i-Learn PAPER 5

Gegevensbescherming

Referentie

i-Learnteam. (2022). *i-Learnpaper 5: Gegevensbescherming (5).* i-Learn. URL

De i-Learnpapers worden mogelijk gemaakt door het voltallige i-Learnteam bestaande uit leden van het consortium imec, itec & KU Leuven.
Gepubliceerd in juni 2023.

Inhoud

Over de i-Learnpapers

Het i-Learnproject werd mogelijk gemaakt door de Vlaamse overheid, KU Leuven en imec.

De i-Learnpapers zijn de vrucht van het gelijknamige project dat in opdracht van de Vlaamse overheid is gestart in september 2019 en zal lopen tot juni 2023. Met het i-Learnproject wil de Vlaamse overheid inzetten op verantwoord en duurzaam gebruik van technologie en wil men leerkrachten helpen om personalisatie te implementeren in de Vlaamse lagere en secundaire scholen.

Via het i-Learnplatform bieden we leerkrachten en leerlingen laagdrempelige digitale tools aan die niet de inhoud, maar wel de didactische omkadering aanpassen om de dagelijkse klaspraktijk te ondersteunen, waarin de leerling en leerkracht centraal staan. Zo vergroten we de autonomie van de leerkracht zonder de planlast te verhogen en geven we leerlingen inzicht en inspraak in hun leerproces. Bovendien zetten we in op professionalisering van leerkrachten en de verbreding van de Vlaamse EdTech-sector.

De expertise en evidence-based practices die we hebben opgedaan tijdens het uitdenken, het ontwikkelen en het evalueren van het i-Learnproject, worden nu uitgeschreven en gedeeld aan de hand van de i-Learnpapers.

DOEL VAN DEZE PAPER

Er zijn veel verschillende gegevens nodig om adaptiviteit en personalisatie mogelijk te maken in leerplatformen zoals i-Learn. Die gegevens, ook wel data genoemd, kunnen automatisch worden gegenereerd via de interacties tussen de leerder en het platform, de leerkracht en het platform, en middels de persoonlijke gegevens die de leerder of de leerkracht expliciet deelt. Het is van groot belang om zorgvuldig met die enorme hoeveelheid verschillende gegevens om te gaan, om zo de privacy te verzekeren van de personen die ze delen.

Deze paper stelt zich ten doel om dieper inzicht te geven in hoe i-Learn omgaat met het vraagstuk rond gegevensbescherming. In het eerste deel schetsen we het fenomeen van digitale data in het Vlaamse onderwijs. Daarin formuleren we ook de kansen die het biedt, waarna we enkele kanttekeningen maken bij de evolutie. We onderzoeken de juridische en ethische randvoorwaarden die tools moeten naleven om veilig en verantwoordelijk met gegevens om te gaan. In het tweede gedeelte zullen we zes concrete tips delen, op basis van onze eigen praktijkervaring bij i-Learn, om aan die randvoorwaarden te voldoen. Tot slot sluiten we de paper af met een oproep om samen te zitten met verschillende onderwijspartners en duidelijke, gestandaardiseerde krachtlijnen te formuleren voor de hele sector. In dat slotstuk proberen we de bal ook aan het rollen te brengen door vier concrete aanbevelingen te geven, voornamelijk gericht op beleidsmakers en leveranciers van onderwijskundige tools.

In deze paper worden termen zoals 'digitale technologie', 'digitaal leermiddel', 'online toepassing' en 'tool' door elkaar gebruikt. Er wordt met deze termen steeds bedoeld: een online platform of app waarop educatieve inhoud wordt aangeboden aan leerlingen.

VOOR WIE?

Dit document is samengesteld met als doel onze kennis en inzichten over gegevensbescherming bij educatieve tools te delen met een breed en geïnteresseerd publiek. Elke i-Learnpaper biedt een inkijk in de expertise, knowhow en/of evidencebased practices die we hebben verzameld tijdens de ontwikkeling en uitwerking van het i-Learnproject.

In tegenstelling tot de vorige papers richten we ons in deze paper meer op toolontwikkelaars en –leveranciers en onderwijsinstellingen. Bij hen ligt een grote verantwoordelijkheid om de privacy van leerlingen, van leerkrachten en andere actoren in het onderwijs ter harte te nemen. Niettegenstaande biedt deze paper ook zeer leerrijke inzichten voor een breder publiek, waaronder ook leerkrachten en schooldirecties vallen.

Inleiding

Human Rights Watch onthulde in een rapport uit 2022 een onthutsende praktijk dat de sector van educatieve technologie in een niet zo'n positief daglicht stelde: Ze gaven aan dat maar liefst 146 van de 164 onderzochte platformen wereldwijd al eens gegevens van kinderen hadden gedeeld met een derde partij, vooral advertentiebedrijven die de leerlingen zo konden benaderen met gepersonaliseerde reclame. Die platforms werden in sommige gevallen ook uitdrukkelijk aangeboden of aanbevolen door 39 verschillende nationale overheden, waaronder ook landen uit de Europese Unie (Human Rights Watch).

De concrete bevinding was dat leerplatformen soms zonder disclaimer een trackingtechnologie op het leerplatform installeerden, dat AdTech-bedrijven (Ad. Staat hier voor *advertising*) soms toegang kregen tot de unieke identificatiegegevens van leerlingen en dat zo de fundamentele rechten van het kind tastbaar ondermijnd werden (Security.NL, 2022).

Het probleem van deze al dan niet bewuste handel in gegevens stelde zich voor het eerst duidelijk tijdens de coronapandemie. Toen daardoor de reguliere onderwijspraktijk in gedrang kwam, probeerden scholen en overheden overhaast om met hun leerlingen in contact te blijven. De abrupte aanpassing als gevolg van de nieuwe onbekende situatie bracht echter ook met zich mee dat de aandacht voor gegevensbescherming op de achtergrond belandde.

Ook al is gegevenshandel of zijn gegevenslekken in vele gevallen niet kwaadschiks, deze mistoestand doet desalniettemin een paar belangrijke vragen voor Vlaanderen rijzen. Zou zo'n gegevenshandel ook aan het licht kunnen komen bij Vlaamse toolproviders? Bestaat er een algemeen bindend kader dat zulke praktijken bij educatieve partners voor scholen aan banden legt? Zijn scholen voldoende op de hoogte van de gegevens die van hun leerlingen circuleren?

1. Digitale Data in het onderwijs: een context

1.1 DIGITALE DATA IN OPMARS

Voordat we ons storten op die vragen, willen we eerst de context schetsen van de opkomst van digitale data in het onderwijs. Het voorbije decennium zijn de toepassingen die *digital data* gebruiken als paddenstoelen uit de grond geschoten. Ondertussen gebruiken marketeers gegevens om hun advertenties naadloos op je af te stemmen, overheden stoelen erop om je inkomsten, uitkeringen en belastingen te bepalen en gezondheidsinstellingen monitoren je gezondheid aan de hand van de gegevens uit je medisch dossier. Die lijst van toepassingen is lang niet exhaustief en breidt almaar uit. Natuurlijk heeft ook de onderwijs-technologische sector de voordelen van gegevens omarmd. Meer en meer scholen streven ernaar om hun leerlingen een persoonlijke leerervaring te bieden, willen het studietraject van hun leerlingen nauwer opvolgen. Diverse EdTech-spelers speelden op die vraag in door zelf een toepassing op de markt te brengen die het gepersonaliseerd leren in de hand werkt. Eén zaak hebben alle spelers begrepen: om de leerbehoeften van leerlingen beter te begrijpen, zijn gegevens tegenwoordig onmisbaar geworden (De Argumentenfabriek & Het Kennisnet, 2016).

Vooral de gegevens over onze persoonlijke levenssfeer, de zogenoemde **persoonsgegevens**, zijn interessant. Onder die parapluterm valt alle informatie die rechtstreeks of onrechtstreeks aan een individu kan worden gelinkt. En wat we bedoelen met die informatie, dat suggereert eigenlijk precies de naam. Persoonsgegevens kunnen namelijk naam, voornaam, leeftijd en geslacht, evenals opleidings- of professionele gegevens zoals de naam van de school, het schooljaar en het onderwijstype van de leerling omvatten.

Ten tweede neemt men in het EdTech-veld ook vaak **loggegevens** onder de loep. De verwerking daarvan draagt ook in sterke mate bij tot de creatie van een persoonlijke leeromgeving. Daarbij gaat het om alle technische informatie gekoppeld aan een individuele login of aanmelding op een website, zoals een gebruikersnaam of wachtwoord.

De laatste decennia zijn ook **learning analytics** (LA) op het speelveld gekomen. Via deze praktijk worden gegevens gegenereerd uit de activiteit van een leerling, waarmee de digitale leeromgeving nog meer op de leerling afgestemd kan worden. Learning analytics hebben als uniek doel het leerproces te begrijpen en op verschillende manieren te optimaliseren.

Met name die laatste categorie kreeg al veel aandacht in de context van gegevens in het onderwijs. Individualiteit van leerlingen en de uniciteit van leerprocessen staan namelijk meer dan ooit op de voorgrond. Tegelijk is het voor leraren en schoolleiders een hele opgave geworden die leerdiversiteit zonder ondersteuning te moeten opvangen. Het mag dan ook niet verwonderen dat al ettelijk aantal Tech-bedrijven brood zien in de ontwikkeling van zulke learning analytics.

LEARNING ANALYTICS IN I-LEARN

Ook i-Learn gebruikt gegevens om zijn leerplatform mogelijk te maken en doet daarvoor aan **Learning Analytics (LA)**. Bij i-Learn worden bijvoorbeeld LA verzameld om de leerkracht via een dashboardsysteem een blik te geven op de voortgang en het leerproces van de leerling. In een testfase werden LA ook al ingezet om leerkrachten op basis van hun eigen activiteit nieuwe aanbevelingen te geven over leersporen.

Wil je meer weten over Learning Analytics en welke rol die spelen voor i-Learn? Lees dan zeker paper 3 die zich uitsluitend aan het thema wijdt.

Zeker als gevolg van de coronapandemie is er dus sprake van een versnelde digitalisering en een toegenomen belangstelling voor digitale data. Die vooruitgang manifesteert zich in alle sectoren, zo ook in het onderwijs. Het is belangrijk om het groeipotentieel van LA en andere tools verder te stimuleren. Maar tegelijk moeten er eerst nog een paar groeipijnen geheeld worden: het blijkt namelijk dat de EdTech-markt nog versplinterd is en dat ook op juridisch vlak er nog verschillende onduidelijkheden heersen (Imec, 2022).

1.2 DIGITALE DATA VOOR DE ONDERWIJSPRAKTIJK: EEN MEDAILLE MET TWEE ZIJDEN?

1.2.1 De voordelen van digitale data

Laten we eerst even bezinnen over de gebruiksdoeleinden van digitale data in het onderwijs. Er zijn momenteel al heel wat toepassingen beschikbaar die zich richten op (1) het ondersteunen van administratieve taken in het onderwijs, (2) het versterken van de lespraktijk van leraren en (3) het verbeteren van de leeromgeving van studenten (Prinsloo, 2020; Selwyn, 2015). Wat ons in de context van deze paper echter het meest interesseert, zijn toepassingen (2) en (3). Daar zetten EdTech-spelers namelijk het liefst op in. Een volledig overzicht geven van alle mogelijke onderwijstoepassingen zou ons te ver leiden. We beperken ons daarom tot een kleine greep uit de lijst van wat de voordelen zijn van digitale data in de onderwijssector:

1. Eerst en vooral kunnen gegevens op individueel niveau gebruikt worden om het **leren** van studenten te personaliseren op basis van hun interesses, kennis en vaardigheden. Slimme tools kunnen bijvoorbeeld een leeromgeving op maat creëren voor de leerling. Ze kunnen leerkrachten ook inzicht geven in het leerproces van hun leerlingen, zodat zij de individuele behoeften van elke leerling beter kunnen aanpakken.
2. Op klasniveau kunnen gegevens leraren ook een handje helpen, door het **lesgeven** te verrijken. Een voorbeeld daarvan is dat een leerkracht op basis van gegevens gemakkelijk leerlingen met vergelijkbare behoeften kan groeperen en hen zo via een specifieke remediëring verder kan begeleiden. In die situatie dragen gegevens aan een efficiëntiewinst voor de leerkracht bij.
3. Zowel op individueel als op klasniveau kunnen gegevens het **evalueren** vergemakkelijken. Leerlingen kunnen onmiddellijke feedback ontvangen tijdens het maken van oefeningen, of leerkrachten kunnen een voortgangsdashboard inkijken waarmee ze interpretaties kunnen maken over het leerproces van hun leerlingen.
4. Op school- of schoolbreed niveau kunnen gegevens tot slot ingezet worden om patronen en trends te identificeren door leeruitkomsten van leerlingen met elkaar te vergelijken. Op basis daarvan kunnen we ons onderwijsbeleid aanpassen of kunnen we nieuwe studiemethodes **ontwikkelen**.

Kortom, het gebruik van digitale data kan een positief effect hebben voor (1) het leerproces, (2) de lespraktijk, (3) de evaluatiepraktijk en (4) de verdere ontwikkeling van educatief-pedagogische kennis.

1.2.2 De valstrikken van digitale data

Of het nu is om de productiviteit van een leerkracht te verhogen of om de leerresultaten te optimaliseren, digitale data kunnen de kwaliteit van het onderwijs dus op diverse fronten versterken. Het is dan ook een betere reflex om deze vernieuwing te omarmen dan te weren.

Maar zoals altijd bij de komst van nieuwe technologieën blijkt de medaille ook een keerzijde te hebben. Het lijkt erop dat nieuwe spelers zich in de praktijk nog te oppervlakkig inlaten met bepaalde randvoorwaarden of beperkingen voor ze gegevens gaan verwerken. De beperkingen die we voor onszelf hebben gecreëerd, zijn echter zeer waardevol. Ze dwingen ons namelijk om na te denken over de handelingen die we met de gegevens verrichten (van Trigt, 2019).

