling moet je beoordelen of het nieuwe doeleinde verenigbaar is met de doeleinden waarvoor de gegevens oorspronkelijk werden verkregen. Zo ja, dan is de verwerking gesteund door de rechtsgrond op basis waarvan u de gegevens oorspronkelijk verkreeg en verwerkte.

Vanuit de leerlingenadministratie heb je de adressen van de leerlingen. Het is niet omdat je als onderwijsinstelling deze gegevens hebt, dat je deze zomaar kan gebruiken om op een klaslijst te plaatsen en aan alle ouders mee te geven. Deze verwerking is onverenigbaar met de oorspronkelijke, maar wil je dit toch doen moet je toestemming vragen aan de leerling (of de ouders)

Vanuit de wettelijke verplichting moet je afwezigheden van de leerlingen registreren (is dus een administratieve actie). Deze gegevens zal je echter ook gebruiken in de begeleiding van de leerling indien deze te veel dagen afwezig is. Deze verwerkingen zijn verenigbaar met elkaar.

Een school installeert een bewakingscamera met het oog om vandalisme te voorkomen. De beelden van de camera mogen enkel gebruikt worden om vandalisme te voorkomen en niet om de arbeidsprestatie van een leerkracht die toevallig gefilmd wordt, te evalueren.

Juistheid van gegevens

Het is evident dat de persoonsgegevens van leerlingen en personeel juist moeten zijn. Voorzie een procedure waarbij de leerlingen en personeel hun gegevens kunnen (laten) aanpassen indien ze niet juist zijn. Meestal kan dit door melding te doen bij het leerlingen- of personeelssecretariaat. De onderwijsinstelling draagt geen eindverantwoordelijkheid indien een leerling of een andere betrokkene foute informatie verstrekt maar de onderwijsinstelling moet wel proactieve inspanningen leveren om voor de hand liggende fouten te detecteren en recht te zetten.

De betrokkene heeft trouwens ook een recht op inzage (en kopie) van zijn persoonsgegevens. Indien hij merkt dat deze fout zijn of niet meer ter zake dienend zijn, heeft hij ook recht op verbetering van de gegevens.

Opslagbeperking

Een onderwijsinstelling mag persoonsgegevens nooit langer bewaren dan noodzakelijk is om de vooropgestelde doeleinden te bereiken. Zodra deze doeleinden zijn volbracht of wegvallen, moet de onderwijsinstelling de persoonsgegevens wissen. Immers, bij gebrek aan een doeleinde valt de noodzaak tot het bewaren en verwerken weg. Daarom moet de onderwijsinstelling maximale bewaartermijnen vastleggen voor al haar persoonsgegevens. Vanuit de onderwijswetgeving zijn er voor een aantal gegevens al verplichte (minimale) bewaartermijnen vastgelegd.

Zo moet je volgens het Besluit van de Vlaamse regering betreffende de organisatie van het voltijds secundair onderwijs (19/07/2002) bij beslissingen van de klassenraad de processen-verbaal en de notulen van de klassenraad gedurende dertig jaar bewaard worden.

Het is echter niet omdat onderwijsinstellingen de notulen minimaal 30 jaar moeten bewaren, dat ze ook alle bewijsstukken voor gewettigde afwezigheden van die leerling 30 jaar moet bewaren. Voor die administratieve documenten kan de school een bewaartermijn houden van bijvoorbeeld nog 1 schooljaar extra na het aanleveren van het bewijsstuk.

Voer eventueel een bewaarpolitiek in met een gedifferentieerde toegang. Zo is het evident dat de gegevens van een leerlingen die momenteel op school zit beschikbaar en toegankelijk zijn voor de klassenraad die les geeft aan deze leerling. Van zodra een leerling de school verlaat wordt het dossier gearchiveerd, waarbij de gegevens slechts beperkt beschikbaar en toegankelijk zijn (bijvoorbeeld enkel beschikbaar voor secretariaat en directie). Die tweede bewaarmethode is verantwoord gelet op doeleinden van de verdere bewaring, zoals de naleving van de wettelijke voorschriften inzake verjaring of verplichte bewaartermijnen. Wanneer ook die bewaring niet langer nuttig is, moeten de gegevens geanonimiseerd of gewist worden.

Let ook op voor andere wetgevingen: zo zullen persoonsgegevens die zijn opgenomen in de boekhouding pas na zeven jaar gewist worden. Artikel III.88 van het Wetboek Economisch Recht bepaalt immers dat ondernemingen hun boeken moeten bewaren gedurende 7 jaar. Dezelfde redenering gaat op voor documenten, zoals facturen, die de onderwijsinstelling moet bewaren door BTW wetgeving of voor directe belastingen.

Minimale gegevensverwerking

De verzameling en verwerking van persoonsgegevens moeten zich beperken tot wat strikt noodzakelijk is om de vooropgestelde doeleinden te vervullen. De opgevraagde gegevens moeten toereikend zijn. Dit betekent dat je als onderwijsinstelling, voor ieder persoonsgegeven dat je verwerkt, moet kunnen aantonen waarom die informatie noodzakelijk is om het doeleinde te bereiken. Indien je dit niet kan niet aantonen, dan zijn de persoonsgegevens overbodig en moeten ze gewist worden.

In het kader van de leerlingenadministratie is het vrij duidelijk welke gegevens je verwerkt (naam, adres, telefoonnummer…) en met welk doel je dit verwerkt. Voor een aantal andere persoonsgegevens is dit niet altijd relevant waarom je ze verwerkt (bijvoorbeeld beroep van de ouders)

Voor leerlingenbegeleiding is het belangrijk dat je een onderscheid gaat maken tussen de gegevens “need to know” en “nice to know”. Enkel gegevens die behoren tot deze eerste categorie kunnen opgenomen worden in een leerlingendossier.

Transparantie

Zonder noodzakelijke informatie over hun rechten, het hoe en waarom van de verwerkingsactiviteit, kunnen de betrokkenen hun rechten niet uitoefenen. Daarom is transparante communicatie cruciaal. Als verwerkingsverantwoordelijke moet de onderwijsinstelling proactief communiceren zodat betrokkenen precies weten wie de persoonsgegevens verwerkt, waarom en tot wie zij zich kunnen richten bij problemen.

Meestal is dit vrij duidelijk en krijgt de leerling of cursist die informatie bij zijn eerste inschrijving op de onderwijsinstelling. Verdere informatie kan staan in het schoolreglement of op de website van de onderwijsinstelling. Deze communicatie over de verwerking van persoonsgegevens bestaat uit duidelijke en begrijpelijke bewoordingen die zijn afgestemd op het doelpubliek. Bovendien moet de informatie gemakkelijk toegankelijk zijn. Dit betekent dat het voor de betrokkene duidelijk moet zijn waar hij of zij de nodige informatie kan vinden.

