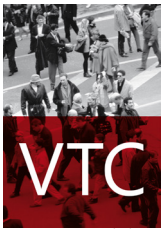
In 7 stappen naar gegevensbescherming in het onderwijs

Volgens De ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) van de EU

Deze brochure kwam tot stand in samenwerking met de Privacycommissie, de Vlaamse Toezichtcommissie en de onderwijsverstrekkers.

CBPL
Commissie voor de **bescherming**
van de **persoonlijke levenssfeer**



In 7 stappen naar gegevensbescherming in het onderwijs

Volgens De ALGEMENE VERORDENING
GEGEVENSBESCHERMING (AVG) van de EU

WAT

is de Algemene Verordening Gegevensbescherming (AVG)?

De Algemene Verordening Gegevensbescherming (AVG) is een nieuwe Europese verordening die regels oplegt waaraan overheden, bedrijven en alle andere organisaties moeten voldoen als ze persoonsgegevens verwerken.

De AVG biedt een betere bescherming aan burgers bij het verwerken[1] van hun persoonsgegevens, maar stelt een aantal regels scherper, geeft verduidelijking, of is een uitbreiding bij de bestaande wetgeving. Het is zoals de Privacycommissie schrijft: "Er is een nieuwe wind op komst, geen orkaan".

Vanaf 25 mei 2018 treedt de nieuwe verordening in werking.

In onderwijsinstellingen[2] zijn er tal van informatiebronnen die persoonsgegevens bevatten. Bijvoorbeeld: alle documenten voor de personeelsadministratie, het leerling- of cursistvolgsysteem, de agenda's van de kinderen, rapporten, het inlichtingenblad dat gevraagd wordt om in te vullen bij de inschrijving ...

1 De term 'verwerking' omvat alle handelingen die je doet met persoonsgegevens: vanaf het verzamelen tot en met het verwijderen van persoonsgegevens (o.a opslaan, raadplegen, wijzigen, uitwisselen, verspreiden). Persoonsgegevens zijn alle gegevens die betrekking hebben op een natuurlijk persoon ('de betrokkene') die rechtstreeks of onrechtstreeks geïdentificeerd wordt of kan worden. We bedoelen onder meer: de naam van een persoon, een foto, een telefoonnummer, een code, een bankrekeningnummer, een e-mailadres, een vingerafdruk ...

2 Onder de term 'onderwijsinstelling' verstaan we, ongeacht het onderwijsniveau, scholen, academies, internaten, centra voor leerlingbegeleiding, centra voor volwassenenonderwijs en de centra voor basiseducatie.

WAT

zijn nu de grootste veranderingen?

» Een grotere verantwoordingsplicht van diegene die de persoonsgegevens verwerkt.

  De onderwijsinstelling zal zelf moeten aantonen dat ze persoonsgegevens volgens de regels van de AVG verwerkt. Dit betekent dat de persoonsgegevens op een veilige manier en met een groot bewustzijn voor de bescherming van de privacy van alle partijen (ouders, kinderen, personeelsleden ...) moeten worden verwerkt.

» Onderwijsinstellingen duiden een aanspreekpunt aan dat op de hoogte is van deze wetgeving en binnen de onderwijsinstelling deze wetgeving mee kan helpen toepassen.

  De vereniging van onderwijsverstrekkers kan zo nodig op zijn beurt ook een functionaris voor de gegevensbescherming of data protection officer (DPO) aanduiden.

» De onderwijsinstelling moet een register van verwerkingsactiviteiten bijhouden.

  Een register van verwerkingsactiviteiten brengt onder andere in kaart van wie en welke persoonsgegevens een onderwijsinstelling verwerkt, waar ze vandaan komen en met wie ze worden gedeeld.

» De wetgeving schrijft een meldplicht bij gegevenslekken voor.

  Als er persoonsgegevens uitlekken, ben je als onderwijsinstelling in bepaalde gevallen verplicht om dit gegevenslek te melden aan de Gegevensbeschermingsautoriteit[3] (en eventueel aan de betrokken personen).

» Een sterker toezicht

  Bij het niet naleven van de AVG, kan de Gegevensbeschermingsautoriteit sanctionerende maatregelen alsook geldboetes opleggen.

3 Vanaf 25 mei 2018 wordt de Privacycommissie hervormd naar de Gegevensbeschermingsautoriteit.

HOE

moet je als onderwijsinstelling persoonsgegevens verwerken?

De belangrijkste principes waaraan een onderwijsinstelling moet voldoen bij het verwerken van persoonsgegevens, zijn:

» Persoonsgegevens verwerk je voor welbepaalde, gerechtvaardigde doelen. Gebruik persoonsgegevens alleen daarvoor en verwerk ze niet verder voor een ander doel.