Ten eerste zou elke gegevensverwerker enkele **didactisch-technologische randvoorwaarden** moeten vervullen. Dat omsluit het vermogen om gegevens op een juiste manier te analyseren, interpreteren en te nuanceren. Dat lijkt logisch, maar slechts als een toolverstrekker voldoende vaardigheden in *data literacy* of datageletterdheid heeft ontwikkeld, kan die gerechtvaardigd data-analyse inzetten om het leerproces in de hand te werken. Hetzelfde geldt overigens voor leraren, leerlingen en ander onderwijsondersteunend personeel die gegevens van een tool incorporeert in het leerproces.

Daar houdt het niet bij op. Bij het verwerken van gegevens is niet alleen datavaardigheid nodig, maar het vereist ook het vermogen om kritisch te reflecteren op de ethische omgang met gegevens. Verder vraagt het ook enige kennis van de wetgeving.

De voorgenoemde basisvereisten voor gegevensverwerking plaatsen we onder de noemer van **ethische en juridische randvoorwaarden.** De beginselen van die randvoorwaarden staan opgetekend in de AVG (GDPR). Die wetgeving verwacht dat scholen en onderwijsondersteunende instellingen goed documenteren waar, op welke juridische grond en voor welke doeleinden gegevens van leerlingen verwerkt worden. Het verplicht hen ertoe om ze te beschermen.

DE AVG (GDPR)

De **AVG** (Algemene Verordening voor Gegevensbescherming) is de Europese regelgeving die bepaalt hoe men moet omgaan met de persoonsgegevens van individuen (*Verordeningen: Verordening (EU) 2016/679 van het Europese Parlement en de Raad*, 2016). De verordening trad in 2018 over de hele Europese Economische Ruimte in werking. Ze werd geformuleerd met als voornaamste doel het hoofd te bieden aan de uitdagingen voor bedrijven, overheden en organisaties om over landsgrenzen heen persoonsgegevens te verwerken.

Nu de hoeveelheid gegenereerde gegevens blijft toenemen, zijn die voorwaarden meer dan ooit belangrijk. Er wordt een inspanning verwacht om je gegevensverwerkingspraktijk op een lijn te brengen met de ethische en juridische randvoorwaarden van de Europese Unie. Er belandt een belangrijke verantwoordelijkheid op de schouders van tool-providers.

1.3 DIGITALE DATA IN DE ONDERWIJSPRAKTIJK: DE UITDAGINGEN

1.3.1 Een gebrek aan overzicht en bewustzijn

Alle gegevens voor administratieve doeleinden brengen scholen doorgaans goed en volledig in kaart. Maar wanneer het gaat om de verwerking van gegevens in educatieve toepassingen in de klas, ontbreekt het hen vaak aan een helder overzicht. Hoewel sommige scholen een beleidsplan hebben ontwikkeld of in ontwikkeling hebben met betrekking tot digitale leermiddelen, worden de lessen vaak nog door de leerkracht zelf verrijkt met digitale leermiddelen die hij of zij zelf kiest. En niet altijd is de leerkracht op de hoogte van waar de gegevens van de leerlingen dan naartoe gaan.

1.3.2 Een nieuwe uitdaging voor de scholen

Nu is het wel zo dat er bij de contracten met aanbieders van zulke digitale leermiddelen – we noemen ze ook wel **leveranciers** – vaak verwerkersovereenkomsten worden afgesloten. Toch sluipen er ook veel toepassingen in de lespraktijk van een leerkracht waar geen contract voor nodig is, denk maar aan niet-commerciële spelers of aan tools met een gratis aanbod. Het bewustzijn rond gegevensverwerking bij deze toepassingen wordt vaak te beperkt gestimuleerd of onderzocht, laat dus te wensen over. Verschillende privébedrijven speelden inmiddels al in op deze lacune, door scholen tegen betaling hun expertise en diensten aan te bieden.

Een duurzamere oplossing zou uiteraard zijn dat bedrijven in de EdTech-sector duidelijke privacyoorschriften kunnen naleven. In de praktijk blijkt echter dat er nog veel onduidelijkheid bestaat over de te volgen privacyvoorschriften, waardoor niet alle tools dezelfde normen hanteren (Berghmans et al., 2020). Terecht hebben scholen daarom vragen over de samenwerking met bepaalde tools en bedrijven. Helaas kan het soms moeilijk zijn om een meer privacyvriendelijk alternatief te vinden voor bepaalde dienst, en verdwijnen die bezorgdheden over privacy soms weer naar het achterplan.

1.3.3 Een nieuwe uitdaging voor edtech-spelers

De AVG brengt tegelijk voor EdTech-spelers heel wat nieuwe verantwoordelijkheden met zich mee. Gezien de verantwoordelijkheden van scholen, moet je het als toolprovider als erezaak beschouwen om je school-partner optimaal te informeren over het privacybeleid dat je hanteert. De AVG is echter een complexe wet vol met regels en uitzonderingen. Het is dus een hele klus om het spreekwoordelijke bos door de bomen te ontwaren. Waar moet je als beginnende EdTech-speler een antwoord vinden op dat probleem?

In wat volgt delen we onze eigen best practices en geven we enkele concrete tips waarmee de educatieve partners van scholen aan de slag kunnen. We beantwoorden vragen zoals welke rechten van de leerling tools in oog moeten houden, welke principes de gegevensverwerker heilig moeten zijn bij het gebruiken van data, welke instanties overzicht en ondersteuning kunnen bieden in het kluwen van de wetgeving, welke documenten daarbij onontbeerlijk zijn en hoe werk te maken van een waterdicht privacybeleid.

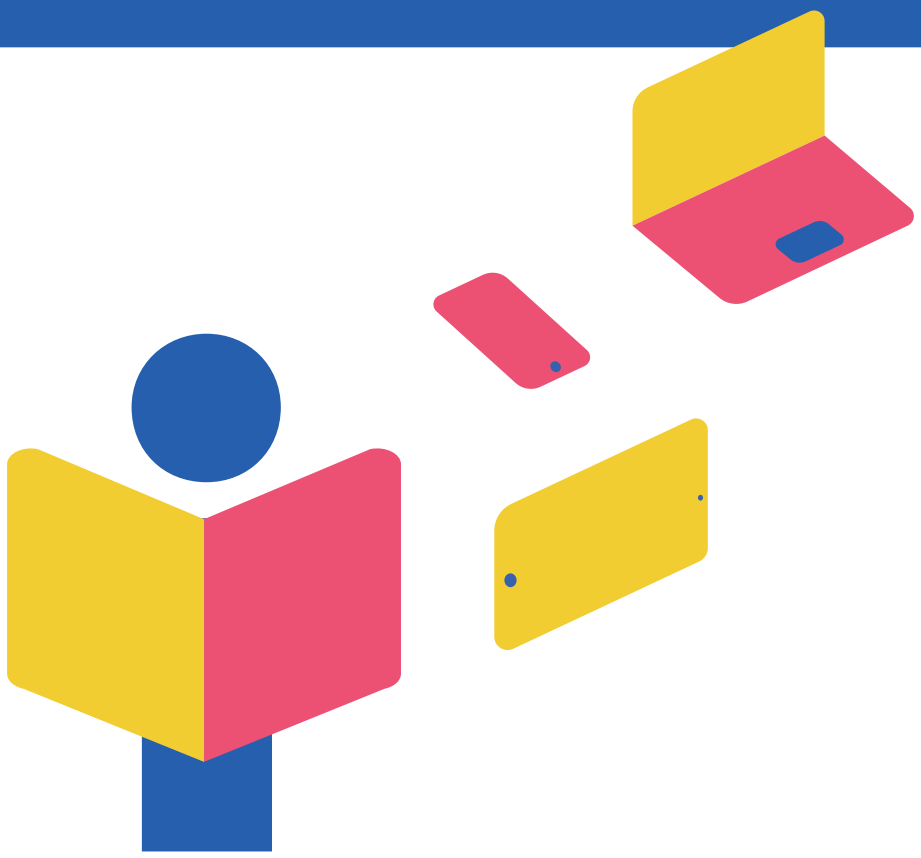
ESSENTIËLE ROLLEN IN HET VERWERKINGSPROCES

Gegevensverwerking is een complex en gestructureerd proces waarbij verschillende spelers strikt afgelijnde verantwoordelijkheden hebben. Twee actoren spelen daarbij een hoofdrol: de **verwerkingsverantwoordelijke** en de **verwerker**.

- **De verwerkingsverantwoordelijke** is de opdrachtgever van de gegevensverwerking, de partij die daarom ook belast is met de eindverantwoordelijkheid ervan. De verwerkingsverantwoordelijke bepaalt het doel, de regels en de middelen van de verwerking en kan een verwerker aanstellen om hem te ondersteunen.

- **De verwerker** verwerkt de gegevens in opdracht van een verwerkingsverantwoordelijke. De verwerker kan op eigen houtje geen persoonsgegevens verwerken of doorgeven aan derden zonder dat daar toestemming voor is gegeven door een verwerkingsverantwoordelijke.

In ons verhaal is de verwerkingsverantwoordelijke meestal de school- of onderwijsinstelling, de verwerker meestal de toolprovider of –leverancier. Het is belangrijk om te weten dat die rolverdeling echter kan variëren naargelang de context van gegevensverwerking (“De AVG in het onderwijs: dit moet je weten”, 2019).



2. Ethische en juridische randvoorwaarden bij digitale data in het onderwijs: best practices van i-Learn

2.1 BEST PRACTICE 1: KEN DE RECHTEN VAN DE BETROKKENEN

Als we aan gegevensbescherming denken, dan is de AVG misschien het eerste wat in ons opkomt. De **AVG** (Algemene Verordening voor Gegevensbescherming) is de Europese regelgeving die bepaalt hoe men moet omgaan met de persoonsgegevens van individuen (*Verordeningen: Verordening (EU) 2016/679 van het Europese Parlement en de Raad*, 2016). De AVG is doorgaans beter bekend onder het Engelse letterwoord **GDPR** (General Data Protection Regulation).

EEN KORTE GESCHIEDENIS VAN DE AVG

Even wat achtergrond schetsen bij de AVG: voordat de wet in 2018 in voege trad, stond ze al langer in de steigers. De wildgroei en –circulatie van gegevens deden al vanaf het begin van de 21ste eeuw heel wat sociale, juridische en ethische vragen rijzen. Bovendien vroeg de toenemende internationale context waarin deze gegevens circuleerden om een geharmoniseerd beleid binnen de Europese Economische Ruimte (Burgess, 2020). Nationale wetten op het gebied van gegevensbescherming waren veelal niet toereikend om gelijke tred te houden met die evolutie.

In 2016 publiceerde de Europese Unie daarom de AVG. Vervolgens gaven ze organisaties en lidstaten twee jaar tijd om deze nieuwe wetgeving te implementeren. In België werd de AVG uiteindelijk op 25 mei 2018 van kracht en verving zij haar voorganger, de Privacywet. Ironisch genoeg was de nood aan deze wet een paar maanden voordien nog op de voorgrond gekomen. Het schandaal rondom Cambridge Analytica, dat aan het licht bracht dat het databedrijf gegevens van 87 miljoen Facebook-gebruikers in handen had gekregen (Jvh & Blg, 2022), had de gevolgen van privacy-inbreuken een duidelijk gezicht gegeven.

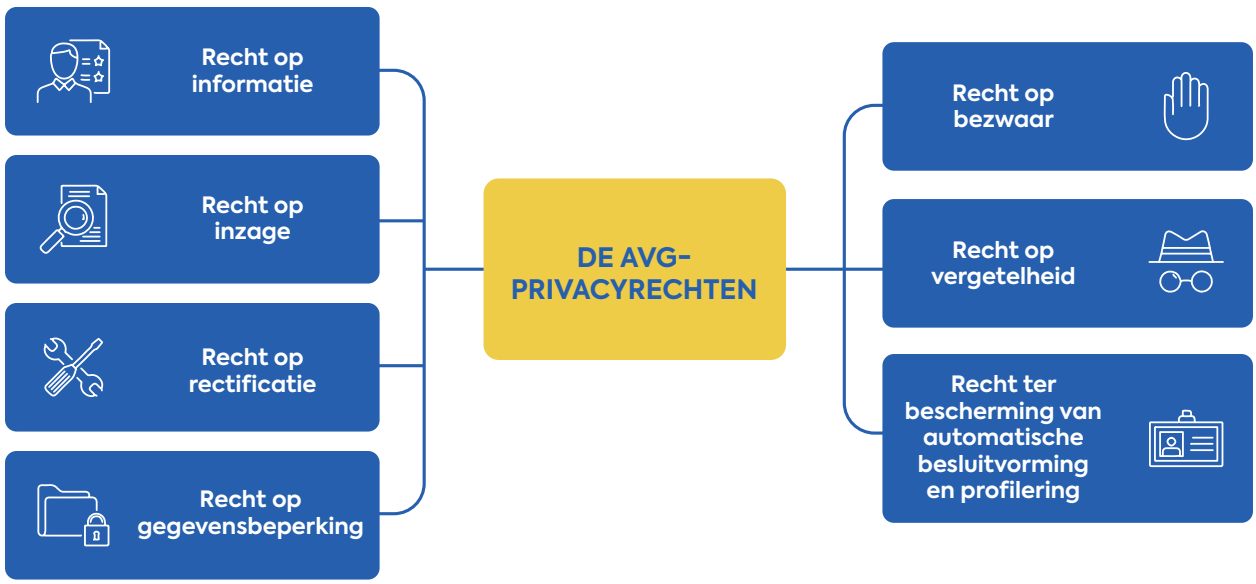
De AVG biedt dus een wettelijk kader voor de bescherming van alle persoonsgegevens binnen de Europese Economische Ruimte (EER). Daarvan zijn de persoonsgegevens die komen uit het onderwijs natuurlijk niet uitgesloten. De AVG stelt dat scholen als verwerkingsverantwoordelijke de correcte verwerking en veilige bewaring van persoonsgegevens van hun leerlingen en leerkrachten moeten kunnen bewijzen. Dat zorgt er dus voor dat scholen uitsluitend in zee zouden mogen gaan met tools die over een AVG-conform beleid beschikken ("Wegwijs in de AVG voor Onderwijsinstellingen", 2018).