Beveiliging

Elke onderwijsinstelling moet passende technische en organisatorische maatregelen nemen om de veiligheid van de persoonsgegevens te garanderen. Deze maatregelen zijn zowel organisatorisch als technisch – een kant-en-klaar beveiligingssoftwarepakket aanschaffen volstaat dus niet altijd! De onderwijsinstelling moet de persoonsgegevens beschermen tegen ongeoorloofde toegang of verwerking, verlies en beschadiging.

De concrete implementatie van deze verplichting kan variëren volgens de risico’s en de omvang van die verwerking, de kost en de technische haalbaarheid. De AVG verlangt dus niet noodzakelijk dat onderwijsinstellingen het neusje van de zalm aanschaffen inzake informatiebeveiliging. Standaard zijn er een aantal organisatorische en technische maatregelen die je zeker kan nemen als onderwijsinstelling.

Organisatorische maatregelen

- Informeer en sensibiliseer iedereen! Tijdens bewustmakingscampagnes zorg je ervoor dat iedereen (directeur, administratief- en onderwijzend personeel, opvoeders, ouders, leerlingen en cursisten, poetsteam, de conciërge, vrijwilligers…) op de hoogte is van de vernieuwde wetgeving en het correct omgaat met persoonsgegevens.
- Duidt een 'aanspreekpunt informatieveiligheid' aan die het bestuur en directie meehelpt met het uitstippelen van een informatieveiligheids- en privacybeleid.
- Zorg voor gedifferentieerde toegang tot leerlingengegevens: Directie heeft toegang tot alle leerlingengegevens, de zorgcoördinator zal ook toegang hebben tot de zorggegevens van de leerlingen die door hem begeleid worden, leerkrachten die lesgeven aan de leerling hebben toegang tot de informatie die relevant zijn bij het lesgeven maar daarom niet tot alle zorggegevens. Leerkrachten die geen lesgeven aan de leerling kunnen in principe enkel naam, klas en foto van de leerling zien maar geen andere informatie.

Technische maatregelen

- gebruik een virusscanner en update deze systematisch en tijdig;
- maak systematisch een back-up om je gegevens te beschermen tegen verlies;
- update systematisch en automatisch het besturingssysteem en alle softwareprogramma's;
- installeer een "firewall"(kan zowel hard- als softwarematig);
- voer een toegangssysteem in met een uniek identificatiemiddel (login) voor elke gebruiker met een authenticatiemechanisme. Bij toegang tot gevoelige gegevens kan het aangeraden zijn om een tweetrapsverificatie te gebruiken.

Verwerkersovereenkomst

Onderwijsinstellingen doen vaak beroep op externe leveranciers om bepaalde persoonsgegevens voor hen te verwerken. Denken we maar aan de leerlingenadministratie en leerlingenvolgsystemen die we gebruiken, systemen die het toelaten dat leerlingen online oefeningen invullen en de leerkracht dit proces kan volgen. Maar het gaat ook de systemen om te communiceren of een online leerplatform. Vaak staan deze programma's in de cloud en ook daar moet rekening worden gehouden met oa de veiligheid van de uitgewisselde persoonsgegevens.
Deze leveranciers van diensten en producten worden in de AVG "verwerkers" genoemd.

Onderwijsinstellingen mogen uitsluitend beroep doen op verwerkers die afdoende garanties bieden opdat de verwerking aan de vereisten van de AVG zou voldoen en de rechten van de betrokkene gewaarborgd blijven. De garanties moeten onder meer betrekking te hebben op de beveiliging en het toepassen van passende technische en organisatorische maatregelen.

Wanneer de verwerking van persoonsgegevens aan een verwerker wordt toevertrouwd, moeten beide partijen een "verwerkersovereenkomst" afsluiten. Dit contract moet uitdrukkelijk bepalen dat de dienstverlener de persoonsgegevens uitsluitend op basis van de schriftelijke instructies van de onderwijsinstelling mag verwerken.

Onderwijsverstrekkers en Leveranciers van producten en diensten voor onderwijs hebben samen een 'model van verwerkersovereenkomst' opgesteld waarvan onderwijsinstellingen en verwerkers gebruik van kunnen maken. Zo maken Onderwijsinstellingen en hun verschillende verwerkers gebruik van dezelfde standaardcontractbepalingen.

Onderwijsinstellingen kunnen op www.privacyinonderwijs.be nakijken of welke leverancier gebruik maken van deze standaard modelovereenkomst.

De overeenkomst moet zeker de volgende elementen bevatten:

- onderwerp en duur van de overeenkomst, de doeleinden en aard van de verwerking, het soort gegevens, de categorieën van betrokkenen en de rechten en verplichtingen van beide partijen;
- de verwerker garandeert dat hij de persoonsgegevens enkel op basis van de schriftelijke instructies van de onderwijsinstelling zal verwerken en niet voor enige andere doeleinde zal aanwenden (behoudens een uitdrukkelijke wettelijke verplichting);
- de verwerker garandeert om passende technische en organisatorische maatregelen te zullen nemen om een op het risico afgestemd beveiligingsniveau te waarborgen;
- de verwerker belooft geen andere verwerker (onderaannemer) in dienst te nemen zonder voorafgaande schriftelijke toestemming van de onderwijsinstelling. Als de verwerker toch een onderaannemer inschakelt moet de verwerker alle verplichtingen opleggen aan de onderaannemer die voortvloeien uit de eerste verwerkingsovereenkomst tussen de onderwijsinstelling en de eerste verwerker;
- de verwerker waarborgt dat personen die door hem gemachtigd zijn tot het verwerken van de persoonsgegevens(bijv. technici belast met het beheer van de dienst) zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- de verwerker gaat akkoord om de onderwijsinstelling voor zover mogelijk bijstand te verlenen bij het vervullen van diens plicht om aan de verzoeken om uitoefening van de rechten van de betrokkenen te beantwoorden;
- de verwerker verklaart zich bereid om, waar passend, aan de onderwijsinstelling bijstand te verlenen bij het doen nakomen van haar verplichtingen wat betreft beveiliging, melding en/of mededeling van een inbreuk in verband met persoonsgegevens of een Gegevensbeschermingeffectbeoordeling (GEB);
- de gegevens worden niet buiten de Europese Economische Ruimte doorgegeven naar bestemmingen die geen adequaat beschermingsniveau bieden of zonder bijkomende passende waarborgen die eerst met de onderwijsinstelling zullen worden afgesproken;
- de verwerker waarborgt dat na afloop van de dienstverlening alle persoonsgegevens veilig gewist of aan de onderwijsinstelling terugbezorgd zullen worden, en bestaande kopieën verwijderd zullen worden;
- de verwerker gaat akkoord om aan de onderwijsinstelling alle informatie ter beschikking te stellen die nodig is om de nakoming van diens verplichtingen aan te tonen en audits, waaronder inspecties, door de onderwijsinstelling of een door de onderwijsinstelling gemachtigde controleur mogelijk te maken en eraan bij te dragen.