» Voorbeeld: vanuit de administratie kent een onderwijsinstelling van alle leerlingen of cursisten het thuisadres.

Het is niet omdat een onderwijsinstelling over deze persoonsgegevens beschikt, dat ze deze persoonsgegevens zomaar kan doorgeven aan een uitgever van educatief lesmateriaal of dat de onderwijsinstelling ze kan gebruiken om een adressenlijst naar de ouders of medecursisten te verspreiden. Bij dit voorbeeld heb je nog toestemming nodig van de leerling (of zijn ouders), cursist om deze persoonsgegevens verder te verspreiden.

» Wees transparant bij de verwerking van de persoonsgegevens. Leg zo volledig en duidelijk mogelijk uit wat er met de persoonsgegevens gebeurt: onder andere waarom de school bepaalde persoonsgegevens gaat verwerken, hoe lang de persoonsgegevens worden bijgehouden, welke rechten de betrokkene heeft.... Maak hiervoor eventueel een privacyverklaring op.

» Iedere verwerking van persoonsgegevens is maar rechtmatig als ze aan ten minste één van de wettelijke grondslagen voldoet.

De belangrijkste grondslagen waarop een onderwijsinstelling zich kan baseren, zijn:

- ✓ **De wettelijke verplichting**: als een wet, decreet of ordonantie het oplegt, mogen de persoonsgegevens worden verwerkt.

  Het gaat bijvoorbeeld over administratieve en begeleidende persoonsgegevens van het kind, maar ook de taal die het kind thuis spreekt met ouders, broers en zussen of het bereikte opleidingsniveau van de moeder.

  Zo is ook een bewijs van goed gedrag en zeden nodig om een leerkracht aan te stellen**.**

- ✓ **De overeenkomst**: persoonsgegevens van leerlingen, cursisten en personeel mogen worden verwerkt als zij noodzakelijk zijn voor de uitvoering van een overeenkomst.

  Bijvoorbeeld: doordat de poetsvrouw een personeelslid is van de onderwijsinstelling, heeft de onderwijsinstelling nood aan bepaalde persoonsgegevens om bijvoorbeeld het loon uit te betalen.

- ✓ **De toestemming**: er is toestemming van de leerling/cursist of de ouders van de leerling jonger dan 16 jaar nodig om persoonsgegevens, waar onderwijsinstellingen vanuit wettelijk standpunt of de overeenkomst geen nood aan hebben, te verwerken voor bepaalde doelen.

  Bijvoorbeeld: voor het nemen en publiceren van foto's van leerlingen op de website van de onderwijsinstelling zal er toestemming nodig zijn.

» Een onderwijsinstelling **verwerkt niet meer persoonsgegevens dan nodig** om het welbepaalde, gerechtvaardigde doel te bereiken.

  Bijvoorbeeld: bij de inschrijving van een leerling of cursist hoeft een onderwijsinstelling niet te weten wat het inkomen is van de ouders of van de cursist.

» De persoonsgegevens die een onderwijsinstelling verwerkt, **moeten juist zijn en gecorrigeerd kunnen worden**.

  Bijvoorbeeld: van een leerling die verhuist, moet de onderwijsinstelling het adres aanpassen.

» **Bewaar de persoonsgegevens niet langer dan nodig.**

  Op sommige persoonsgegevens staat een wettelijke bewaartermijn. Respecteer minimaal deze wettelijke bewaartermijn. Als er geen wettelijke bepalingen zijn, leg je zelf een bewaartermijn vast.

» Neem als onderwijsinstelling passende **beveiligingsmaatregelen** om persoonsgegevens te beschermen tegen ongeoorloofde verwerkingen.

Het bestuur van de onderwijsinstelling is verantwoordelijk voor de naleving van deze principes en moet kunnen aantonen dat persoonsgegevens volgens deze verordening verwerkt worden.

HOE

ga je als onderwijsinstelling te werk?

Elke onderwijsinstelling moet vanaf 25 mei 2018 aan de nieuwe verordening voldoen. Het stappenplan is een houvast om de nieuwe verordening te realiseren.

STAP 1
Informeer en sensibiliseer

Het veilig omgaan met persoonsgegevens in een onderwijsinstelling is een zaak van iedereen: directeur, leerkrachten, medewerkers van de administratie, ouders, leerlingen en cursisten, poetsteam, de conciërge, vrijwilligers ...