Vandaar ons eerste advies voor het naleven van de AVG-richtlijnen: **Doorgrond de rechten van de persoon van wie je gegevens verwerkt goed, en ken je plichten bij het verwerken van persoonsgegevens**.

2.1.1 Wat zijn de rechten van wie gegevens verwerkt worden?

Ieder individu bezit een set basisrechten waarrond de AVG opgetrokken is. Met al die rechten dient de gegevensverwerker rekening te houden. De **betrokkene** - de persoon wiens gegevens worden verwerkt - heeft onder meer het recht om te weten wie welke gegevens over hem verwerkt en voor welke doeleinden. De betrokkene moet daarover correct en tijdig geïnformeerd worden en indien nodig, vrij en geïnformeerd, toestemming geven voor deze verwerking. Deze toestemming kan te allen tijde worden ingetrokken en de gegevens moeten kunnen worden gecorrigeerd. Er bestaan nog enkele andere rechten voor betrokkenen, maar die zijn niet altijd absoluut en kunnen doorgaans alleen in bepaalde omstandigheden worden ingeroepen.

FIGUUR 1: De privacyrechten van een individu zoals beschreven in de AVG



We zetten de acht rechten van de betrokkene, zoals vooropgesteld door de AVG, op een rijtje en geven enkele voorbeelden van de manier waarop ze van belang kunnen zijn voor de verwerker. De verwerkingsverantwoordelijke is verantwoordelijk voor het correct toepassen van deze rechten maar de verwerker heeft hier een belangrijke rol in:

1. Het recht op informatie: de betrokkene heeft het recht om op de hoogte te zijn van de gegevensverwerking en alle relevante bijbehorende informatie. Dit recht impliceert dat de toolaanbieder de nodige inspanningen leveren om alle nodige informatie duidelijk en transparant aan te reiken. Dat kan bijvoorbeeld worden gedaan via een informatiebrochure of een privacystatement op hun website.
   Om te voldoen aan het recht op informatie, moet de betrokkene geïnformeerd worden over verschillende zaken, zoals de bewaartermijn van de gegevens en de procedures voor bezwaar, toegang en rectificatie. Privacyinonderwijs.be biedt daarover een volledige overzicht aan in zijn technische brochure 'WEGWIJS in de AVG voor Onderwijsinstellingen' (2018).

2. Het recht op inzage: de betrokkene moet zijn verwerkte gegevens te allen tijde kunnen inkijken of moet er een kopie van kunnen opvragen. Als EdTech-speler kan je anticiperen op dit recht door al de krijtlijnen van een vlotte procedure uit te tekenen waarbij de onderwijsinstelling binnen een redelijke termijn de gegevens kunnen ter beschikking stellen van de betrokkene.

3. Het recht op rectificatie: heeft de betrokkene verkeerde of onvoldoende gegevens uitgewisseld, of is er iets veranderd aan de situatie? In dat geval moet de betrokkene de fout nog vlot kunnen rechtzetten, of de gegevens gemakkelijk kunnen vervolledigen. Als toolaanbieder kun je best de nodige procedures hebben om de onderwijsinstelling daarbij te ondersteunen.

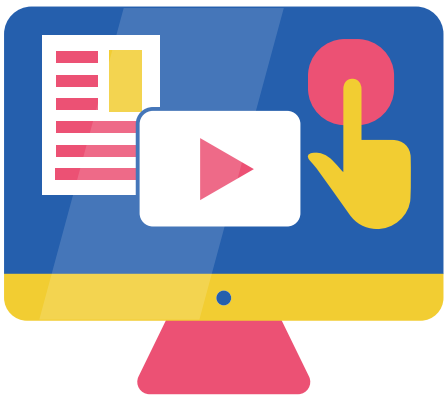
4. Het recht op gegevensbeperking: de betrokkene kan er in bepaalde situaties voor kiezen om zijn gegevens tijdelijk af te schermen van verwerking. De onderwijsinstelling moet evalueren of deze aanvraag gerechtvaardigd is en indien dat zo is, moet de toolaanbieder de mogelijkheid bieden om dit recht te kunnen uitvoeren, tenzij dit een onredelijke inspanning of risico met zich meebrengt.

5. Het recht op bezwaar: in een aantal gevallen kan de betrokkene bezwaar maken tegen de verwerking van zijn of haar persoonsgegevens. Op dat moment rust de verantwoordelijkheid bij de onderwijsinstelling om een afweging te maken tussen de belangen van de gegevensverwerking en het bezwaar van de betrokkene. Afhankelijk van de rechtsgronden kan de verwerking dan worden stopgezet en moet de toolaanbieder dit uitvoeren. Het recht op bezwaar is echter niet onvoorwaardelijk en kan alleen worden ingeroepen in specifieke situaties. Er is echter één situatie waarin het recht op bezwaar altijd te behartigen is: wanneer persoonsgegevens worden gebruikt voor marketingdoeleinden.

6. Het recht op vergetelheid: sterker dan het bezwaar, kan een betrokkene in sommige situaties ook zijn of haar recht op vergetelheid of gegevenswissing inroepen. Zoals de naam al doet vermoeden, kan de betrokkene in dat geval al zijn gegevens laten verwijderen. Ook het recht op vergetelheid is echter niet absoluut, omdat in veel situaties de onderwijsinstellingen de gegevens moeten verwerken in het kader van juridische of administratieve redenen niet zomaar kunnen schrappen. Als de gegevens toch verwijderd moeten worden, dan moet de toolaanbieder dat ook correct uitvoeren.

7. Het recht op gegevensoverdraagbaarheid: Een recht dat minder van toepassing is voor een EdTech-speler in relatie tot de leerling, is het recht op gegevensoverdraagbaarheid. Bij dit recht kunnen betrokkenen de onderwijsinstelling verzoeken om hun gegevens op een digitaal en machineleesbaar formaat over te dragen, zodat die vervolgens voor een andere dienst hergebruikt kan worden. Dergelijke verzoeken tot dataportabiliteit worden bijvoorbeeld ingediend wanneer een leerling van school verandert en zijn persoonsgegevens wil meenemen. In deze situatie dient de toolaanbieder de onderwijsinstelling te ondersteunen bij het vervullen van dit verzoek.

8. Het recht tegen automatische besluitvorming en profilering: dit houdt het recht in om niet geprofileerd te worden op basis van je gegevens. Als een tool bijvoorbeeld gebruik maakt van algoritmes die een automatische analyse – dat staat in dit geval gelijk aan analyses zonder menselijke tussenkomst – uitvoeren op persoonsgegevens en daardoor profilerende feedback of lesmateriaal geeft aan een leerling, dan kan de betrokken leerling dit recht inroepen. Wat onder de noemer van ‘profilering’ valt, staat nauwgezet opgetekend in de AVG.

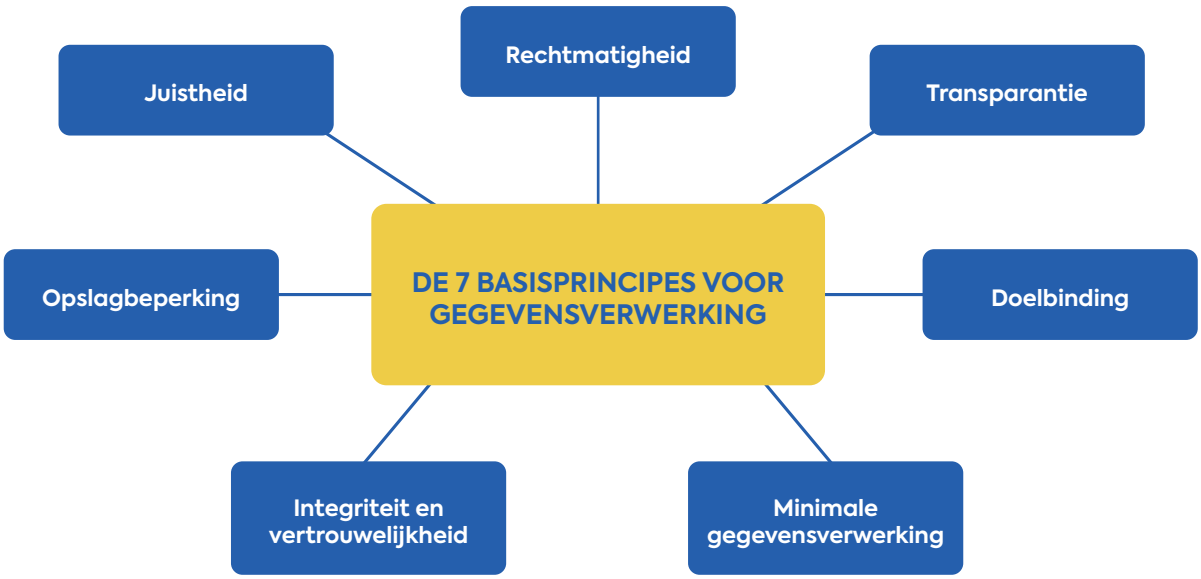


2.2 BEST PRACTICE 2: KEN JE PLICHTEN BIJ DE GEGEVENSVERWERKING

2.2.1 Met welke basisprincipes voor gegevensverwerking moeten alle actoren in het onderwijs rekening houden?

Al wie gegevens verwerkt, hoort met een paar limieten rekening te houden, zo staat het in artikel 5 van de AVG. In de Europese wetgeving voor het onderwijs lezen we negen sleutelwoorden of beginselen voor de verwerking van persoonsgegevens die doorgaans in **zeven basisprincipes** worden gebundeld: rechtmatigheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en integriteit.

FIGUUR 2: De 7 basisprincipes voor gegevensverwerking



Voor alle actoren binnen het onderwijs is het essentieel om deze zeven principes als kompas te gebruiken om zich door het privacylandschap te navigeren. Laat ons daarom even stilstaan bij deze principes die elke partij die persoonsgegevens verwerkt voor om het even welke vorm van gegevensverwerking ter harte zou moeten nemen:

1. Rechtmatigheid: Volgens dit principe moet de verwerking van persoonsgegevens altijd juridisch verantwoord kunnen worden, met andere woorden: ze moet gebeuren op basis van een bepaalde rechtsgrond of grondslag ("Wegwijs in de AVG voor Onderwijsinstellingen", 2018). Er zijn verschillende rechtsgronden die in het onderwijs frequent voorkomen en gecombineerd worden:

a. **De rechtsgrond wettelijke verplichting**: in sommige gevallen is er de mogelijkheid om zich te beroepen op een wetgeving om een bepaalde gegevensverwerking te rechtvaardigen. Zo mogen er bijvoorbeeld op basis van het decreet *rechtspositie personeelsleden* van 27 maart 1997 reglementair gegevens bijgehouden worden van personeelsleden in het kader van het vlotte verloop van personeelsadministratie. Ook bij leerlingen kan deze rechtsgrond worden ingeschakeld, wanneer leerkrachten verplicht aanwezigheden moeten bijhouden.

b. **De rechtsgrond overeenkomst**: leerlingengegevens mogen in sommige gevallen bijgehouden worden op basis van een ondertekend schoolreglement. Dat noemt men de rechtsgrond overeenkomst. Houd er dan wel mee rekening dat het schoolreglement optimale transparantie moet bieden over de persoonsgegevens die voor welke doeleinden verwerkt kunnen worden en de verwerkersovereenkomsten die ze sluit met verschillende leveranciers.

c. **De rechtsgrond gerechtvaardigd belang**: scholen en toolproviders kunnen zich voor sommige verwerkingen van persoonsgegevens ook beroepen op gerechtvaardigd belang zoals voor beveiligingsdoeleinden, evalueren van mogelijke verbeteringen aan toepassingen en organiseren van andere noodzakelijke dagdagelijkse activiteiten.

d. **De rechtsgrond algemeen belang**: sommige scholen kunnen zich voor bepaalde verwerkingsactiviteiten baseren op algemeen belang omwille van hun maatschappelijke verplichtingen zoals het organiseren van onderwijs en de bijbehorende activiteiten.

e. **De rechtsgrond toestemming**: ten slotte wordt er in schoolcontext ook soms de rechtsgrond toestemming ingeroepen, waarbij de school expliciete toestemming vraagt aan een leerling en/of ouders voor het verwerken van persoonsgegevens, zoals het plaatsen van een foto op de schoolwebsite. Een belangrijke kanttekening is dat de betrokkenen die toestemming te allen tijde moeten kunnen intrekken en dat de school die toestemming ook duidelijk en ondubbelzinnig moet kunnen bewijzen.

2. Transparantie: Vermijd verwarring en misverstanden bij betrokken partijen door altijd open kaart te spelen over de gegevens die worden verwerkt en waarom. Transparantie volgens de AVG houdt onder andere in dat het informeringsproces bij de toestemming actief en volledig is. Bovendien moet dat informeringsproces helder worden gedocumenteerd.

3. Doelbinding: Doelbinding wil zeggen dat een school persoonsgegevens enkel mag aanwenden voor bepaalde vooropgestelde doeleinden, en niet voor andere zoals marketing of onderzoek. Doelen waartoe men de gegevensverwerking meestal wel eenvoudig mag verbinden, zijn bijvoorbeeld leerlingenadministratie, leerlingenbegeleiding en communicatie. Als de school toch gegevens wil verwerken voor nieuwe doeleinden, dan moet ze een nieuwe doelbinding aangaan vooraleer een nieuwe gegevensverwerking te kunnen opstarten. Afhankelijk van wat het nieuwe doel is, zal die gelinkt moeten worden aan een nieuwe grondslag uit de AVG (zie rechtmatigheid hierboven).