Vanaf schooljaar 2018-2019 zal je dus als onderwijsinstelling alle contracten opnieuw moeten bekijken en deze verwerkersovereenkomst toevoegen bij bestaande contracten.

Waar zijn gegevens gelokaliseerd?

Onderwijsinstellingen doen vaak beroep op buitenlandse verwerkers. Zo kan het zijn dat je gebruik maakt van een app (waar je persoonsgegevens mee uitwisselt, bijvoorbeeld de naam en email van de studenten) waarvan de servers zich bevinden in het buitenland. Binnen de Europese Economische Ruimte mogen volgens de AVG alle persoonsgegevens vrij circuleren. Als de gegevensverwerking plaatsvindt in bijvoorbeeld Nederland, dan hoeft je geen extra waarborgen te eisen. Vindt de gegevensverwerking echter plaats buiten de Europese Economische Ruimte dan mag de doorgifte van de persoonsgegevens slechts plaatsvinden onder strikte voorwaarden.

De doorgifte naar een "derde land" buiten de Europese Economische Ruimte is toegelaten:

- wanneer deze bestemming door de Europese Commissie erkend is als een bestemming met een gelijkaardig beschermingsniveau (een adequaatheidsbesluit). Op dit ogenblik (mei 2018) gaat het om volgende landen: Andorra, Argentinië, Canada (voor de delen die vallen onder Canadian Personal Information Protection and Electronic Documents Act), Faeröer Eilanden, Guernsey, Israël, Het Eiland Man, Jersey, Nieuw Zeeland, Uruguay, VS (onder de vorm van het EU-U.S. Privacy Shield) en Zwitserland.
- wanneer de verwerker in de overeenkomst bijkomende passende waarborgen biedt om een gelijkaardig beschermingsniveau op contractuele wijze tot stand te brengen. Dit kan door modelbepalingen toe te voegen die de Europese Commissie of de GBA heeft goedgekeurd;

Deze mechanismen garanderen de veiligheid van de persoonsgegevens en zorgen ervoor dat betrokkenen hun rechten kunnen uitoefenen, ook al vindt de verwerking plaats in een land met andere soort privacywetgeving.

Het is vooral van belang dat de onderwijsinstelling op de hoogte is waar haar gegevens naartoe gaan (of verwerkt worden) en weet dat een doorgifte buiten de Europese Unie extra waarborgen vereist.

Aanspreekpunt informatieveiligheid

De AVG verplicht bepaalde organisaties om een functionaris voor gegevensbescherming (DPO, data protection officer) aan te stellen.

Een DPO zorgt er mee voor dat een organisatie voldoet aan de actuele privacywet- en regelgeving. De onderwijsverstrekkers zullen namens de scholen die tot hun net of koepel behoren een DPO aanduiden.

Als onderwijsinstelling duid je een **aanspreekpunt informatieveiligheid** aan. Het aanspreekpunt treedt op als contactpersoon voor de DPO van de onderwijsverstrekkers. Scholen kunnen dus te allen tijde terecht bij de DPO van hun onderwijsnet (Voor onderwijsinstellingen van het gemeentelijk/provinciaal onderwijs neemt de informatieveiligheidsconsulent of DPO van de gemeente/provincie deze taak op zich).

Het aanspreekpunt kent idealiter de aard van de data waarover een onderwijsinstelling beschikt en de datastromen binnen de onderwijsinstelling.

Het aanspreekpunt helpt mee aan het bewustmakingsproces over hoe de onderwijsinstelling veilig moet omgaan met persoonsgegevens en helpt mee om samen met directie en bestuur het informatieveiligheids- en privacybeleid in de instelling toe te passen. Daarnaast zal hij/zij het eerste

aanspreekpunt zijn bij gegevenslekken en de nodige documenten kunnen opstellen om aan te tonen dat de onderwijsinstelling aan de AVG voldoet.

Verder is het belangrijk te weten dat het aanspreekpunt van de onderwijsinstelling niet de eindverantwoordelijkheid draagt i.v.m. het naleven van de AVG. De eindverantwoordelijkheid voor het naleven van de AVG ligt bij het bestuur van de onderwijsinstelling.

Let op: Indien de onderwijsaanstelling zelf een functionaris voor gegevensbescherming aanduidt, moet u alle regels naleven van de AVG over de taken en de positie van de functionaris. Let dus op met een lichtzinnig gebruik van de functietitel DPO of functionaris! Gebruik deze titel alleen als het gaat om een échte functionaris voor gegevensbescherming in de zin van de AVG.

Register van verwerkingsactiviteiten

Onderwijsinstellingen zijn verplicht om een register van verwerkingsactiviteiten op te stellen en moeten dit desgevraagd kunnen voorleggen aan de gegevensbeschermingsautoriteit. Het bevat een overzicht van alle verwerkingsactiviteiten van persoonsgegevens die onder de verantwoordelijkheid van de onderwijsinstelling plaatsvinden.

Het register bevat een overzicht van de verwerkingsdoeleinden en niet van de persoonsgegevens zelf.

Het moet op zijn minst de volgende informatie vermelden:

- Wie: naam en contactinformatie van de verwerkingsverantwoordelijke en functionaris (DPO);
- Waarom: per verwerking vermeldt het register in detail de verwerkingsdoeleinden;
- Wat: per verwerking vermeldt het register de soorten van persoonsgegevens en betrokkenen;
- Waar: het register vermeldt alle categorieën ontvangers van de persoonsgegevens, de doorgiftes naar een land buiten de Europese Unie en de eventuele passende waarborgen voor zo een doorgifte;
- Bewaartermijn: indien mogelijk, de termijn waarbinnen men persoonsgegevens moet wissen;
- Beveiliging: indien mogelijk, een algemene beschrijving van de beveiligingsmaatregelen.

Voor het onderwijs is er een sjabloon ontwikkeld dat onderwijsinstellingen kunnen gebruiken en waar de meeste verwerkingsdoeleinden die in onderwijs verricht worden vermeld staan. Onderwijsinstellingen hoeven per verwerking enkel nog aan te geven welke verwerkers ze inschakelen. Indien ze nog andere verwerkingen uitvoeren moeten ze dit uiteraard zelf verder aanvullen in dit modelregister.

Rechten van de betrokkene

Naast het opleggen van bepaalde verplichtingen die hierboven werden besproken, voorziet de AVG in rechten die iedere betrokkene kan uitoefenen. De betrokkene oefent deze rechten uit ten aanzien van de verwerkingsverantwoordelijke.

De verwerker, moet de verwerkingsverantwoordelijke bijstaan om de uitoefening van deze rechten mogelijk te maken.

Het gaat in het bijzonder om:

1. het recht op informatie/de plicht om te informeren
2. het recht van inzage
3. het recht op verbetering
4. het recht op gegevenswissing
5. het recht op beperking van de gegevensverwerking
6. het recht van bezwaar
7. het recht op gegevensoverdraagbaarheid
8. het recht om niet aan geautomatiseerde individuele besluitvorming onderworpen te worden

Let op: sommige rechten gelden niet voor elke rechtmatigheid! Bij de bespreking van ieder recht lichten we steeds het verband tussen de rechtsgrond en het recht verder toe.