Zorg tijdens het bewustmakingsproces dat iedereen op de hoogte is van de nieuwe regelgeving en op een correcte manier waakt over de veiligheid van persoonsgegevens.

- ✓ Maak veilig omgaan met persoonsgegevens bespreekbaar en heb er aandacht voor tijdens overlegmomenten: personeelsvergaderingen, ouderraad, overleg onderwijsinstelling - CLB ...
- ✓ Pas zo nodig de volgende teksten aan: het school- of centrumreglement, het arbeidsreglement, de privacyverklaring, het informatieveiligheidsplan, het communicatiebeleid en het ICT-beleidsplan ...

STAP 2 – Aanduiden van een DPO én een aanspreekpunt in de onderwijsinstelling

- ✓ 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** 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[4].

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.

4 Voor onderwijsinstellingen van het gemeentelijk/provinciaal onderwijs neemt de informatieveiligheidsconsulent of DPO van de gemeente/provincie deze taak op zich.

STAP 3 – Gebruik het modelregister van verwerkings-activiteiten

De onderwijsverstrekkers hebben samen een model van **register van verwerkings-activiteiten** voor onderwijsinstellingen gemaakt. Dat bracht al een groot deel van de persoonsgegevens die courant in onderwijsinstellingen worden verwerkt in kaart.

Als je gebruik maakt van dit model dan hoef je als onderwijsinstelling alleen nog de specifieke eigen gegevensverwerkingen toe te voegen.

Het register stel je elektronisch op en hou je actueel.

- ✓ Breng zorgvuldig in kaart welke persoonsgegevens de onderwijsinstelling verwerkt.

Stel ook de volgende vragen:

- ✓ Waarvoor gebruikt de onderwijsinstelling de persoonsgegevens?
- ✓ Waar worden de persoonsgegevens bewaard (pc, papier, externe drager, werken in de cloud)?
- ✓ Met welke internen en externen worden de persoonsgegevens gedeeld? Is hier een geldige motivering voor?
- ✓ Voldoet de onderwijsinstelling aan een legitieme verplichting om de persoonsgegevens te verwerken?
- ✓ Hoelang worden de persoonsgegevens bewaard?
- ✓ Ga eerst na of er wettelijke bewaartermijnen zijn voor het bewaren van persoonsgegevens. Als er geen bewaartermijn is, bepaal zelf een bewaartermijn. Hanteer dan het principe “niet langer bewaren dan noodzakelijk” waarbij je die noodzakelijkheid ook duidt.
- ✓ Wie heeft er toegang tot persoonsgegevens?
- ✓ Ga na wie precies welke toegang krijgt tot persoonsgegevens (lezen, aanpassen, verwijderen ...) en hoe de persoonsgegevens worden afgeschermd. Let wel, toegang kan zowel digitaal als fysiek zijn. Hou dus bijvoorbeeld ook rekening met wie tot welke ruimtes toegang heeft waar persoonsgegevens bewaard worden.

STAP 4 – Overeenkomsten met partners

Onderwijsinstellingen doen vaak een beroep op externe partijen of op bepaalde ICT-diensten die persoonsgegevens voor hen bijhouden.

Zo maken onderwijsinstellingen bijvoorbeeld gebruik van leveranciers van digitale pakketten rond leerlingenadministratie- en leerlingvolgsystemen, van personeelsadministratiesystemen en van educatieve leermiddelen. De AVG beschouwt dergelijke leveranciers doorgaans als 'verwerkers'. De contracten met deze leveranciers moeten conform de AVG herbekeken worden. Besturen van onderwijsinstellingen zijn volgens de AVG immers verplicht een schriftelijk contract af te sluiten met alle externe partijen die persoonsgegevens verwerken.

Softwareleveranciers kunnen intekenen op de **intentieverklaring "privacy in onderwijsmiddelen"**, waarmee ze zich engageren om te voldoen aan de nieuwe regelgeving. Deze intentieverklaring is opgesteld tussen softwareleveranciers enerzijds en de onderwijsverstrekkers anderzijds en waarborgt dat persoonsgegevens bij de verwerker volgens de AVG verwerkt worden.

Onderwijsinstellingen kunnen bij het afsluiten van contracten met softwareleveranciers die intekenden op de intentieverklaring, gebruik maken van het **model van verwerkingsovereenkomst** dat bij de intentieverklaring geleverd wordt.

In de verwerkersovereenkomst worden o.m. afspraken opgenomen over de technische en organisatorische beveiligingsmaatregelen, de bewaartermijnen, informatieverschaffing aan de onderwijsinstelling, beëindiging van contract ...

Ga nu al aan de slag!