4. Minimale gegevensverwerking: Een volgende vereiste die de AVG voorschrijft, is dat er niet meer gegevens verwerkt mogen worden dan nodig en wenselijk zijn. Als gegevensverwerker moet je dus een denkoefening maken waarbij je je afvraagt wat '*need to know*' is, en wat '*nice to know*' is. Alles wat niet relevant is, mag niet zonder motivatie opgenomen worden in de gegevensverwerking. Weten wat het beroep is van de ouders van je leerlingen, kan misschien interessant zijn, maar kan enkel in specifieke gevallen verantwoord worden.

5. Juistheid: verwerkte gegevens moeten ook altijd correct en actueel zijn. Dat houdt bijvoorbeeld in dat een school de mogelijkheid moet geven aan leerlingen en ouders om hun eigen dossier te laten corrigeren of te updaten als er iets fout is. Het treffen van gepaste maatregelen om die accuraatheid te garanderen, is daarbij onontbeerlijk.

6. Opslagbeperking: Voor elk gegeven moet een te verantwoorden bewaartermijn worden vastgelegd, zodat ze niet langer opgeslagen worden dan noodzakelijk voor het doeleinde. Die bewaartermijnen worden meestal vastgelegd in decreten. Voor persoonsgegevens van leerlingen uit secundaire scholen geldt bijvoorbeeld een bewaartermijn van vijf jaar na de voltooiing van het secundaire curriculum (Vlaams ministerie van onderwijs en vorming, 2003).

7. Integriteit en vertrouwelijkheid: De AVG benadrukt ook dat gegevens binnen een technisch beveiligde en afgeschermde omgeving moeten worden verwerkt, waarbij de toegang beperkt is tot de leerkrachten en directieleden voor wie de gegevens van belang zijn. Het is aan de scholen om technische maatregelen te treffen die daar gehoor aan geven, zoals het opzetten van een dubbele authenticatie, het installeren van een firewall op het schoolnetwerk en het regelmatig uitvoeren van systeemback-ups.

Deze zeven fundamentele principes van gegevensverwerking - rechtmatigheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en integriteit - bieden een solide basis voor verantwoordelijk en ethisch gebruik van gegevens. **Onze tweede best practice is dus om als toolprovider te streven naar het waarborgen van veiligheid en vertrouwen voor alle betrokkenen, door deze principes als het hoogste goed te beschouwen.**

2.3 BEST PRACTICE 3: KEN DE ORGANISATIES DIE PRIVACYRECHTEN HELPEN WAARBORGEN

Wil je als toolprovider met gegevensbescherming aan de slag? Dan is het minstens even interessant om te weten welke instanties je daarin kunnen bijstaan. De eerlijkheid gebiedt namelijk te erkennen dat niet iedereen zich even gemakkelijk een weg kan banen in het doolhof van AVG-richtlijnen. Voor de handhaving van een complexe wet zoals de AVG die is, bestaan er gelukkig gespecialiseerde controle- en ondersteuningsorganen, ook voor het onderwijs.

Laat ons eerst ingaan op de controleorganen. In eerste plaats treedt de Gegevensbeschermingsautoriteit (GBA) als waakhond op voor de grondbeginselen van de AVG. Hun bevoegdheid reikt federaal en strekt zich over verschillende sectoren uit, zowel die van de overheid als die van de privé. Het takenpakket van de GBA is meerledig: ze verlenen niet enkel advies, maar focussen zich evenzeer op het sensibiliseren over de AVG. Zo lanceerde de GBA de website ikbeslis.be om privacy voor het voetlicht te brengen van jongeren, ouders en leerkrachten. Bovendien grijpt de autoriteit ook in bij datalekken en aanverwante overtredingen. Het is bij de GBA dat scholen als eerste verplicht zijn om dergelijke inbreuken te rapporteren, waarna haar inspectiedienst de risico's en de juridische gevolgen van de situatie nauwgezet in kaart brengt.

In de tweede plaats is er de Vlaamse Toezichtscommissie (VTC), die toeziet houdt op de correcte naleving van de AVG binnen Vlaamse overheidsinstellingen. De VTC werd opgericht in 2018, kort nadat de AVG van kracht ging, en heeft als belangrijke taak te adviseren over de verwerking van persoonsgegevens aan de Vlaamse bestuursinstanties. Het is echter belangrijk om op te merken dat, wegens haar focus op de publieke sector, de VTC geen controle uitoefent over bedrijven in de privésector.

Onder de bevoegdheid van de VTC valt ook het onderwijs in Vlaanderen, waarvoor zij dan ook regelmatig aanbevelingen doet. Een voorbeeld van de invloed van de VTC op het onderwijs vinden we bijvoorbeeld terug, naar aanleiding van de bekendmaking van de Digisprong*. In het kader van het digitaliseringsplan beloofde de Vlaamse overheid ICT-toestellen aan elke leerling. De VTC adviseerde scholen over de manier waarop ze konden omgaan met de aanschaf van deze ICT-infrastructuur en analyseerde de risico's van grootschalige aankopen. Zo raadde de commissie de scholen aan om voldoende aandacht te besteden aan het opnemen van privacyvoorwaarden in de bestekken met de leveranciers van de apparaten (Digitaal Vlaanderen, z.d.).

DE DIGISPRONG

In Vlaanderen tekent de implementatie van *digital data* in het onderwijs zich af tegen de achtergrond van de zogenoemde 'digisprong' ("Visienota "Digisprong"", 2020). De Vlaamse Overheid wil met dit plan onder andere een gericht databeleid uitbouwen, door bijvoorbeeld te bouwen aan een datagestuurd kennis- en adviescentrum. In het plan wordt expliciet gesteld dat gegevens en artificiële intelligentie noodzakelijk zijn voor de beleids- en missievorming van scholen in de toekomst. Het beleidsplan benadrukt verder ook het belang van het volgen van privacyvoorschriften als speerpunt voor een data-onderbouwd schoolbeleid.

Tot slot hebben er ook verschillende **Vlaamse onderwijsverstrekkers** (d.i. alle scholenkoepels onder de verschillende onderwijsnetten zoals GO!, OVSG, POV en GVO) bakens gezet voor de praktische implementatie van de AVG. Zij vervullen een ondersteunende rol in het beschermen van privacy. In een persbericht van 2018, kort voor de AVG van kracht ging, garandeerden de onderwijsverstrekkers al enkele privacyacties te hebben ondernomen (*Persbericht 'Modelovereenkomst beschermt persoonsgegevens in onderwijs'*). Zo hadden ze al ingezet op het verhogen van het bewustzijn over privacygevoelige informatie en het aanwijzen van contactpersonen voor informatieveiligheid.

DE INTENTIEVERKLARING VAN DE VLAAMSE ONDERWIJSVERSTREKKERS

In het eerder vermelde persbericht van 2018 kondigden de onderwijsverstrekkers ook een intentieverklaring aan. Bij het latere uitschrijven van die intentieverklaring genaamd "*Privacy in digitale onderwijsmiddelen*" verbonden de scholenkoepels, waaronder grote spelers zoals KOV en GO!, zich aan de afspraak om gegevensbescherming in schoolgemeenschappen actief te ondersteunen. De verklaring is ondertekend door de meerderheid van de onderwijsverstrekkers alsook door andere instellingen zoals de Vrije CLB-koepel, de Federatie Centra voor Basiseducatie, de Groep Educatieve en Wetenschappelijke Uitgevers en verschillende softwareontwikkelaars ("Intentieverklaring Privacy in Digitale Onderwijsmiddelen", 2018)

Een belangrijk onderdeel van de intentieverklaring was trouwens de invoering van een schriftelijk contract, genaamd een **verwerkersovereenkomst**. Dat konden scholen als houvast gebruiken om zich te beschermen tegen risico's bij samenwerking met 'gegevensverwerkers'. De overeenkomst legt de spelregels voor zowel de verwerkingsverantwoordelijke (dat is bv. een school) als de verwerker (dat is bv. een onderneming die een digitale educatieve toepassing aanbiedt en daarvoor leerlingengegevens moet verwerken) tot in de details vast. Meer over de verwerkersovereenkomst vind je bij best practice 4.

Van de VTC tot de GBA en de Vlaamse onderwijsverstrekkers - de bovenstaande controle- en ondersteuningsorganen bieden waardevolle richtlijnen en helpen toolproviders op weg door de complexiteit van de AVG. **Onze derde best practice luidt dus om als toolprovider je beleid zorgvuldig op hun adviezen en expertise af te stemmen.**

2.4 BEST PRACTICE 4: MAAK GEBRUIK VAN DE VERWERKERSOVEREENKOMST

In de vorige best practice vermeldden we dat er vanuit verschillende hoeken al initiatieven zijn genomen om privacy en gegevensbescherming in het Vlaams onderwijs te coördineren. Als antwoord op de inwerkingtreding van de AVG creëerden diezelfde partijen (de VTC, GBA en Vlaamse onderwijsverstrekkers) in 2018 een voorbeeldleidraad in de vorm van een **verwerkersovereenkomst** ("Model Verwerkersovereenkomst", 2018).

De verwerkersovereenkomst is een standaardsjabloon waarin de afspraken tussen de verschillende partijen betrokken bij de gegevensverwerking worden vastgelegd. Het zorgt ervoor dat contracten tussen deze partijen over heel Vlaanderen een helder en uniform karakter krijgen. Bovendien passeren alle verplichte juridische en ethische bepalingen uit de AVG erin de revue. Ondertussen heeft menig toolleverancier zich het model al eigen gemaakt.

Waaruit bestaat de verwerkersovereenkomst? In het inleidende gedeelte van het contract worden enkele belangrijke afspraken vastgelegd, onder meer over de rolverdeling in het gegevensverwerkingsproces, het doel van de verwerking, de plichten van de verwerkers en subverwerkers, de rechten van de betrokkenen en de gevolgen van schending van het contract. Daarop volgen twee bijsluiters: in de privacybijsluiter wordt de aard van de verwerking tot in de puntjes toegelicht, de tweede bijsluiter biedt een overzicht van technische en organisatorische beveiligingsmaatregelen die de verwerkers moeten treffen als ze informatie delen of als er een gegevenslek zou optreden.

EERSTE HULP BIJ GEGEVENSLEKKEN

Alle preventiemaatregelen ten spijt, wat als je als toolleverancier toch met een gegevenslek te maken krijgt? Artikel 7 van de verwerkersovereenkomst formuleert de stappen die de verschillende partijen moeten zetten om het gevaar bij een inbreuk in te dijken:

Opgelet: niet elk gegevenslek wordt als risicovol beschouwd. Daarom moeten niet voor elke soort gegevenslek de onderstaande stappen worden doorlopen. De situaties waarin het risico groot is, kan je nalezen via Kluwereasyweg.be.

1. Komt de inbreuk aan het licht, dan dient **de toolleverancier (de gegevensverwerker)** de school (de verwerkingsverantwoordelijke) zonder onredelijke vertraging en met zo veel mogelijk informatie op de hoogte te stellen. Is er vermoeden dat persoonsgegevens gelekt zijn en de inbreuk dus een verhoogd risico inhoudt, dan moet de school gewoon onmiddellijk ingelicht worden.

2. **De school (de verwerkingsverantwoordelijke)** moet vervolgens de impact inschatten van de data-inbreuk op de rechten en de vrijheden van de leerlingen (de betrokkene).

3. **Beide partijen** nemen de nodige maatregelen om de schending van de privacy waar mogelijk in perken te houden, en soortgelijke inbreuken in de toekomst te vermijden.

Onder de maatregelen die een school (de verwerkingsverantwoordelijke) moet nemen, als het gegevenslek risicovol is, behoren:

- Het gegevenslek melden bij de GBA door een formulier in te dienen (© Gegevensbeschermingsautoriteit 2023, z.d.). Het niet melden van een gegevenslek kan leiden tot een sanctie. Meer informatie over de situaties en de manier waarop je dit moet melden, kan je lezen op Kluwereasyweg.be.
- De leerlingen, ouders, personeel en andere betrokkenen op de hoogte brengen.
- Het intern privacybeleid updaten om gelijkaardige datalekken in de toekomst te voorkomen, ook bij laag risico.
- Elke bovenvermelde maatregel nauwgezet documenteren, ook bij laag risico.

Onder de maatregelen die een toolleverancier (de verwerker) moeten nemen behoren:

- De verantwoordelijke zo goed mogelijk ondersteunen en bijstand verlenen bij zijn taken. Dat kan bijvoorbeeld door inzage in de gegevens te geven of door expertise te delen.
- Het intern privacybeleid updaten om gelijkaardige datalekken in de toekomst te voorkomen.
- Elke bovenvermelde maatregel nauwgezet documenteren.

Deze modelverwerkersovereenkomst kan voor uniformiteit en sluitende duidelijkheid zorgen voor zowel de verwerker als de verwerkingsverantwoordelijke. **Vandaar adviseren we toolproviders om op dit model voort te bouwen elke keer dat een nieuwe overeenkomst afgesloten wordt met een verwerkersverantwoordelijke school.**

2.5 BEST PRACTICE 5: IMPLEMENTEER EEN GEGEVENSBELEID

In onze interacties met andere EdTech-tools valt ons op dat het kennisniveau en de uitvoeringsgraad omtrent privacyregelgeving stijgt. Veel tools investeren onder andere in medewerkers die een privacybeleid uitwerken en in de werking implementeren. Op platformen krijgen privacyverklaringen ook vaker een prominente plaats. Verder kunnen tools meer en meer rekenen op de ondersteuning van een eigen functionaris voor gegevensbescherming (Engels: DPO), een expert in privacywetgeving en AVG.

Er circuleren echter ook EdTech-tools waarvan het gegevensbeleid nog niet op punt staat. **Maakte je als toolprovider nog geen (of nog te weinig) werk van een uitgekiende strategie, dan stellen we dus als vijfde best practice voor om dat zo snel mogelijk te doen.** Voor elke medewerker die in contact komt met gegevens kan het namelijk nuttig zijn om een beroep te kunnen doen op een IT-coördinator of een DPO, of gewoonweg een gegevensbeleid om zijn of haar twijfels over een kwestie te kunnen aftoetsen. Het beschikken over zo'n expert kan organisatiebreed veel duidelijkheid scheppen in het kluwen van de privacywetgeving.