Leerlingen jonger dan 13 jaar mogen volgens de AVG zelf nog geen beslissingen nemen over privacygerelateerde onderwerpen en daarom zullen de ouders of personen die het ouderlijk gezag over deze jongere uitoefenen de rechten van de betrokkene uitoefenen. Ouders oefenen nog wel steeds het ouderlijk gezag uit totdat de leerling de leeftijd van 18 jaar bereik heeft. Tot die leeftijd moeten ouders ook nog steeds het schoolreglement ondertekenen.

Het is dus niet zo dat de leerling vanaf 13 jaar, op basis van de AVG, zou kunnen weigeren dat zijn rapport naar de ouders of voogd doorgegeven wordt. Als de onderwijsinstelling, in het kader van individuele leerlingenbegeleiding, van een leerling vertrouwelijke informatie verwerkt en de leerling wil niet dat de ouders of voogd dit vernemen, moet je dit recht wel respecteren en de informatie niet aan hen doorgeven. Denk er bij het verstrekken van informatie altijd aan het principe dat je deze informatie geeft **in het belang van de betrokkene**.

In de uitoefening van de rechten van de betrokkenen speelt transparantie ook een sleutelrol. Zo moet de verwerkingsverantwoordelijke:

- de betrokkene duidelijk informeren over bestaan van deze rechten;
- in begrijpelijke en heldere taal communiceren als een betrokkene rechten uitoefent.

De onderwijsinstelling mag geen betaling vragen voor het uitoefenen van deze rechten.

Enkel indien het verzoek van de betrokkene ongegrond of buitensporig is, mag wel een vergoeding aangerekend worden. (Waar je wel moet kunnen aantonen dat het verzoek duidelijk ongegrond of buitensporig is.) De vergoeding moet afgestemd zijn op de administratieve kost voor de onderwijsinstelling om gevolg te geven aan het verzoek.

Wanneer de betrokkene één van haar rechten uitoefent, moet de onderwijsinstelling hier binnen één maand op reageren. Gaat het om een complex verzoek, dan kan de onderwijsinstelling de termijn met twee maanden verlengen nadat de betrokkene hier binnen één maand van op de hoogte is gebracht. Als de onderwijsinstelling kan aantonen dat het verzoek duidelijk ongegrond of

buitensporig is, mag zij het verzoek negeren. Zo kan het zijn dat bijvoorbeeld (de ouders van) een leerling wekelijks de onderwijsinstelling een verzoekt stuurt om zijn recht tot inzage uit te oefenen. Na antwoord gegeven te hebben op het eerste verzoek, kan de onderwijsinstelling deze bijkomende verzoeken negeren of een vergoeding aanrekenen die overeenstemt met de administratieve kost van het bezorgen van een antwoord.

Wanneer de onderwijsinstelling geen gevolg geeft aan het concrete verzoek van de betrokkene, moet zij één maand na ontvangst van het verzoek meedelen waarom het verzoek zonder gevolg blijft (bijv. waarom ze een gegevenswissing niet doorvoert).

Bovendien moet de onderwijsinstelling betrokkene wijzen op de mogelijkheid om klacht neer te leggen bij de GBA of beroep in te stellen bij een rechter.

Het recht op informatie/de plicht om te informeren

Elke betrokkene heeft **recht** op bepaalde informatie wanneer de onderwijsinstelling gegevens verwerkt die op hem of haar betrekking hebben.

Maar als onderwijsinstelling heb je ook de **plicht** om de betrokkene te informeren.

Welke informatie?

De AVG maakt een onderscheid tussen de rechtstreekse inzameling van persoonsgegevens bij de betrokkene zelf (rechtstreekse inzameling – artikel 13 AVG) en de situatie waarbij de persoonsgegevens niet bij de betrokkene zelf maar uit een andere bron zijn verkregen (onrechtstreekse inzameling – artikel 14 AVG). Onrechtstreekse inzameling is bijvoorbeeld doordat een leerling van school verandert en de oude school persoonsgegevens doorgeeft aan de nieuwe school.

Zowel bij de rechtstreekse als onrechtstreekse inzameling van persoonsgegevens moet een onderwijsinstelling als verwerkingsverantwoordelijke bepaalde informatie verstrekken aan de betrokkene. Hier overlopen we de basisinformatie die je bij rechtstreekse dan wel onrechtstreekse inzameling aan de betrokkene **moet** meedelen:

Informatie	Rechtstreeks	Onrechtstreeks
doeleinden en rechtsgrond van de verwerking	X	X
identiteit en contactgegevens van de verwerkings-verantwoordelijke	X	X
Contactgegevens van de Data Protection Officer	X	X
de ontvangers of categorieën ontvangers van de gegevens	X	X
bij doorgifte buiten de EU: het bestaan van een adequaatheids-besluit of passende waarborgen en hoe u hiervan een kopie kan krijgen	X	X
uitleg over het gerechtvaardigde belang van de verwerkingsverantwoordelijke als de verwerking steunt op deze rechtsgrond	X	
de categorieën van verwerkte gegevens		X

Op de inschrijvingsfiche is het dus belangrijk dat je naast de contactgegevens van de school ook die van het schoolbestuur gaat vermelden (indien verschillend). Daarnaast kan je ook de naam en contactgegevens van het aanspreekpunt informatieveiligheid binnen de school en moet je het contactadres van de DPO vermelden. De gegevens worden verzameld in het kader van leerlingenadministratie en leerlingenbegeleiding. Indien je medische informatie van de leerling

opvraagt, weet dat de leerling deze informatie altijd vrij moet kunnen geven. Vermeld bij het deel van de inschrijvingsfiche waar de leerling medische info kan noteren, deze informatie niet verplicht moet geven worden. Verwerk hier enkel informatie in het belang van de leerling.

Bovendien schrijft de AVG voor dat een onderwijsinstelling de onderstaande informatie moet verstrekken om een behoorlijke en transparante verwerking te waarborgen.

Informatie	Rechtstreeks	Onrechtstreeks
de bewaartermijn, of indien onmogelijk, de criteria om die termijn te bepalen	X	X
het recht op toegang, uitwissing, verbetering, beperking, bezwaar en overdraagbaarheid	X	X
het recht om een klacht in te dienen bij een toezichthoudende autoriteit	X	X
steunt de verwerking op toestemming: het recht om de toestemming te allen tijde in te trekken	X	X
Bij het bestaan van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica hiervan en de verwachte gevolgen van die verwerking voor de betrokkene	X	X
uitleg over het gerechtvaardigde belang van de verwerkingsverantwoordelijke als de verwerking steunt op deze rechtsgrond		X
de bron van de gegevens		X
of de betrokkene verplicht is de persoonsgegevens te verstrekken (door de wet of een contract) en wat de gevolgen zijn bij een weigering om die gegevens te verstrekken	X	

De verwerkingsverantwoordelijke moet de bovenstaande informatie uit deze tweede tabel opnieuw meedelen bij een verdere verwerking voor een nieuw maar verenigbaar doeleinde dat afwijkt van het oorspronkelijk doeleinde. In dit geval moet de onderwijsinstelling de betrokkene ook informatie geven over de analyse die aantoont dat het nieuwe en oude doeleinde verenigbaar zijn

Wanneer moet de informatie worden verstrekt?