- ✓ Maak een lijst van alle softwarepakketten[5] binnen de onderwijsinstelling die persoonsgegevens verzamelen.
- ✓ Vergeet ook de apps en website niet. Verzamel de contracten met providers van deze toepassingen.
- ✓ Bij het afsluiten of hernieuwen van de contracten met de softwareleverancier (in het begin van het schooljaar) kan je gebruik maken van het model verwerkersdocument voor de softwareleveranciers. de onderwijsverstrekkers zullen je hierover verder op de hoogte houden zodra het model beschikbaar is.

STAP 5 – Controleer of toestemming nodig is

Met het register van verwerkingsactiviteiten kan de onderwijsinstelling controleren voor welke verwerkingen van persoonsgegevens een toestemming vereist is.

Bijvoorbeeld: ook foto's en video's waar personen herkenbaar op staan zijn persoonsgegevens. Als de onderwijsinstelling het beeldmateriaal wil gebruiken om op de website te plaatsen kan dit alleen maar als er toestemming is van diegene die op de foto staat (of van de ouders).

5 Onder deze softwarepakketten verstaan we onder andere aan administratie- en volgsystemen voor leerlingen en cursisten, personeelsadministratiesystemen, financieel beheersystemen, roostersystemen, leerling- en oudercommunicatiesysteem, agendasystemen, toets-, rapport-, en evaluatiesystemen, educatieve leermiddelen, elektronische leeromgevingen en leerplatformen (niet limitatieve lijst).

Ga na hoe de toestemming wordt gevraagd en onderwerp ze aan de checklist:

- ✓ Gebruik duidelijke en klare taal en geen kleine letters
- ✓ Vermeld waarom de persoonsgegevens worden gebruikt en wat ermee zal gebeuren
- ✓ Vermeld hoe de persoonsgegevens geraadpleegd en gewijzigd kunnen worden
- ✓ Vermeld ook het recht om vergeten te worden. In sommige gevallen, mag/kan je de informatie van een persoon niet verwijderen omdat het wettelijk niet mag. Neem dit ook op in je tekst
- ✓ Er moet sprake zijn van een actieve handeling

  Bijvoorbeeld: als je toestemming via een elektronisch formulier vraagt, mag het vakje niet automatisch aangevinkt staan.
- ✓ Als de toestemming niet wordt gegeven, mag het geen negatieve gevolgen hebben voor de betrokkene (leerling, cursist, personeelslid ...).

  Bijvoorbeeld: als er geen toestemming gegeven is om foto's te publiceren op Facebook, mag het geen andere gevolgen hebben voor de leerling, cursist of het personeelslid, bijvoorbeeld uitsluiting van een activiteit.

STAP 6 – Fysieke beveiliging en beveiliging van de ICT-infra structuur

Fysieke beveiliging

De toegang tot ruimtes waarin zich persoonsgegevens bevinden of gebruikt/bewerkt worden, beperkt de onderwijsinstelling het best tot de bevoegde personen. Hetzelfde geldt voor serverrooms die persoonsgegevens bevatten.

- ✓ Neem preventieve maatregelen en voorkom zo schade of diefstal. Bijvoorbeeld: gepaste branddetectie, brandblusapparatuur, toegangscontrole ...

ICT-veiligheid

Het is belangrijk om alle IT-soft- en -hardware goed te beveiligen zodat de persoonsgegevens voldoende beschermd zijn.

Neem als onderwijsinstelling daarom de nodige maatregelen om het risico op verlies van persoonsgegevens te voorkomen.

- ✓ Bescherm je computers, laptops, tablets, smartphones … tegen bedreigingen zoals virussen en andere malware.
- ✓ Maak regelmatig back-ups.
- ✓ Evalueer je toegangsbeleid.
- ✓ Leer personeel, leerlingen en cursisten hoe ze geïnfecteerde bestanden herkennen, ermee omgaan en hoe ze veilig kunnen downloaden.
- ✓ Beslis of het personeel, de leerlingen en cursisten toestemming krijgen om persoonlijke mobiele apparatuur te gebruiken of bestanden te downloaden op infrastructuur van de onderwijsinstelling.