HOE WERKT HET IN I-LEARN?

Voor zijn gegevensbeleid deed i-Learn een beroep op de expertise van imec Privacy Office, voerde het een gegevensbeschermingseffectbeoordeling (GEB) uit met een bureau dat advies rond gegevensbeleid geeft (zie bijlage) en vroeg formeel – en paste vervolgens toe - het advies van de Vlaamse Toezichtscommissie. Specifiek voor het wetenschappelijk onderzoek binnen i-Learn werd het gegevensbeleid telkens aan de hand van een privacydossier door de ethische commissie van KU Leuven geëvalueerd.

2.6 BEST PRACTICE 6: VOER EEN GEB UIT

Elke nieuwe gegevensverwerking is uniek en complex, en soms moet je als toolprovider onbegane grond bewandelen als het op gegevensverwerking aankomt. De gegevensverwerking aftoetsen aan je gegevensbeleid dekt ook niet altijd alle zorgen die er kunnen zijn over de privacyrisico's. In zulke gevallen is het aangeraden om een **gegevensbeschermingseffectbeoordeling (GEB, Engels: DPIA)** te overwegen, de ideale check-up voor je gegevensverwerking.

Een GEB uitvoeren is een manier om de mogelijke risico's verbonden aan je gegevensverwerking boven water te halen. Een GEB is geen vast recept dat je zomaar kunt volgen. Het is een goed gedocumenteerd proces van nadenken over de mogelijke risico's die je loopt als je gegevens verwerkt. De Algemene Verordening Gegevensbescherming (AVG) geeft wel een paar richtlijnen waar je op moet letten (*Data Protection Impact Assessment*, 2021).

Wanneer is zo'n GEB nu juist aan de orde? Dat hangt af van de aard en de omvang van de verwerking en de mogelijke impact op de rechten van de betrokkenen. Volgens de AVG is er sprake van zo'n verhoogd privacyrisico als (1) iemand systematisch wordt geprofileerd op basis van zijn persoonsgegevens, (2) de gegevensverwerking bijzonder grootschalig is of (3) als de gegevens bijvoorbeeld verzameld worden via camerabewaking in de openbare ruimte. Dat zijn echter niet de enige situaties waarin een GEB nodig is. Om het overzicht te bewaren, stelde de VTC daarom een lijst op met alle categorieën van verwerkingen waarvoor een GEB verplicht is (De Vlaamse Toezichtscommissie, 2022).

De verantwoordelijkheid voor het uitvoeren van een GEB ligt bij de verwerkingsverantwoordelijke. Het is aan hen om ervoor te zorgen dat een GEB effectief heeft plaatsgevonden en dat de nodige maatregelen zijn genomen om de privacy te beschermen. Denk bijvoorbeeld aan een onderwijsinstelling die een tool inschakelt om gegevens namens de school te verwerken voor een bepaald educatief doeleind. De opdrachtgever-school draagt in eerste instantie de verantwoordelijkheid en hoeft de verwerker-tool hier niet mee te belasten.

Het is echter niet altijd nodig dat de verwerkingsverantwoordelijke zelf de GEB uitvoert. Ze kan ook kiezen om de taak uit te besteden aan een derde partij buiten de organisatie. In dat laatste geval is het wel belangrijk dat de verantwoordelijke het proces goed in de gaten houdt en, indien mogelijk, de eigen DPO nauw betrekt bij de uitvoering.

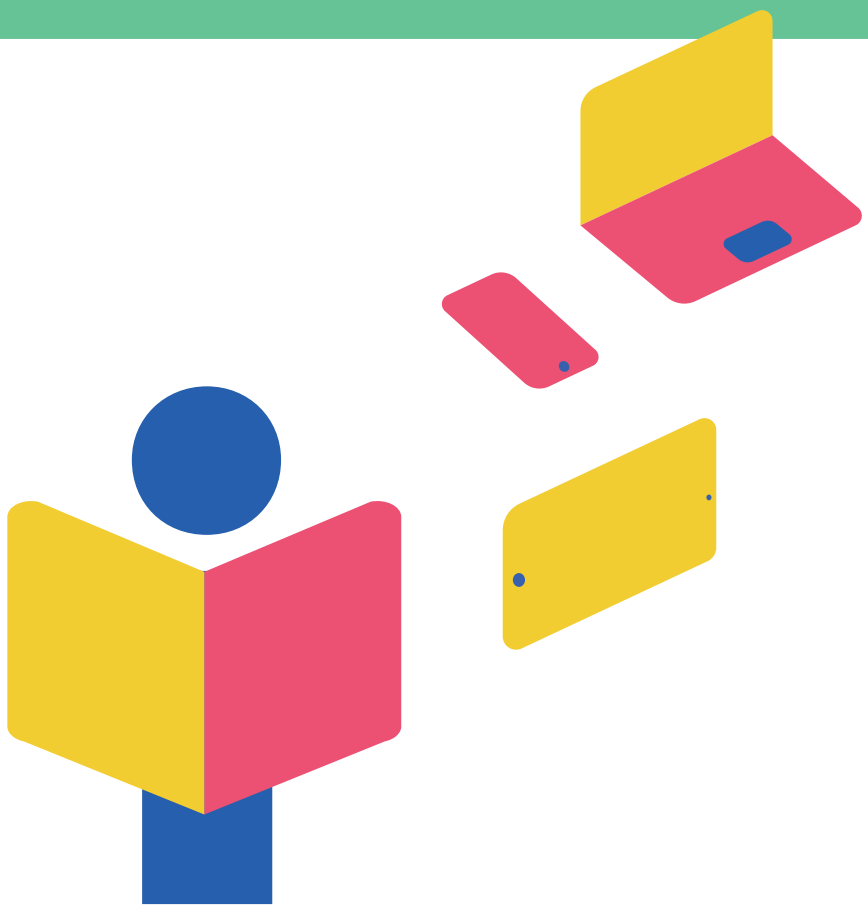
Ook al ben je als toolprovider geen verwerkingsverantwoordelijke en is het niet verplicht, toch is het zeer verstandig om in sommige gevallen een GEB te laten uitvoeren. Het helpt namelijk om zorgvuldig met gegevens om te gaan en om het vertrouwen van het publiek te consolideren. Er hoeft geen ruchtbaarheid gegeven te worden aan het feit dat een GEB is uitgevoerd, maar het kan wel goed zijn voor de reputatie van de tool.

HOE WERKT HET IN I-LEARN?

Het i-Learnproject verwerkt heel wat persoonsgegevens van leerlingen en leerkrachten om gepersonaliseerd leren mogelijk te maken. Het is van cruciaal belang dat op een verantwoorde manier met deze persoonsgegevens wordt omgegaan, gezien de gevoeligheid van de doelgroep en de verhoogde verantwoordelijkheid die het project heeft als overheidsopdracht. Om een optimale bescherming te garanderen, heeft i-Learn dus op eigen initiatief een GEB (of DPIA) laten uitvoeren. Op die manier werden de privacyrisico's van de verwerking van persoonsgegevens goed in kaart gebracht en konden proactief maatregelen worden genomen om de privacyrisico's in te dijken.

i-Learn is een verwerker en de verwerkingsverantwoordelijkheid van de gegevens zelf ligt strikt genomen bij de scholen. En zoals voorheen aangehaald komt de uitvoering van een GEB neer op de schouders van de verwerkingsverantwoordelijke. Toch hebben wij beslist om een eerste stap te zetten, en hebben we scholen alvast proberen te helpen door een eerste GEB uit te voeren op onze eigen verwerkingspraktijken. Scholen die i-Learn gebruiken, kunnen die GEB bij het gebruik van ons platform gerust verzetten om alle concrete privacyrisico's verbonden aan de eigen schoolcontext nog beter te schetsen.

Ben je benieuwd naar de scope van onze GEB en naar welke concrete vaststellingen daaruit zijn gekomen? Aarzel dan niet om het verslag na te lezen in bijlage.



2.7 BEST PRACTICE 7: BLIJF JEZELF INFORMEREN

Een laatste gouden tip en best practice is om eenvoudigweg constant met privacy en gegevensbescherming bezig te blijven. Met elke nieuwe technologische ontwikkeling om de zoveel tijd worden er nieuwe richtlijnen geschreven, worden wetgevingen aangepast. Om bij te blijven, moet je jezelf voortdurend informeren.

Om je op weg te helpen, refereren we nog naar interessante documenten en websites voor toolproviders, directies, leerkrachten en onderwijsinstellingen met aanvullende informatie over privacyrechten, verplichtingen en procedures:

Interessante documenten en websites voor toolproviders (zijde van de verwerker):

- De intentieverklaring *privacy in Digitale Onderwijsmiddelen* en de bijhorende modelverwerkersovereenkomst: https://www.privacyinonderwijs.be/

Interessante documenten en websites voor leerkrachten, directie en onderwijsinstellingen (zijde van de verwerkersverantwoordelijke):

- Het privacy-abc van Mediawijs, Vlaams Kenniscentrum Digitale en Mediawijsheid (Heyman et al., 2019): https://assets.mediawijs.be/2021-10/mediawegwijzer_privacy_herdruk19_def_lr.pdf

- Handleiding voor het melden van gegevenslekken bij de Gegevensbeschermingsautoriteit (GBA): https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-over-het-gebruik-van-invulformulieren.pdf

- Stappenplan om de AVG succesvol te implementeren in het beleid van de onderwijsinstelling: https://onderwijs.vlaanderen.be/sites/default/files/2021-07/In-7-stappen-naar-gegevensbescherming-in-het-onderwijs_Privacycommissie.pdf

- Wegwijzer door de AVG voor ICT-coördinatoren en directie: https://assets.vlaanderen.be/image/upload/v1664979613/wegwijzer_-_GDPR-AVG_q1qyel.pdf

3. Besluit

We komen even terug op het nieuwsartikel uit de inleiding. We stelden ons de vraag of het Vlaamse toollandschap wel immuun was voor gegevenshandel of datalekken. Door ons contact met toolproviders, onderwijsinstellingen en beschermingsautoriteiten kunnen we wel bevestigen dat er over het algemeen veel inspanningen geleverd worden om een mistoestand zoals in Nederland aan het licht was gekomen, te vermijden. Dat wil echter niet zeggen dat we op onze lauweren kunnen rusten en niet meer voortdurend op ons hoede moeten zijn voor een onverantwoordelijke manier van gegevensverwerking.

We kunnen er namelijk niet aan onderuit: het gebruik van gegevens in het onderwijs vertoont een almaar opwaartse trend – een evolutie die nog eens versneld is door de coronapandemie –. Het aantal gegevens dat we gebruiken om onze educatieve praktijk te ondersteunen, zal er in de toekomst niet op achteruitgaan. Er staan ons nog heel wat uitdagingen te wachten op vlak van gegevensbescherming en het waarborgen van privacy in het onderwijs.

In wat volgt staan we daarom nog een laatste keer stil bij de voornaamste uitdaging voor het onderwijs en geven we enkele aanbevelingen die we zowel richten tot beleidsmakers, onderwijsinstellingen als toolsontwikkelaars:

3.1 UITDAGINGEN EN AANBEVELINGEN VOOR EDUCATIEVE TOOLS

We merken dat enkele partijen in het educatieve toollandschap in 2018 al een privacycharter https://www.privacyinonderwijs.be/overzichtslijst.html hebben ondertekend en daarmee aangaven de bijhorende verwerkingsovereenkomst te hanteren. De lijst van die actoren is echter bijzonder beperkt en werd volgens de website sinds 2018 niet meer bijgewerkt. Inmiddels zijn er echter heel wat nieuwe educatieve tools op de markt verschenen.

Een hedendaagse school moet een breed scala aan digitale leermiddelen kunnen hanteren, zonder dat ze zich daar constant de vraag bij moeten stellen of de privacy van hun leerlingen in gedrang komt. Desalniettemin ontbreekt het momenteel aan een up-to-date kader of richtlijnen voor privacybeleid met betrekking tot deze leermiddelen. Dat zou niet alleen een geruststelling voor leraren zijn, maar ook voordelig zijn voor de toolproviders zelf.

Bovendien vormt het voor aanbieders van digitale leermiddelen ook een grote uitdaging om bij te blijven met de voortdurend veranderende regelgeving rond privacy. De constante wijzigingen in het onderwijs, de digitale wereld en de toepasselijke regelgeving slingeren hen om de oren. Een charter kan ervoor zorgen dat de AVG en de privacyrichtlijnen toch top of mind blijven.

De vraag rijst of standaardisatie van een sectorale gedragscode of op zijn minst informatie-uitwisseling op verschillende niveaus geen betere oplossing zou bieden? Op basis van onze ervaringen in i-Learn en *lessons learned* uit andere samenwerkingen, willen we al een bijdrage leveren en willen we enkele aanbevelingen doen, gericht aan leveranciers en beleidsmakers:

- **Aanbeveling 1**: De AVG biedt de mogelijkheid om **sectorale gedragscodes op te stellen** als vorm van certificering voor een bepaalde sector. Dat geldt ook voor de aanbieders van digitale leermiddelen, die dan vrij zijn om te bepalen of ze daaraan willen voldoen. Door zo'n gedragscode op te stellen en te laten valideren door de gegevensbeschermingsautoriteit, kunnen afnemers van digitale leermiddelen een bepaald niveau van garantie krijgen met betrekking tot privacygerelateerde aspecten.