Bij de rechtstreekse inzameling moet de onderwijsinstelling de informatie meedelen op het moment van inzameling van de persoonsgegevens, meestal is dat bij de inschrijving van de leerling.

Bij de onrechtstreekse inzameling van persoonsgegevens moet de onderwijsinstelling de informatie geven ten laatste binnen één maand na de initiële verkrijging van de persoonsgegevens. Die maximale termijn van één maand wordt ingekort – nooit verlengd – :

- indien de persoonsgegevens worden gebruikt voor communicatie met de betrokkene. De onderwijsinstelling informeert dan uiterlijk op het moment van eerste contact met de betrokkene;
- indien de gegevens aan een andere ontvanger worden doorgegeven. De onderwijsinstelling informeert dan uiterlijk op het tijdstip van de doorgifte van de persoonsgegevens.

Voor de duidelijkheid: als de doorgifte of het eerste contact later plaatsvindt dan één maand na de initiële verkrijging van de persoonsgegevens, moet de onderwijsinstelling de informatie gewoon binnen de maand na de initiële verkrijging meedelen. Bij elke latere wijziging aan de verwerking (bijv. nieuw ontvangers, verenigbaar doeleinde, doorgifte buiten de EU, etc.…) moet de onderwijsinstelling

de betrokkene hier ruim op voorhand over informeren zodat deze een redelijk termijn heeft om de impact ervan te appreciëren en zijn/haar rechten uit te oefenen. Indien

Wanneer moet de onderwijsinstelling geen informatie meedelen?

De onderwijsinstelling moet deze informatie NIET meedelen indien de betrokkene deze al eerder ontving. Bij inschrijving van de leerling heb je deze gegevens normaliter al gegeven, je hoeft ze dus bij elke nieuwe bevraging niet nogmaals te communiceren.

Bij onrechtstreekse inzameling van persoonsgegevens gelden bijkomende uitzonderingen. De mededeling van informatie is dan niet noodzakelijk indien:

- het verstrekken van die informatie onmogelijk is of onevenredig veel inspanning vergt. De lat voor deze uitzondering ligt echter zeer hoog waardoor een verwerkingsverantwoordelijke slechts uitzonderlijk deze situaties kan inroepen; of
- het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven door de wet;
    - de wet verplicht de fiscus om bepaalde informatie over een werknemer op te vragen bij de werkgever. De fiscus hoeft de werknemer zelf niet te informeren. De werkgever zal in het kader van zijn plicht om te informeren de werknemer wel op de hoogte stellen van het feit dat de fiscus één van de ontvangers is van de persoons-gegevens.
- de persoonsgegevens vertrouwelijk moeten blijven door een wettelijk beroepsgeheim.
    - De onderwijsinstelling geeft informatie door aan het CLB. Het CLB moet de leerling hiervan niet op de hoogte brengen.

Hoe moet de informatie worden verstrekt?

We raden aan om informatie te verstrekken in lagen. Op die manier vermijdt u dat een teveel aan informatie de transparantie schaadt en de betrokkene verdrinkt in een overvloed van informatie. De gelaagde verstrekking van de informatie verzoent de vereiste van beknoptheid met de vereiste om alle noodzakelijke informatie te verstrekken. Dit vereenvoudigt niet alleen de taak van de verwerkingsverantwoordelijke, maar stelt ook de betrokkene in staat om snel en efficiënt de kerninformatie op te nemen.

Om te waken over een eerlijke informatieverstrekking zou de voorstelling van deze informatie er als volgt uit kunnen zien:

• een eerste laag met basisinformatie die je op het inschrijvingsformulier opneemt maar ook in het schoolreglement

- WAT?: de noodzakelijke basisinformatie die de betrokkene nodig heeft om de impact en draagwijdte van de verwerking in te schatten (bijvoorbeeld: de identiteit van de verwerkingsverantwoordelijke, de doeleinden, de categorieën ontvangers, de bron van de gegevens…).
- HOE?: tijdens het verzamelen van de persoonsgegevens geeft u op het inschrijvingsformulier deze informatie aan.

• een tweede laag met gedetailleerde, bijkomende informatie.

- WAT?: dit deel presenteert op een begrijpelijke en overzichtelijke manier de overige informatie die de onderwijsinstelling krachtens artikel 13 en artikel 14 AVG moet meedelen.
- HOE?: de bijkomende informatie kan op verschillende manieren worden verstrekt bijv. via hyperlinks op te nemen in het schoolreglement waar de betrokkene deze verder informatie

kan vinden. De bijkomende informatie moet een balans vinden tussen beknoptheid en precisie. De informatie moet gestructureerd zijn zodat deze makkelijk leesbaar is.

Het recht van inzage

Het recht op inzage stelt de betrokkene in staat om de rechtmatigheid van elke verwerkingsactiviteit te controleren. Het recht op inzage is drieledig:

1) De betrokkene heeft het recht om te weten of de onderwijsinstelling al dan niet zijn of haar persoonsgegevens nog verwerkt. Normaliter blijft de onderwijsinstelling nog steeds persoonsgegevens van oud-leerlingen en personeel verwerken. Je doet dit meestal omdat er op deze gegevens een minimale bewaartermijn staan.

2) Zo ja, heeft de betrokkene het recht om de onderstaande informatie te verkrijgen:

- de doeleinden van de verwerking;
- de categorieën van persoonsgegevens;
- de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- de bewaartermijn van de persoonsgegevens of de criteria om die termijn te bepalen;
- het recht op de gegevenswissing, verbetering van persoonsgegevens en het recht om de verwerking te beperken of hiertegen bezwaar te maken;
- het recht een klacht in te dienen bij een toezichthoudende autoriteit;
- de bron van de gegevens (bij onrechtstreekse inzameling);
- bij doorgifte buiten de EU: de passende waarborgen ;
- het bestaan van geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica hiervan en de verwachte gevolgen van die verwerking voor de betrokkene.

Hiervoor kan je verwijzen naar bijvoorbeeld je website waar deze gegevens onder de vorm van een privacybeleid beschikbaar zijn.