  Leg de voorwaarden hiervoor vast.
- ✓ Pas de basisregels m.b.t. wachtwoordbeveiliging strikt toe en zorg dat leerlingen, cursisten en het personeel van de onderwijsinstelling ze strikt naleven.
- ✓ Laat het gebruik van verwijderbare opslagapparaten uitsluitend toe voor lesopdrachten en eis dat leraren, leerlingen en cursisten alle verwijderbare media scannen op malware voor gebruik. Leer hen om zo'n procedure met succes uit te voeren.
- ✓ Vermijd het opslaan van persoonsgegevens op verwijderbare opslagapparaten (bijvoorbeeld externe harde schijven, USB-sticks …) tenzij het niet anders kan. In dat geval codeer of versleutel je de persoonsgegevens met een paswoord zodat bij verlies de persoonsgegevens niet zomaar geraadpleegd kunnen worden.

Extra aandachtspunten m.b.t. persoonsgegevens

- ✓ Let op met Phishing!

  Phishing is internetfraude waarbij de oplichter het slachtoffer - meestal via mail - naar een valse webpagina lokt en waar er naar een gebruikersnaam en wachtwoord gevraagd wordt Het vormt één van de grootste beveiligingsrisico's. Bespreek dit met het personeel zodat het risico beperkt wordt dat iemand persoonsgegevens doorgeeft.

- ✓ Laat geen documenten met persoonsgegevens achter op de (publieke) printers.

- ✓ Geef geen documenten met persoonsgegevens mee met de gewone papieromhaling.

- ✓ Idealiter gebruik je voor toegang tot persoonsgegevens een tweefactor authenticatie.

- ✓ Bewaar je wachtwoorden op een veilige plaats en deel het nooit met anderen. Schrijf bijvoorbeeld niet al je wachtwoorden op één papier.

- ✓ Log altijd uit.

- ✓ Vergrendel je computer, tablet, smartphone ... ook als je maar voor even je werkplek verlaat. Gebruik de toetscombinatie Win-L.

- ✓ TIP! Hou Safeonweb.be in de gaten en maak gebruik van hun sensibiliseringsmateriaal.

STAP 7 – Inbreuken in verband met persoonsgegevens en meldingsplicht

Een gegevenslek is een situatie waarin persoonsgegevens dreigen ongeoorloofd openbaar te worden gemaakt, verloren te gaan, vernietigd of gewijzigd te worden.

Voorbeelden van gegevenslekken zijn:

- ✓ Het moedwillig stelen van persoonsgegevens door cybercriminelen (hacking, phishing)
- ✓ Verlies of diefstal van verwijderbare opslagapparaten waarop persoonsgegevens staan (externe harde schijf, USB-stick, laptop ...)
- ✓ Technisch falen. Bijvoorbeeld: een lek in een softwareprogramma
- ✓ Het onzorgvuldig omgaan met wachtwoorden
- ✓ Het per ongeluk verzenden van een e-mail met persoonsgegevens.

TO DO VOOR ONDERWIJSINSTELLINGEN

- ✓ Leg een intern register voor gegevenslekken aan en voorzie een interne procedure om lekken op te sporen, te rapporteren, te onderzoeken en nodig te melden.
- ✓ Elk gegevenslek noteer je intern.

  Als het gegevenslek enige vorm van schade kan veroorzaken aan de betrokkene(n), meld je het lek via je aanspreekpunt aan je DPO, die zo nodig binnen 72 uur de Gegevensbeschermingsautoriteit kan verwittigen.

  Bij een hoog risico voor de rechten en de vrijheden moet dit ook aan de betrokkene(n) zelf gemeld worden.

  Voorbeeld: een melding aan de Gegevensbeschermingsautoriteit en de betrokkenen is nodig in geval van diefstal of verlies van niet versleutelde medische gegevens.

WIL

je meer weten over AVG?

- ✓ De Privacycommissie ontwikkelde een uitgebreide portal met een thema-dossier over de AVG. Bekijk daar ook het algemene stappenplan: “AVG. Bereid je voor in 13 stappen.” https://www.privacycommission.be/nl
- ✓ Raadpleeg de uitgebreide technische brochure voor onderwijsinstellingen, specifiek voor directies, ICT-coördinatoren en/of aanspreekpunten. U vindt die binnenkort ook terug op de website van de Privacycommissie.
- ✓ Voor info en inspiratie is de onderwijswebsite van de Privacycommissie www.ikbeslis.be een nuttig instrument en bron van informatie, zeker als je over deze thema’s aan de slag wilt gaan met leerlingen. Er is een jongeren-, een ouder-, en een leerkrachtengedeelte.
- ✓ De onderwijsverstrekkers hebben verschillende voorbeelddocumenten gemaakt waarvan onderwijsinstellingen gebruik kunnen maken. Zo zijn er brieven waarmee je toestemming kan vragen, een register van verwerkingsactiviteiten, een privacyverklaring … beschikbaar. Contacteer daarvoor de contactpersoon binnen uw organisatie.