- **Aanbeveling 2:** Een andere optie is om digitale leerplatformen te **certificeren via een onafhankelijke organisatie** die controlepunten vastlegt waaraan de aanbieders moeten voldoen. Als die controle transparant en regelmatig wordt uitgevoerd, dan kunnen scholen zelf beslissen welke digitale leermiddelen ze willen gebruiken. Een transparante certificatie verhoogt ook de transparantie voor ouders en leerlingen omdat zij die informatie ook kunnen inkijken.
  Een voorbeeld van transparante certificatie zien we bij het Amerikaanse gebruik van ISO-standaarden. Het moet echter onderstreept worden dat ISO-standaarden geen Europees concept zijn.
  Niettemin zijn er binnen Europa inmiddels Europese normen in ontwikkeling die momenteel in de goedkeuringsfase zitten en die ook het GDPR-verhaal dekken. Zodra de kaders beschikbaar zijn, zal het nodig zijn om te kijken naar de mogelijkheden voor certificering van EdTech-bedrijven in België. Elk land binnen Europa zal naar verwachting zijn eigen certificeringsprocedures en -normen hanteren, maar uiteindelijk moeten die certificeringen wel Europees worden goedgekeurd.

- **Aanbeveling 3:** Daarnaast zou er een **leidraad** moeten komen voor leerkrachten om snel te kunnen evalueren of het veilig is om digitale leermiddelen te gebruiken die niet onderhevig zijn aan contractuele aspecten, zoals gratis platforms en websites. Die leidraad kan een beperkt overzicht geven van aandachtspunten voor leerkrachten, zoals locatie van gegevensverwerking en het gebruik van cookies.

- **Aanbeveling 4:** Ten slotte is het van belang om al het schoolpersoneel dat met persoonsgegevens in aanraking komt, toegang te geven tot **leermiddelen over het veilig gebruik ervan in digitale leerplatformen**. Als eindgebruikers op een verstandige manier omgaan met die gegevens, dan kunnen veel privacygerelateerde twijfels automatisch opgelost worden en risico's vermeden worden. De leermiddelen kunnen bijvoorbeeld ingaan op het beperken van de gegevens die worden gebruikt en het niet altijd accepteren van alle cookies.

Standaardisatie zal natuurlijk nooit de rol van de privacyexperten in het onderwijs overbodig maken, maar het kan wel helpen om de focus te leggen waar het echt nodig is. Regelmatige validatie en monitoring door beschermingsautoriteiten zullen nog steeds broodnodig blijven, maar de werklast kan dan al gedeeld worden over meerdere partijen.

3.2 AANBEVELINGEN VOOR LEERKRACHTEN EN SCHOLEN

Ben je leerkracht, dan is het belangrijk om waakzaam te blijven over de privacygegevens van je leerlingen als je een digitale tool inzet in de klas. Toegegeven, in afwachting van een gestandaardiseerd kader, is het niet eenvoudig om zich succesvol een weg te banen door de digitale wildgroei. Probeer toch in de mate van het mogelijke na te gaan welke persoonsgegevens worden verzameld en hoe ze worden verwerkt.

4. Bijlage 1: de GEB bij i-Learn

De GEB van i-Learn richt zich specifiek op het portaal i-Learn MyWay, dat gegevens verwerkt van zowel leerkrachten als leerlingen. Aangezien het project gegevens van een gevoelige doelgroep verwerkt en een groot aantal minderjarige leerlingen betreft, was een robuust gegevensbeleid een must. Bij i-Learn zijn we bovendien overtuigd van een *privacy by design*-aanpak. Dat betekent dat we de bescherming van onze persoonsgegevens vanaf het begin meenemen in het ontwerp van ons platform en de ontwikkeling van onze diensten.

i-Learn voerde daarom een uitgebreide GEB uit om de potentiële privacyrisico's van het project aan het licht te brengen en te mitigeren. Op basis van de resultaten van de GEB konden we een voorstel voor mitigatiemaatregelen doen, waarna dat werd voorgelegd aan de Vlaamse Toezichtscommissie en hun advies werd verankerd in i-Learns gegevensbeleid. In deze bijlage zoomen we in op de reikwijdte van deze GEB en bespreken we de resultaten ervan.

4.1 WAT VIEL ER BINNEN HET BEREIK VAN I-LEARNS GEB?

Binnen de GEB van i-Learn MyWay onderzochten we de cloudarchitectuur, de applicatie, de processen, de aanpak, de helpdesk, de optimalisatie van het platform, het onderhoud en de overdracht van gegevens vanuit i-Learn MyWay. Het document gaat later verder op deze onderwerpen.

4.2 WAT VIEL ER BUITEN HET BEREIK VAN I-LEARNS GEB?

Het project i-Learn omvat meer dan enkel het i-Learn MyWay-portaal. Onze GEB had echter wel betrekking op enkel en alleen dit portaal. De volgende aspecten vielen dus buiten de scope van onze GEB:

- **De onderliggende (content)platforms** (Bookwidgets, Dodona, Smartschool, etc.)
- **Het wetenschappelijk onderzoek** (imec-itec-KUL)
- **Het coachingplatform** (i-Learn Academy)
- **De verwerkingsactiviteiten, risico's en AVG-vereisten** die specifiek zijn voor de rol van de verwerkingsverantwoordelijke

Hieronder lichten we kort toe waarom deze aspecten niet tot de kern van onze GEB behoorden en, indien relevant, welke strategieën we hanteren om ook hier de privacy van onze eindgebruikers te beschermen.

4.2.1 Onderliggende platformen

Een van i-Learns doelen was om de toegang en het gebruik van educatieve content te vergemakkelijken. i-Learn MyWay biedt daarom voor scholen toegang tot educatieve toepassingen vanuit een gecentraliseerd platform. i-Learn host echter zelf geen educatieve toepassingen: MyWay leidt de gebruikers telkens vlot naar externe, third-party applicaties. Daarom hebben we ook geen specifieke beoordeling van gegevensbescherming verricht voor al deze externe tools.

i-Learn streeft er desalniettemin naar om de bekendheid en ondersteuning van bestaande initiatieven te vergroten en ervoor te zorgen dat de gegevens van haar gebruikers veilig en beschermd blijven. i-Learn voorziet bijvoorbeeld voor elke toepassingen een ingevulde verwerkersovereenkomst of referentie naar de privacy policy. Van elke individuele tool die een school binnen i-Learn wil gebruiken, kan de administrator van de school die verwerkersovereenkomst inkijken. Vervolgens kan de administrator zeer gemakkelijk de gewenste tools aanvinken, om die daarna ook op te nemen in het schoolreglement.

De manier waarop we de eerdergenoemde ondersteuning bieden verschilt echter per soort onderliggend platform of toepassingen waarmee i-Learn samenwerkt. Als volgt staan we daarom kort stil bij het verschil in aanpak van de tools die we kunnen indelen in drie categorieën: de LTI-gekoppelde tools, de bevriende tools en de klasmanagementsystemen:

- **LTI-gekoppelde tools**

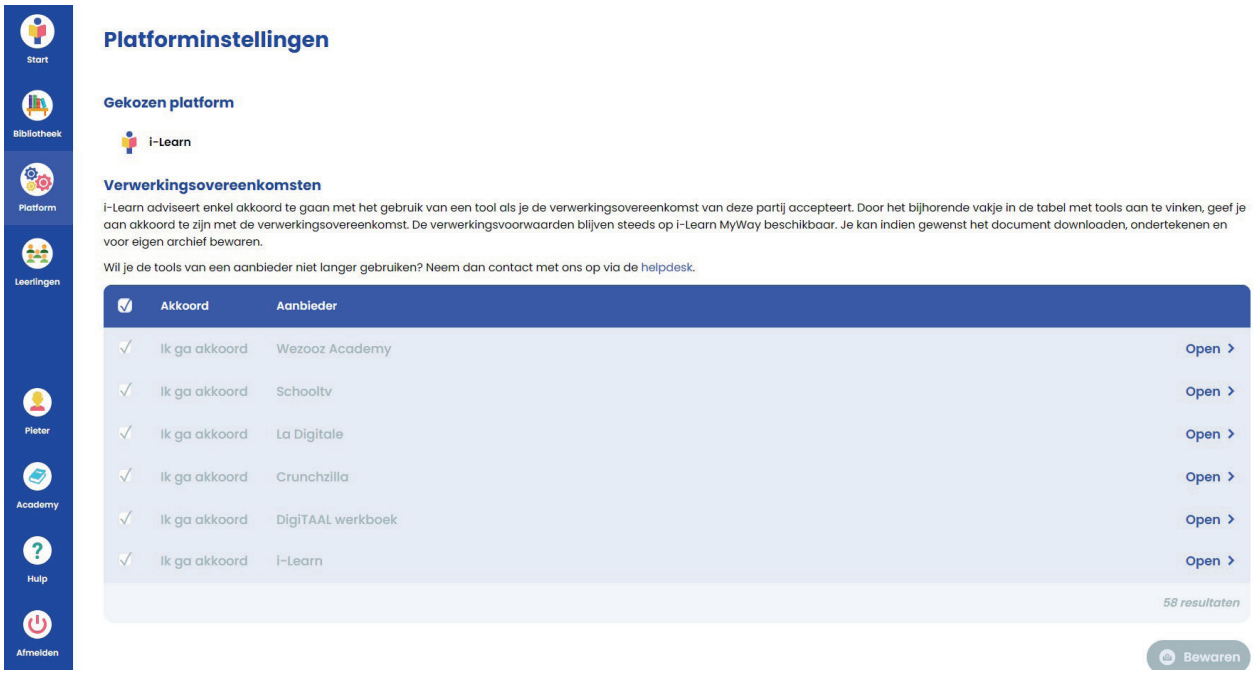
LTI staat voor Learning Tools Interoperability. Wanneer een tool LTI-gekoppeld is, betekent dat dat gebruikers de tool kunnen gebruiken vanuit i-Learn MyWay zonder zich apart bij de tool te hoeven aanmelden. Deze toepassingen verlangen de meeste persoonsgegevens, omdat ze een persoonlijk account per gebruiker aanmaken en de progressie van de gebruiker bijhouden, waarmee opvolging mogelijk is door leerkrachten en soms ook door leerlingen. Voor elke tool van deze categorie heeft i-Learn een verwerkersovereenkomst afgesloten op basis van een modelovereenkomst, die wordt aangepast aan de specifieke vereisten van de tool.

Enkele voorbeelden van LTI-gekoppelde tools die beschikbaar zijn op i-Learn MyWay zijn:

1. Bookwidgets: Via deze tool kan je als leerkracht diverse onlineoefeningen (‘widgets’) maken. Het is een authoring tool die voor alle vakken en leeftijden ingezet kan worden.
2. EduHint: Deze tool biedt digitaal oefenmateriaal wiskunde aan voor de eerste en tweede graad van het secundair onderwijs.
3. Karaton: Dit is een educatieve avonturengame, gemaakt om kinderen te motiveren om dagelijks te oefenen op lezen en schrijven.

Om toegang te krijgen tot deze categorie van tools moet de administrator van de school de verwerkersovereenkomsten van de gewenste apps valideren, ondertekenen en archiveren. Bovendien heeft i-Learn de externe providers ook aangemoedigd om de Intentieverklaring Privacy in Digitale Onderwijsmiddelen te ondertekenen. Daardoor heeft i-Learn die tools ook een hoge verantwoordelijkheid met betrekking tot privacy toegeschreven.

FIGUUR 3: Om toegang te krijgen tot LTI-gekoppelde tools van i-Learn moet de administrator van de school de verwerkersovereenkomsten van de gewenste tools valideren, ondertekenen en archiveren.



- **Bevriende tools**

Bevriende tools zijn vrij toegankelijk en vereisen geen persoonlijke gegevens van leerlingen op het i-Learnplatform. Hoewel bevriende tools dus geen directe integratie met i-Learn hebben, kunnen ze echter nog steeds persoonsgegevens opvangen, dan wel op andere manieren via hun platform zelf. Om die reden biedt i-Learn ook de privacy policy van deze apps de administrator van scholen. De schooladministrator dient die privacy policy dan te valideren, vooraleer de tools te kunnen gebruiken. Als een applicatie zich buiten de EER bevindt en daarom rekening houdt met alternatieve privacyrichtlijnen in plaats van de AVG, dan communiceren wij dat ook duidelijk aan de schooladministrator.

Om scholen te ondersteunen bij die validatie, werd elke bevriende tool bovendien aan een privacycheck onderworpen door het privacy office van imec. Dit omvat onder andere een volledigheidscontrole van het privacystatement, controle op het gebruik van cookies en de controle of er data buiten de EER gaat of niet. Indien er data buiten de EER gaat, betekent dat dat het onderhevig is aan andere wetgeving dan de GDPR.

Op basis van onze bevindingen namen we beslissingen over eventuele aandachtspunten of de noodzaak naar verdere validatie van de tool. De resultaten van onze privacyscreening werden vervolgens aan de tool voorgelegd opdat zij ermee aan de slag kon gaan.

Een voorbeeld van dat proces zien we geïllustreerd in onze samenwerking met de Universiteit van Vlaanderen. De website kreeg aanvankelijk een negatief advies omdat de GDPR niet correct was toegepast. Na contact met de eigenaars werden er door hen met succes aanpassingen doorgevoerd. Intussen is de website volledig conform de Europese regelgeving. De tool maakt sindsdien deel uit van het MyWay-toolaanbod en wordt regelmatig geraadpleegd door onze gebruikers.

FIGUUR 4: De mogelijke resultaten van een toolreview

- **Klasmanagementsystemen**

Leerkrachten en leerlingen hoeven niet telkens te surfen naar i-Learn om met een unieke gebruikersnaam en wachtwoord aan te melden. Ze kunnen snelle toegang krijgen tot i-Learn door middel van externe identiteitsproviders zoals Smartschool, Office365 en Google. Deze klasmanagementsystemen zorgen ervoor dat de gebruiker-leerkracht of -leerling niet opnieuw hoeft in te loggen op i-Learn, doordat hij of zij al geauthentiseerd is via de aanmelding op het systeem.