3) De betrokkene heeft het recht om een gratis kopie te krijgen van zijn of haar persoonsgegevens die de onderwijsinstelling verwerkt. Vraagt de betrokkene om extra kopieën, dan mag de onderwijsinstelling een redelijke vergoeding aanrekenen die niet hoger is dan de administratieve kost hiervan. Wanneer de betrokkene een verzoek elektronisch indient, deelt de onderwijsinstelling de informatie mee in een gangbaar elektronische formaat, tenzij de betrokkene vraagt om een kopie op een andere fysieke drager (bijvoorbeeld papier). Alvorens de kopie te versturen, moet de onderwijsinstelling nagaan of deze mededeling geen afbreuk doet aan de rechten en vrijheden van andere betrokkenen (bijv. indien er informatie over meer dan één persoon in eenzelfde bestand wordt verwerkt).

- een personeelslid van de onderwijsinstelling vraagt toegang tot zijn of haar personeelsdossier en wil hiervan een gratis kopie krijgen. De onderwijsinstelling bezorgt een kopie van het personeelsdossier samen met een (verwijzing naar de) toelichting van de verwerking (zie punt 2) hierboven).
- Vanuit dit recht heeft een leerling ook recht op inzage in zijn individueel leerlingendossier.

Het recht op verbetering

De betrokkene heeft het recht om onjuiste gegevens te verbeteren of onvolledige gegevens aan te vullen, onder meer door een aanvullende verklaring toe te voegen. Als de onderwijsinstelling deze persoonsgegevens heeft doorgegeven aan derde partijen, moet zij deze op de hoogte brengen van de aangebrachte verbetering, tenzij dit onmogelijk is of onevenredig veel inspanning vergt.

- Als een cursist meldt aan de onderwijsinstelling dat hij/zij is verhuisd. De onderwijsinstelling moet het adres in haar cursistenbestand aanpassen.
- De leerling heeft het recht om zijn dossier aan te vullen en zijn versie van de feiten te geven. Deze informatie moet ook in het dossier opgenomen worden.

Het recht op gegevenswissing

Een betrokkene kan eisen dat de onderwijsinstelling persoonsgegevens wist waarvoor geen gegronde reden meer bestaat om deze te verwerken. Het recht om gegevens te wissen is niet absoluut. De betrokkene kan dit recht slechts in de onderstaande gevallen uitoefenen:

- de persoonsgegevens zijn niet langer noodzakelijk om het nagestreefde doel te vervullen;
- de onderwijsinstelling verwerkt de persoonsgegevens onrechtmatig;
- de onderwijsinstelling moet de persoonsgegevens wissen door toedoen van een wettelijke verplichting;
- na een succesvolle uitoefening van het recht van bezwaar (zie 'Recht van bezwaar');
- minderjarigen die toestemming gaven om een online dienst te gebruiken kunnen steeds vragen om die persoonsgegevens te wissen (ongeacht hun huidige leeftijd).

Gaf u de gewiste gegevens voordien door aan iemand anders? Dan moet de onderwijsinstelling deze ontvangers op de hoogte brengen van de gegevenswissing, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.

De onderwijsinstelling mag ook weigeren om de persoonsgegevens te wissen wanneer de verwerking noodzakelijk is voor onder andere:

- de uitoefening van het recht op vrijheid van meningsuiting en informatie;
- de instelling, uitoefening en de onderbouwing van een vordering in rechte;
- de vervulling van een wettelijke plicht of een taak van algemeen belang die op de onderwijsinstelling rust;
- onderzoek, statistiek, volksgezondheid, archivering in het algemeen belang – onder specifieke voorwaarden.

Onderwijsinstellingen zullen meestal de gegevens bijhouden en niet kunnen wissen omdat er een wettelijke verplichting op hen rust. Zo kan bijvoorbeeld een net ontslagen personeelslid vragen om al zijn/haar persoonsgegevens te wissen uit het personeelsdossier. De onderwijsinstelling is echter wettelijk verplicht om een aantal sociale documenten (personeelsregister, individuele rekening, kopie van loonstaten enz.) gedurende vijf jaar te bewaren. Voor deze documenten moet de onderwijsinstelling het verzoek om gegevenswissing weigeren.

Het recht op beperking van gegevensverwerking

Artikel 18 van de AVG bepaalt dat in bepaalde omstandigheden de betrokkene een "beperking" van de gegevensverwerking kan eisen. De beperking bevriest de gegevensverwerking. Bijgevolg mag de onderwijsinstelling de persoonsgegevens alleen nog maar opslaan en moet zij alle andere verwerkingsactiviteiten stopzetten.

De betrokkene heeft het recht om de beperking van de gegevensverwerking te verkrijgen wanneer:

- de betrokkene de juistheid van de persoonsgegevens betwist, gedurende een periode die de onderwijsinstelling in staat stelt de juistheid van de persoonsgegevens te controleren;
- de verwerking onrechtmatig is, kan de betrokkene in de plaats van de wissing van de gegevens, verzoeken om het gebruik van de persoonsgegevens te beperken;
- de onderwijsinstelling de persoonsgegevens niet meer nodig heeft, maar de betrokkene wel voor de uitoefening van een rechtsvordering;
- de betrokkene zijn recht van bezwaar uitoefent. De beperking geldt in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de onderwijsinstelling zwaarder wegen dan die van de betrokkene.

Indien de betrokkene het recht op beperking succesvol uitoefent, mag de onderwijsinstelling de gegevens oa nog gebruiken met de toestemming van de betrokkene of voor de instelling van een rechtsvordering.

Het recht van bezwaar

Iedere betrokkene kan bezwaar maken tegen de verwerking van persoonsgegevens die op hem of haar betrekking hebben “vanwege met zijn specifieke situatie verband houdende redenen”. Het recht van bezwaar kan uitsluitend uitgeoefend worden wanneer de verwerking steunt op één van de volgende rechtsgronden:

- het gerechtvaardigde belang van de onderwijsinstelling of een derde;
- de vervulling van een taak van algemeen belang of het openbaar gezag.

In andere gevallen kan de betrokkene geen bezwaar maken omdat voor de overige rechtsgronden alternatieven bestaan om hetzelfde doel bereiken: bij toestemming kan de betrokkene deze intrekken; tegen verwerking die de wet oplegt kan de betrokkene geen bezwaar maken.

De uitoefening van het recht op bezwaar dwingt de onderwijsinstelling tot een belangenafweging. De onderwijsinstelling staakt iedere verwerking van de persoonsgegevens tenzij zij dwingende gronden kan opwerpen die zwaarder wegen dan de rechten en vrijheden van de betrokkene (bijv. een vordering in rechte). De onderwijsinstelling moet deze gronden documenteren en meedelen aan betrokkene.

Op deze belangenafweging bestaat een belangrijke uitzondering in het voordeel van de betrokkene: bij **direct marketing** heeft de betrokkene altijd het recht om zonder enige motivering bezwaar aan te tekenen. Dit bezwaar leidt dan automatisch tot de stopzetting van de verwerking voor dit doeleinde. De onderwijsinstelling moet de mogelijkheid tot het uitoefenen van het recht op bezwaar, duidelijk en apart van ander informatie onder de aandacht van de betrokkene brengen.