4.2.2 Onderzoek vanuit itec

Een van de pilaren waarop i-Learn steunt is wetenschappelijke onderzoek. Het project vertrekt vanuit bestaande wetenschappelijke inzichten en wil tegelijk nieuwe inzichten brengen/mogelijk maken door i-Learn als testbed in te zetten voor verschillende vraagstukken. Dat onderzoek wordt gevoerd door de onderzoekers van de imec onderzoeksgroep, verbonden aan de universiteit van Leuven (itec). Hoewel gegevensverwerking via zulke wetenschappelijke onderzoeken niet in de GEB wordt meegenomen, worden er wel strenge maatregelen genomen om de privacy van de deelnemers aan het onderzoek te waarborgen.

Voordat er wetenschappelijk onderzoek kan worden gedaan, moet het onderzoek eerst **bij de KU Leuven intern** worden beoordeeld op ethische en privacyaspecten. Dat is de taak van de Sociaal-maatschappelijke Ethische Commissie (SMEC), die ervoor zorgt dat het onderzoek op één lijn ligt met de AVG (Research Coordination Office KU Leuven, 2023). Pas als het onderzoek door SMEC is goedgekeurd, mag de gegevensverwerking van start gaan.

Bij wetenschappelijk onderzoek via i-Learn wordt er ook nog een tweede maatregel getroffen om de privacy van deelnemers te beschermen: persoonsgegevens worden gepseudonomiseerd zodat de informatie die verzameld werd moeilijk terug te traceren is naar een individu. Als er toch een link moet worden gelegd tussen de informatie en het individu, dan wordt er om uitdrukkelijke toestemming gevraagd van het individu zelf of van hun ouder of voogd als het individu minderjarig is.

4.2.3 Coachingplatform

Een succesvolle adoptie van nieuwe tools is ondenkbaar zonder de nodige ondersteuning voor de gebruikers. Die wordt in i-Learn aangeboden aan leerkrachten via de i-Learn Academy. Hier vinden leerkrachten zowel online documentatie en e-learning, als ook vormingen en opties om on-site coaching en begeleiding aan te vragen. Aangezien de verwerking van persoonlijke gegevens op dit platform minimaal is en enkel volwassen leerkrachten toegang hebben tot dit onderdeel van i-Learn, is de Academy ook niet inbegrepen in de GEB. Zo worden er op Academy enkel naam, voornaam en e-mailadres op automatische basis bijgehouden. Wanneer er toch persoonsgegevens worden opgevraagd, dan is het invullen nooit verplicht en wordt er om expliciete toestemming gevraagd. Leerkrachten moeten ook de gebruiksvoorwaarden en privacy policy eenmalig accepteren voordat ze kunnen inloggen op Academy.

4.2.4 Specifieke verwerkingsactiviteiten van de school

De school die gebruik maakt van i-Learn MyWay is altijd eindverantwoordelijk voor de verwerking van gegevens. De verwerkingsactiviteiten van de school zelf zijn uiteraard specifiek aan de school en kunnen daarom onmogelijk opgenomen worden in de GEB die het i-Learn-project uitvoert. Elke school moet zelf beoordelen of ze hun verwerkingsactiviteiten laten keuren.

4.3 DE FASES VAN I-LEARNS GEB

In dit onderdeel lees je hoe het i-Learnteam, samen met een gespecialiseerd adviesbureau en de DPO van imec, het GEB-proces voor het MyWay-portaal heeft aangepakt. Het proces bestond uit de volgende vijf fases:

4.3.1 Fase 1: de workshops

Het adviesbureau ging in eerste fase in gesprek met verschillende leden van het i-Learnteam, zoals de product owner, technical lead en programmamanager, om een duidelijk beeld te krijgen van het portaal en de dataflow. Elke workshop behandelde één specifiek thema dat in de diepte werd uitgespit, waaronder de architectuur, de rollen, de rechtsgrond, de transparantie en de retentieperiode van persoonsgegevens in ons portaal. De resultaten van alle workshops werden gebundeld in een finaal document, waarvan de belangrijkste conclusies verder in dit document worden besproken.

4.3.2 Fase 2: de gesprekken

Nadat we het opzet van het i-Learn MyWay-portaal in kaart hadden gebracht, samen met de privacyrisico's die eraan verbonden waren en onze strategieën om die risico's te mitigeren, gingen we in gesprek met verschillende partijen om ons plan voor te stellen. Op basis van de feedback die we hebben verzameld tijdens die gesprekken, hebben we de eerste versie van onze GEB uitgewerkt.

We spraken met verschillende scholen en benadrukten hun potentiële rol als verwerkingsverantwoordelijke voor i-Learn MyWay. Daarnaast onderzochten we toolproviders om te zien of zij soortgelijke privacyrisico's op een betere manier konden mitigeren. Ook hebben we contact opgenomen met de werkgroep informatieveiligheid (Departement Onderwijs en Vorming) om onze bevindingen en mitigatiestrategieën voor te leggen en hebben we de DPO van het Departement Onderwijs & Vorming geraadpleegd.

4.3.3 FASE 3: DE CONSULTATIE BIJ DE VLAAMSE TOEZICHTSCOMMISSIE

In een derde fase vroegen we het advies van de VTC. We legden onze eerste versie van de GEB voor en in het bijzonder enkele privacyrisico's en -strategieën met betrekking tot onze cloudarchitectuur. Een sterk uitgebouwde cloudarchitectuur, waarbij gegevens veilig opgeslagen, verwerkt en gedeeld worden, is namelijk essentieel om de toegankelijkheid van digitale middelen in de klas te garanderen. Een krachtige cloud zorgt er bijvoorbeeld voor dat i-Learn MyWay efficiënt en performant kan omgaan met een hoog piekgebruik tijdens de lesuren en een laag gebruik buiten de schooltijd.

EEN CLOUDARCHITECTUUR VINDEN: EEN VERHAAL VAN BALANCEREN TUSSEN FUNCTIONALITEIT EN PRIVACY

Voor het vinden van een passende cloudarchitectuur voor i-Learn heeft het advies van de Vlaamse Toezichtscommissie (VTC) een cruciale rol gespeeld. De VTC had namelijk het gebruik van Amerikaanse cloudservices, zoals AWS (Amazon), Azure (Microsoft) en Google Cloud, rigoureus onder de loep genomen waardoor ze er op privacyvlak zeer kritisch over stond (Van der Stadt, 2023).

De motivatie van de VTC om die harde lijn te hanteren, komt voort uit verschillende overwegingen. Ten eerste hebben Amerikaanse bedrijven te maken met de Cloud Act en de Foreign Intelligence Surveillance Act (FISA), die in wezen stellen dat veiligheidsdiensten het recht hebben om gegevens op te vragen bij elk Amerikaans bedrijf, ongeacht de locatie van de server, in het geval van een crimineel onderzoek. Bovendien verwerken scholen gevoelige informatie, met name gegevens van kinderen. Het belang van privacy en gegevensbescherming wordt daardoor verder versterkt.

i-learn zelf is niet rechtstreeks onderhevig aan de monitoring van de VTC. Imec, de organisatie achter i-learn, valt namelijk niet onder de bevoegdheid van de VTC. Niettemin beoordeelden we dat het verstandig was om proactief advies in te winnen over onze aanpak en cloudstrategie bij de VTC. i-learn maakt momenteel namelijk gebruik van Azure, een Amerikaanse cloudservice.

Zoals verwacht adviseerde de VTC ons om Amerikaanse clouds te vermijden en om passende maatregelen te nemen. Hoewel we daartegenin ook de waarde van Amerikaanse clouds erkenden voor de beveiliging en technische services die elders niet even goed ontwikkeld zijn, wilden we ook het advies van de VTC ter harte nemen. Om risico's te minimaliseren slaan we nu directe identificatoren op in een Europese cloud, terwijl gecodeerde log- en gegenereerde informatie opgeslagen wordt in de Amerikaanse cloud. Waar mogelijk, streven we ernaar om over te stappen op Europese alternatieven, zoals het LeerID-initiatief. Door deze maatregelen verkleinen we het risico voor betrokkenen, terwijl we toch gebruikmaken van de functionaliteiten van Amerikaanse cloudproviders.

Omdat Europese cloudproviders dus nog minder ver ontwikkeld zijn, hebben we de voor- en nadelen zorgvuldig afgewogen om een weloverwogen beslissing te nemen die gegevensbescherming en privacy waarborgt zonder in te boeten op functionaliteit en technische voordelen. Door onze consultatie bij de VTC konden we uiteindelijk een gepaste balans vinden tussen functionaliteit en privacy op onze zoektocht naar een cloudarchitectuur.

4.3.4 Fase 4: De afwerking door de DPO van KU leuven

Na ons overleg met de VTC legden we de laatste hand aan het document met onze conclusies van de GEB. Die finale versie werd gevalideerd door de DPO van imec en nog een laatste keer afgestemd met de DPO van KU Leuven en de DPO van het Departement Onderwijs en Vorming, waarna we ze uiteindelijk konden afkloppen.

4.3.5 Fase 5: de permanente follow-up

Belangrijk is dat de afwerking van onze GEB geen eindpunt was, maar een startpunt moest zijn voor een voortdurende privacymonitoring. Scholen kunnen het gebruiken om hun eigen risico's in kaart te brengen en hun verantwoordelijkheid als verwerkingsverantwoordelijke beter te begrijpen. Het i-Learn-team zal de laatste GEB ook regelmatig tegen het licht houden en indien nodig updaten, bijvoorbeeld als er nieuwe functionaliteiten aan het platform worden toegevoegd.

4.4 RESULTATEN VAN DE GEB

Wat hebben we uit onze GEB geleerd? Op basis van de GEB hebben we de gegevens die MyWay verwerkt, kunnen opdelen in drie categorieën:

- **De werkingsgegevens (categorie 1)**: dit zijn de absolute basisgegevens die MyWay verwerkt om het portaal te kunnen aanbieden aan leerkrachten en leerlingen. Tot deze categorie rekenen we onder andere identificatiegegevens en leerresultaten.
- **De optimalisatiegegevens (categorie 2)**: deze gegevens worden gebruikt om het MyWay-portaal te kunnen verbeteren, te optimaliseren. Daartoe behoren onder andere feedback en gebruikersstatistieken.
- **De onderzoeksgegevens (categorie 3)**: deze gegevens worden verzameld met het oog op wetenschappelijk onderzoek naar bijvoorbeeld digitaal gepersonaliseerd leren. Zoals eerder aangegeven behoorden die niet tot de scope van onze GEB.

Voor elke categorie hebben we een korte analyse van de gegevensverwerking gemaakt, onder meer op basis van de rechtmatigheid en de doelbinding ervan:

Categorie 1: de werkingsgegevens

Voor deze categorie is de school de verwerkingsverantwoordelijke en i-Learn MyWay de verwerker. Daarom wordt de rechtsgrond voor verwerking van werkingsgegevens meestal vanuit de school bepaald. Afhankelijk van het type school raden we aan om vanuit de rechtsgrond van 'gerechtvaardigd belang' of 'algemeen belang' te vertrekken.

Na het bepalen van de rechtsgrond sluit de school een verwerkersovereenkomst met i-Learn MyWay af, waarin ook de plichten van i-Learn worden neergeschreven. i-Learn belooft daarin de verwerking van persoonsgegevens te zullen beperken tot wat strikt noodzakelijk is en de toegang ertoe te zullen begrenzen tot de personen die de persoonsgegevens nodig hebben om de werking van i-Learn optimaal te houden. In die verwerkersovereenkomst moet i-Learn ook transparant zijn over de tools die ze de schools laat gebruiken. Daarbij komt kijken dat de verwerkingsverantwoordelijke een privacystatement moet aanvaarden voor elke gekoppelde tool.

Categorie 2: de optimalisatiegegevens

Voor deze categorie is i-Learn MyWay de verwerkingsverantwoordelijke. De rechtsgrond voor de verwerking van deze gegevens is het gerechtvaardigd belang van i-Learn MyWay om het portaal te optimaliseren en te innoveren. i-Learn verbindt zich er altijd toe om het belang van gegevensverwerking van deze tweede categorie telkens goed af te wegen tegenover de potentiële impact voor zijn gebruikers.

Categorie 3: de onderzoeksgegevens

Ook voor deze categorie gegevens ligt de bal in het kamp van i-Learn. Afhankelijk van het type onderzoek dat er gevoerd moet worden, roept i-Learn de rechtsgrond toestemming en/of algemeen belang in. Het onderzoek wordt vooraf steeds geëvalueerd door de Sociaal-Maatschappelijke Ethische Commissie (SMEC) van KU Leuven en de betrokken privacy offices, en kan pas worden gestart als alle nodige toestemmingen zijn verkregen.

Om welk soort gegevens het ook gaat, en wie ook de verwerker is, voor de verwerking van persoonsgegevens bij al deze categorieën kiezen we resoluut voor de meest privacyvriendelijke aanpak. Alleen wie de gegevens echt nodig heeft voor een duidelijk doel, krijgt er toegang toe.

4.5 CONCLUSIE NA DE GEB

Met het GEB-traject hebben we de privacyrisico's van i-Learn in kaart kunnen brengen. We hebben gekeken naar mitigatiestrategieën en die zover mogelijk al geïmplementeerd. We hebben ook stappen gezet om het bewustzijn rond privacy in het onderwijs bij de stakeholders van i-Learn te verhogen.

De belangrijkste bevindingen van het GEB-traject zijn dat:

- de bewustwording met betrekking tot privacy verhoogd is bij alle betrokken partijen. We merken dat het meer *top of mind* is geworden van alle stakeholders, dat wil zeggen zowel de medewerkers aan het i-Learnproject, de stakeholders van de onderwijsinstellingen als de leveranciers van de digitale leermiddelen.

- een tekortschieten in de naleving van de AVG veelal niet voortkomt uit een gebrek aan goede intenties, maar eerder uit onwetendheid, tijdsdruk of schaarste aan middelen. Richtlijnen en advies geven was meestal al voldoende om hun gegevensverwerkingen in lijn te brengen met de AVG, zonder dat er ingrijpende aanpassingen nodig waren.

- het inzetten van cloudinfrastructuur een onontbeerlijk element is bij het aanbieden van digitale leermiddelen. Echter brengt dat tevens een aanzienlijke toename van complexiteit met zich mee als gevolg van de ingewikkelde regelgeving die daaraan verbonden is.

- het bieden van gepersonaliseerd onderwijs op de lange termijn een uitdagende taak zal blijven op vlak van gegevensbescherming. Dit komt omdat de vraag naar personalisatie alleen maar zal toenemen, waardoor ook de mogelijke privacyrisico's groter worden. Om deze kwestie aan te pakken en alle betrokken partijen op koers te houden, zijn voortdurende aandacht, tijd en middelen vereist.

Bronnen

Berghmans, M., Decuypere, M., & van de Oudeweetering, K. (2020, 17 april). *Wat is goed digitaal onderwijs?* Platform L. Geraadpleegd op 17 mei 2023, van https://ppw.kuleuven.be/platforml/blogs/2020/wat-is-goed-digitaal-onderwijs

Burgess, M. (2020, 24 maart). What is GDPR?: The summary guide to GDPR compliance in the UK. *Wired UK*. Geraadpleegd op 23 mei 2023, van https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Commissie voor de bescherming van de persoonlijke levenssfeer & Vlaamse Toezichtscommissie (Reds.). (2018). In 7 stappen naar gegevensbescherming in het onderwijs: Volgens de Algemene Verordening Gegevensbescherming (AVG) van de EU. In *onderwijs.vlaanderen.be*. Geraadpleegd op 12 april 2023, van https://onderwijs.vlaanderen.be/sites/default/files/2021-07/In-7-stappen-naar-gegevensbescherming-in-het-onderwijs_Privacycommissie.pdf

Data Protection Impact Assessment. (2021). privacycompany.eu. Geraadpleegd op 19 april 2023, van https://www.privacycompany.eu/knowledge-base-nl/data-protection-impact-assessment

De ArgumentenFabriek (Red.). (2016). Omgaan met data in het onderwijs: Van en voor bestuurders in po, vo en mbo. In *kennisnet.nl*. Geraadpleegd op 23 mei 2023, van https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Omgaan_met_data_in_het_onderwijs.pdf

De AVG in het onderwijs: dit moet je weten: Veelgestelde vragen uit het primair en voortgezet onderwijs. (2019). In *yoursafetynet.com*. Media Security Networks BV h/o YourSafetynet. Geraadpleegd op 24 mei 2023, van https://www.yoursafetynet.com/wp-content/uploads/2021/03/190523-YourSafetynet-AVG-vragenboekje-v5-Web.pdf

De Vlaamse Minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand. (2020). Visienota "Digisprong": Van Achterstand naar Voorsprong: ICT-plan voor een kwalitatief digitaal onderwijs in uitvoering van het relanceplan "Vlaamse veerkracht". In *publicaties.vlaanderen.be* (VR 2020 1112 DOC.1425/1QUATER). Geraadpleegd op 23 mei 2023, van https://publicaties.vlaanderen.be/view-file/40711

De Vlaamse Toezichtscommissie (Red.). (2022). Beslissing VTC nr. O/2020/01 van 14 januari 2020: betreffende aanname van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming door Vlaamse bestuursinstanties. In *overheid.vlaanderen.be*. Geraadpleegd op 10 mei 2023, van https://overheid.vlaanderen.be/vtc_dpia_lijst

Digitaal Vlaanderen (Red.). (z.d.). *Digitale overheid: Digisprong in het onderwijs: Aanbeveling VTC bij de Digisprong in het onderwijs*. overheid.vlaanderen.be. Geraadpleegd op 23 mei 2023, van https://overheid.vlaanderen.be/digitale-overheid/digisprong-in-het-onderwijs

Gegevensbeschermingsautoriteit (Red.). (2023). *Melding van gegevenslekken: Een lek van persoonsgegevens melden*. gegevensbeschermingsautoriteit.be. Geraadpleegd op 27 april 2023, van https://www.gegevensbeschermingsautoriteit.be/professioneel/acties/datalek-van-persoonsgegevens

Han, H. J. (2023). "How Dare They Peep into My Private Life?": Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic. In *Human Rights Watch*. Geraadpleegd op 23 mei 2023, van https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Heyman, R., De Wolf, R., & De Geest, C. (2019). Het privacy-abc. In S. Hermans, E. Boudry, K. Linten, & H. Vanwynsberghe (Reds.), *assets.mediawijs.be* (D/2019/13.815/7). v.u. imec vzw. Geraadpleegd op 23 mei 2023, van https://assets.mediawijs.be/2021-10/mediawegwijzer_privacy_herdruk19_def_lr.pdf

Human Rights Watch (Red.). (2022, 25 mei). Governments Harm Children's Rights in Online Learning: 146 Authorized Products May Have Surveilled Children and Harvested Personal Data. *Human Rights Watch*. Geraadpleegd op 5 april 2023, van https://www.hrw.org/news/2022/05/25/governments-harm-childrens-rights-online-learning

Imec (Red.). (2022, 19 januari). Vlaamse EdTech-start-ups moeten – letterlijk én figuurlijk – over de grenzen heen durven te kijken: Imec-experten belichten de groeikansen voor (jonge) Vlaamse EdTech-bedrijven. *imec.be*. Geraadpleegd op 23 mei 2023, van https://www.imec.be/nl/articles/vlaamse-edtech-start-ups-moeten-letterlijk-en-figuurlijk-over-de-grenzen-heen-durven-te

Intentieverklaring Privacy in Digitale Onderwijsmiddelen. (2018). In *privacyinonderwijs.be*. Geraadpleegd op 23 mei 2023, van https://www.privacyinonderwijs.be/Intentieverklaring.pdf

Jvh & Blg. (2022, 23 december). Facebook schikt schandaal rond Cambridge Analytica voor 725 miljoen dollar. *De Standaard*. Geraadpleegd op 10 januari 2023, van https://www.standaard.be/cnt/DMF20221223_96167690

Model Verwerkersovereenkomst. (2018). In *privacyinonderwijs.be*. Geraadpleegd op 23 mei 2023, van https://www.privacyinonderwijs.be/Modelovereenkomst.pdf

Persbericht 'Modelovereenkomst beschermt persoonsgegevens in onderwijs' (Door A. Berckmoes, A. De Graeve, N. Jennes, K. Thijssens, M. Van Bogaert, & L. Van der Stockt). (2018, 22 mei). [Persbericht]. https://www.mijnclb.be/informatieveiligheid/downloads/2018_05_22_persbericht_gdpr_def.pdf

Prinsloo, P. (2020). Big data in education. The digital future of learning, policy and practice. *International Studies in Sociology of Education*, *29*(1–2), 183–186. https://doi.org/10.1080/09620214.2019.1690546

Research Coordination Office KU Leuven. (2023, 2 februari). *Sociaal-Maatschappelijke Ethische Commissie (SMEC) - Social and Societal Ethics Committee*. research.kuleuven.be. Geraadpleegd op 30 mei 2023, van https://research.kuleuven.be/en/integrity-ethics/ethics/committees/smec/documenten/index2

Security.NL (Red.). (2022, 31 mei). *"Meeste online onderwijsplatforms delen kinderdata met advertentiebedrijven"*. Security.NL. Geraadpleegd op 5 april 2023, van https://www.security.nl/posting/755384/%22Meeste+online+onderwijsplatforms+delen+kinderdata+met+advertentiebedrijven#:~:text=De%20meeste%20online%20onderwijsplatforms%20waar,onderwijsplatforms%20die%20door%2049%20verschillende

Selwyn, N. (2015). Data entry: towards the critical study of digital data and education. *Learning, Media and Technology*, *40*(1), 64–82. https://doi.org/10.1080/17439884.2014.921628

Van der Stadt, K. (Red.). (2023, 9 maart). Vlaamse Toezichtcommissie geeft vernietigend advies over AWS (update 13/10). *datanews.knack.be*. Geraadpleegd op 5 juni 2023, van https://datanews.knack.be/nieuws/vlaamse-toezichtcommissie-geeft-vernietigend-advies-over-aws-update-13-10/

van Trigt, M. (2019). Hoe data de kwaliteit van het onderwijs kunnen verbeteren. In *surf.nl*. Geraadpleegd op 23 mei 2023, van https://www.surf.nl/files/2019-05/Whitepaper-Hoe-data-de-kwaliteit-van-het-onderwijs-kunnen-verbeteren-2019.pdf

Verordeningen: Verordening (EU) 2016/679 van het Europese Parlement en de Raad: betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). (2016, 27 april). Geraadpleegd op 9 januari 2023, van https://eur-lex.europa.eu/eli/reg/2016/679/oj

Visienota "Digisprong": Van Achterstand naar Voorsprong: ICT-plan voor een kwalitatief digitaal onderwijs in uitvoering van het relanceplan "Vlaamse veerkracht". (2020). In *publicaties.vlaanderen.be* (VR 2020 1112 DOC.1425/1QUATER). De Vlaamse Regering - De Vlaamse Minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand. Geraadpleegd op 23 mei 2023, van https://publicaties.vlaanderen.be/view-file/40711

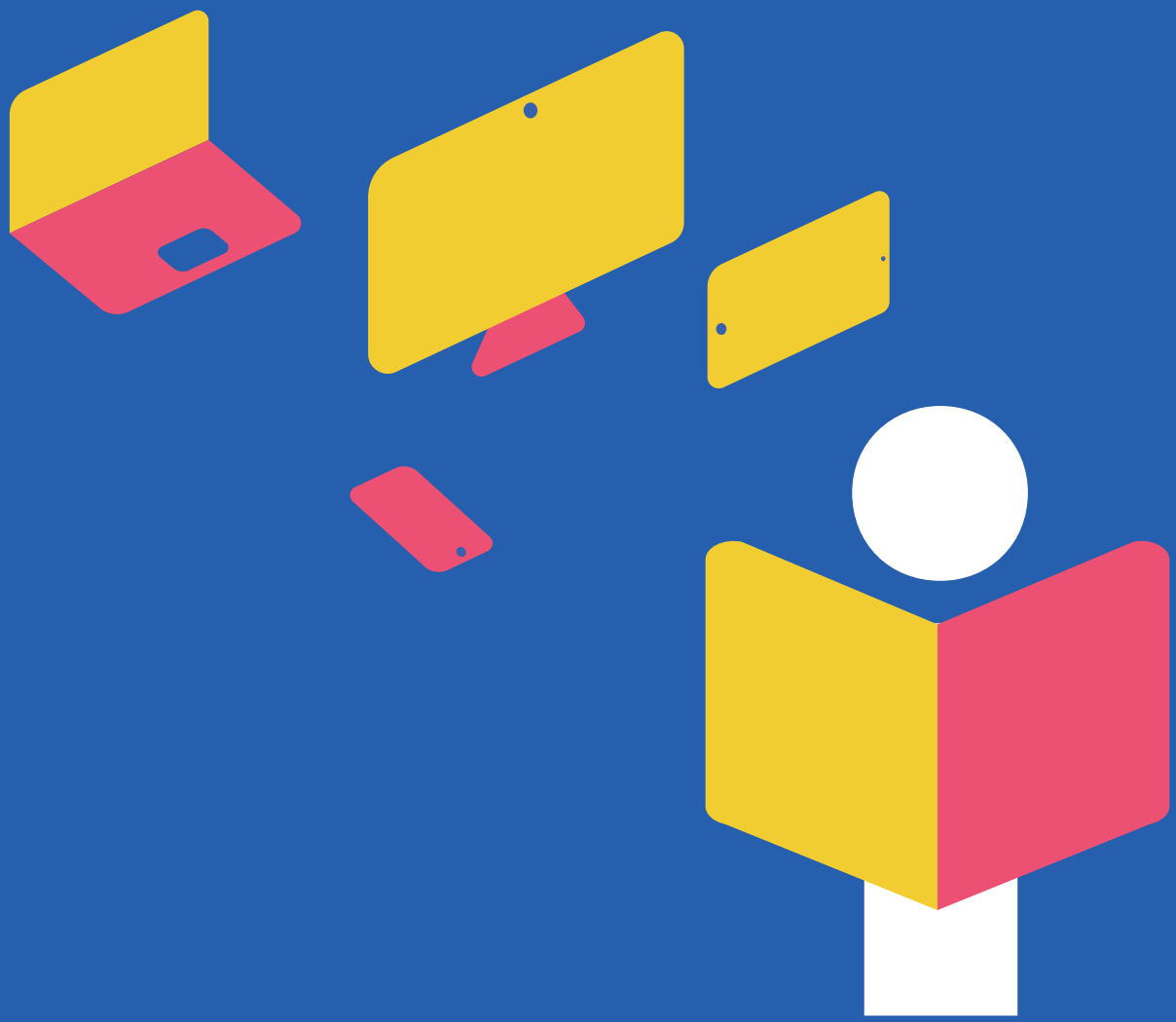
Vlaams ministerie van onderwijs en vorming (Red.). (2003). Bewaartermijn van leerlinggebonden documenten: SO/2003/02. In *data-onderwijs.vlaanderen.be*. Geraadpleegd op 23 mei 2023, van https://data-onderwijs.vlaanderen.be/edulex/document.aspx?docid=13366

Wegwijs in de AVG voor Onderwijsinstellingen: Uitgebreide technische brochure. (2018). In *privacyinonderwijs.be*. Geraadpleegd op 17 april 2023, van https://www.privacyinonderwijs.be/TechnischeBrochure.pdf

Wegwijzer GDPR/AVG. (2022). In *assets.vlaanderen.be*. Geraadpleegd op 25 mei 2023, van https://assets.vlaanderen.be/image/upload/v1664979613/wegwijzer_-_GDPR-AVG_q1qyel.pdf

i Learn

DIGITAAL LEREN
OP MAAT



INFO@I-LEARN.VLAANDEREN | WWW.I-LEARN.VLAANDEREN | WWW.I-LEARN.BE

in opdracht van

imec KU LEUVEN itec brightlab shaping future innovators IDLab INTERNET & DATA LAB

Vlaanderen verbeelding werkt