Onderwijsinstellingen zullen waarschijnlijk niet zo vaak met deze laatste 2 rechten van de betrokkene te maken krijgen. Enkel indien ze op basis van een ‘gerechtvaardigd belang’ persoonsgegevens verwerken en de betrokkenen maakt bezwaar tegen deze verwerking, dan zal het het recht op beperking gelden.

Een mogelijks voorbeeld van ‘bezwaar’ en ‘recht op beperking’ zou in de volgende situatie kunnen optreden: éénzelfde schoolbestuur heeft zowel een basisschool als een secundaire school. Indien de secundaire school de leerlingen uit het zesde leerjaar een informatiebrochure zou toesturen naar het thuisadres van de leerlingen, zou de lagere school vooraf de leerlingen moeten informeren dat zij die dit niet wensen bezwaar tegen kunnen maken omdat hun persoonsgegevens gebruikt worden voor doeleinden van direct marketing. De leerlingen die bezwaar maken ontvangen geen brochure van de secundaire school op hun thuisadres.

Het recht op gegevensoverdraagbaarheid

Het recht op gegevensoverdraagbaarheid stelt de betrokkene in staat om zijn/haar persoonsgegevens te verkrijgen en te hergebruiken voor andere diensten. Op een gebruiksvriendelijke manier kan de betrokkene persoonsgegevens verplaatsen van de ene IT-omgeving naar een andere.

Het recht op gegevensoverdraagbaarheid kan alleen worden uitgeoefend indien aan **drie voorwaarden gelijktijdig** is voldaan:

- ✓ de verwerking vindt plaats op basis van de toestemming of een overeenkomst;
- ✓ het gaat om een geautomatiseerde verwerking (geen papieren documenten); en
- ✓ de betrokkene heeft de gegevens zelf verstrekt.

De betrokkene krijgt het recht om zijn persoonsgegevens:

- te verkrijgen in een gestructureerde, gangbare en machinaal leesbare vorm. De vorm moet de betrokkene in staat stellen om de persoonsgegevens te hergebruiken voor een andere dienst;
    - XML, JSON en CSV zijn courante formats die voldoen aan dit criterium. Ook metadata moet worden doorgestuurd zodat de data kan functioneren op een ander platform. Een Pdf-formaat volstaat niet.
- rechtstreeks te laten overdragen aan een andere verwerkingsverantwoordelijke. De onderwijsinstelling moet dit alleen doen in zoverre een dergelijke rechtstreekse overdracht technisch mogelijk is.

Bij schoolverandering zou een betrokkene kunnen vragen om zijn persoonsgegevens automatisch van de oude school naar de nieuwe school over te dragen. Het gaat hier dan enkel om de administratieve gegevens die de betrokkene aan de oude school heeft gegeven. Gegevens uit een mogelijks tuchtdossier van de leerlingen worden nooit overgedragen tussen onderwijsinstellingen.

Het recht om niet aan geautomatiseerde besluitvorming onderworpen te worden

Een betrokkene mag niet onderworpen worden aan een volledig automatische beslissing – zonder menselijke tussenkomst – die hem of haar aanzienlijk treft of juridische gevolgen heeft.

Profilering kan soms gepaard gaan met geautomatiseerde besluitvorming. Profilering verwijst naar: “elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen” (artikel 4(4) AVG).

Om zich te beroepen op dit verbod moet het gaan om:

- een beslissing die uitsluitend op een geautomatiseerde verwerking berust, zonder menselijke tussenkomst. Dit betekent dat een fysieke persoon geen betekenisvolle controle uitoefent op de beslissing en bijvoorbeeld de beslissing niet kan wijzigen of annuleren.
- een beslissing die voor de betrokkene rechtsgevolgen teweeg brengt of die hem op een andere manier aanzienlijk treft.

In drie situaties is het toch toegestaan om geautomatiseerde individuele besluitvorming toe te passen:

- als een **wet** dit toelaat (bijvoorbeeld voorkoming van belastingfraude en -ontduiking);
- als de besluitvorming berust op een **uitdrukkelijke toestemming** van de betrokkene; of
- als dit noodzakelijk is voor de **totstandkoming of de uitvoering** van een **overeenkomst**.

Past een onderwijsinstelling in één van deze drie gevallen toch geautomatiseerde besluitvorming toe, dan moet deze voorzien in passende maatregelen die de rechten van de betrokkene beschermen. Die maatregelen omvatten minstens de mogelijkheid voor de betrokkene om dit besluit aan te vechten, zijn of haar standpunt kenbaar te maken en een menselijke tussenkomst te vragen.

Wat wil dit voor een onderwijsinstelling zeggen?

Als je bijvoorbeeld gebruik maakt van een online-tool om toetsen af te nemen kan deze tool een student bijvoorbeeld een onvoldoende geven op basis van het aantal gemaakte fouten. Maar de tool mag geen **besluiten** nemen gebaseerd op de persoonlijkheidkenmerken van een student. Het is dus verboden een student automatisch van fraude te beschuldigen en uit te sluiten omdat hij na een reeks onvoldoende toetsen of oefeningen opeens wel goed scoort. De tool mag deze verbetering signaleren maar er is steeds menselijke tussenkomst nodig om een besluit uit deze gegevens te vormen. Is er toch een automatische besluitvorming dan heeft de student steeds het recht om bezwaar tegen dit besluit in te dienen.

Wat als het fout loopt?

Een datalek – documenteer en meld het!

Iedere onderwijsinstelling moet procedures invoeren om bepaalde ‘inbreuken in verband met persoonsgegevens’ (ook wel datalek genoemd) te melden. De AVG omschrijft een datalek als een inbreuk op de beveiliging die per ongeluk of met opzet leidt tot een vernietiging, verlies, wijziging of ongeoorloofde toegang of doorgifte van persoonsgegevens.

Een inbreuk komt gemakkelijker voor dan je denkt:

- een cyberaanval waarbij ransomware de toegang tot de IT-infrastructuur en bestanden blokkeert;
- een verloren of gestolen laptop, USB-stick of andere gegevensdrager met persoonsgegevens;
- een ernstige stroomuitval heeft tot gevolg dat de toegang tot de servers wegvalt;
- een leerling onrechtmatige toegang tot een leerlingenadministratie of volgsysteem heeft bekomen.

De onderwijsinstelling moet elke datalek – ook de allerkleinste – bijhouden in een intern logboek. Dit logboek vermeldt: de oorzaak, de getroffen persoonsgegevens, de gevolgen en de genomen maatregelen. Daarnaast valt het aan te raden om de reden van het datalek al dan niet te melden aan de GBA hier ook op te nemen. Dit logboek kan geïntegreerd worden in het register van verwerkingsactiviteiten.

Bovendien moet de onderwijsinstelling in bepaalde situaties de inbreuk ook melden:

- aan de GBA: als het datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van de betrokkene;
- aan de betrokkene: als het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene.

Melden aan de GBA

Een onderwijsinstelling moet een datalek melden aan de GBA als de inbreuk waarschijnlijk een risico inhoudt voor de rechten en vrijheden van de betrokkene. De AVG zegt dat de verwerkingsverantwoordelijke (de onderwijsinstelling) deze melding moet doen zonder onredelijke vertraging en, indien mogelijk, binnen de 72 uur nadat ze op de hoogte is van dit datalek. Indien een verwerker een datalek opmerkt, dan meldt deze hij dit datalek meteen aan de verwerkings-verantwoordelijke. Die het op zijn beurt weer doorgeeft aan de GBA. Indien je de melding niet binnen de 72 uur dororgeeft aan de GBA moet je de vertraging motiveren. De melding vermeldt minstens: tijdstip van het datalek; tijdstip waarop de onderwijsinstelling op de hoogte was, de vermoedelijke oorzaak, de getroffen persoonsgegevens, de gevolgen, de genomen maatregelen en de contactgegevens van de persoon die het datalek opvolgt binnen de onderwijsinstelling.

De onderwijsinstelling die op de hoogte is van een datalek, maar nog niet over al deze informatie beschikt, mag al overgaan tot melding en de overige informatie later bezorgen.

- bij een inbraak wordt een geëncrypteerde laptop gestolen met personeelsgegevens. De onderwijsinstelling heeft een backup van de gegevens. Zolang de encryptiesleutel niet wordt gestolen of gekraakt is een melding bij gebrek aan risico niet noodzakelijk. Is de laptop niet geëncrypteerd of niet beschermd met een wachtwoord moet je wel melding maken aan de GBA;

Melden aan de betrokkene

Een onderwijsinstelling moet een datalek melden aan de getroffen individuen als het datalek waarschijnlijk **een hoog risico** inhoudt voor de rechten en vrijheden van de betrokkene.

Dit is echter niet noodzakelijk als:

- de onderwijsinstelling veiligheidsmaatregelen had voorzien om toe te passen bij een datalek, zoals bijvoorbeeld een sterke encryptiemethode of dubbele authenticatie;
- de onderwijsinstelling na de datalek maatregelen nam waardoor het hoge risico zich waarschijnlijk niet meer zal voordoen (bijv. wissen op afstand bij diefstal van een laptop);
- de individuele mededeling zou onevenredige inspanningen vergen. Een openbare mededeling is in dit geval aangewezen om de betrokkenen te informeren.

    - Bijvoorbeeld een hacker verkrijgt toegang tot de personeelsgegevens van de school. De intrusie wordt gedetecteerd. Het gaat om: naam, adres, gezinssamenstelling, salaris en ziekteverloven. De school licht de GBA in binnen de 72 uur en brengt ook het personeel op de hoogte.

Wanneer is er een (hoog) risico?

De volgende criteria zijn relevant om te bepalen of er sprake is van een waarschijnlijk (hoog) risico in geval van een datalek. Deze lijst is niet exhaustief en in de praktijk zal de onderwijsinstelling altijd een feitelijke afweging moeten maken in functie van het concrete geval. Daarom net is het van belang om de reden van niet-melden ook op te nemen in het logboek van de inbreuken in verband met persoonsgegevens.

- de gevoeligheid van de gelekte data: bv. gegevens m.b.t. financiële situatie, gezondheid, identiteitsdocumenten;
- de hoeveelheid van de gelekte data: bepaalde gegevens kunnen afzonderlijk onschuldig zijn, maar in combinatie niet;

- de mogelijke gevolgen voor een individu: identiteitsdiefstal, fraude, reputatieschade of vernedering;
- het aantal getroffen individuen;
- de kwetsbaarheid van individuen: persoonsgegevens van kinderen, ouderlingen of gehandicapte personen;
- het gemak om individuen te identificeren: zijn de gegevens al dan niet versleuteld of gecodeerd?

Indien de school een gegevenslek vaststelt in haar leerlingenvolg- of leerlingenadministratiesysteem doordat bijvoorbeeld een leerling een wachtwoord van een leerkracht onderschept, zal dit bijna altijd leiden tot een melding aan de GBA en de betrokkenen.

Een overtreding van de AVG

Bij een overtreding van de AVG kan de betrokkene beroep doen op twee parallelle afdwingings-mechanismen. De betrokkene die meent dat de verwerking van zijn/haar persoonsgegevens inbreuk maakt op de AVG kan een **klacht** tot de GBA richten die kan uitmonden in een **sanctie voor de onderwijsinstelling** of **schadevergoeding** eisen via de gewone rechtbank. Niets sluit uit dat betrokkenen tegelijkertijd een klacht indienen bij de GBA en zich richten tot de rechter.

Sancties

De GBA kan verschillende sancties opleggen bij een niet-naleving van de AVG. Naar aanleiding van een klacht of op eigen initiatief kan de GBA onder andere:

- een waarschuwing of berisping geven;
- dwingen om een verzoek van de betrokkene in te willigen;
- dwingen om binnen een bepaalde termijn de verwerking AVG-conform te maken;
- de verwerking bevriezen of verbieden;
- boetes opleggen tot 2% of 4% van de jaaromzet, afhankelijk van de inbreuk.

De onderwijsinstelling heeft een plicht om medewerking te verlenen bij een eventueel onderzoek van de GBA (artikel 31 AVG). Indien u het niet eens bent met een juridisch bindende beslissing van de GBA die aan u gericht is, kan u een voorziening in rechte instellen tegen die beslissing (artikel 78 AVG).

Schadevergoeding

Iedere persoon die schade lijdt door een inbreuk op de AVG, kan een schadevergoeding eisen voor de rechtbank (artikel 79 AVG). Indien er meerdere verwerkingsverantwoordelijke en/of verwerkers betrokken zijn bij eenzelfde verwerking kan betrokkene zich zowel tot de verwerkingsverantwoordelijke als de verwerker richten (artikel 82 AVG). Elke betrokken verwerkingsverantwoordelijke of verwerker is aansprakelijk voor de gehele schade ten opzichte van het getroffen individu, tenzij zij kunnen bewijzen op geen enkele manier verantwoordelijk te zijn voor de geleden schade.

Na de volledige vergoeding van het getroffen individu, kunnen de verwerkingsverantwoordelijke en de verwerker onderling verhaal uitoefenen. De verwerkingsverantwoordelijke of verwerker die de schade geheel heeft vergoed, kan het deel van de schadevergoeding dat overeenkomt met hun deel van de aansprakelijkheid voor de schade verhalen op andere verwerkingsverantwoordelijken of verwerkers die bij de verwerking waren betrokken.

Let dus op: ook als het probleem zich situeert op het niveau van uw verwerker kan de betrokkene kan zich tot de onderwijsinstelling die verwerkingsverantwoordelijke is, wenden!