Overstapservice: Informatiebeveiliging en privacy

wat een school moet weten bij het gebruik van OSO

Versie 3.0
Auteurs: Debby Sikking, Job Vos, Elly Dingemanse (Kennisnet)

Informatiebeveiliging en privacy

Overal op school worden persoonsgegevens gebruikt. Als het over persoonsgegevens gaat, bedoelen we alle gegevens waarmee direct of indirect een natuurlijk persoon (zoals een leerling of een medewerker) kan worden geïdentificeerd. Het kan bijvoorbeeld gaan om een naam, BSN, geboortedatum, telefoonnummer of IP-adres. Bijzondere persoonsgegevens zijn persoonsgegevens die extra “gevoelig” zijn. Denk aan informatie over gezondheid, gedragsproblemen, godsdienst, seksuele voorkeur of een problematische thuissituatie. Het gebruik van deze bijzondere persoonsgegevens is niet altijd toegestaan en vraagt extra aandacht en beveiligingsmaatregelen van de school.

Ook bij het gebruik van OSO worden (bijzondere) persoonsgegevens gebruikt. Het is belangrijk de privacy van leerlingen bij het gebruik van deze persoonsgegevens te waarborgen. Met privacy bedoelen we het respecteren en beschermen van het privéleven van de natuurlijke personen zoals leerlingen op school.

Om de OSO op een juiste en rechtmatige manier te gebruiken, moet niet alleen de privacy van de leerlingen gegarandeerd worden maar ook de juistheid en vertrouwelijkheid van de gegevens moet goed geregeld zijn (informatiebeveiliging). Deze publicatie legt uit wat de school moet regelen op het gebied van informatiebeveiliging en privacy in het kader van uitwisseling van gegevens via OSO.

Overstapservice Onderwijs

Om ervoor te zorgen dat leerlingen in het basisonderwijs op hun nieuwe school de juiste ondersteuning en begeleiding krijgen, is in de ‘Wet op het primair onderwijs’ geregeld dat de basisschool, de nieuwe school voorziet van een onderwijskundig rapport (OKR). Bij de overstap naar de middelbare school wordt dit ook wel overstapdossier genoemd. Na overleg met het onderwijzend personeel wordt dit rapport opgesteld door de directeur. Het OKR moet een goede, doorlopende leerlijn voor elke leerling garanderen.

De ‘Wet op het voorgezet onderwijs’ kent een overstapdossier. Het gaat daarbij om het contact met een andere school of instelling voor ander onderwijs, ten behoeve van de in- en uitschrijving van die leerling. Onder dit contact wordt mede begrepen de uitwisseling van leergegevens en direct met het leren samenhangende begeleidingsgegevens. Met de Overstapservice Onderwijs (OSO) draag je als school het overstapdossier van de leerling digitaal veilig en snel over.

Door het gebruik van OSO, is een deel van de privacy van de leerlingen goed geregeld. Wat er nog meer op orde moet zijn lees je hieronder.

☐ Regel informatiebeveiliging en privacy (IBP) op school goed.

Het regelen van informatiebeveiliging en privacy op school klinkt moeilijker dan het is. Kennisnet heeft hiervoor, in overleg met de PO-Raad en VO-raad, een praktische aanpak online beschikbaar gesteld. In de Aanpak IBP hebben we een aantal punten op een rij gezet, die voor jou van belang zijn, ook wanneer je OSO gebruikt.
Een aantal punten zijn van belang wanneer je de school wilt aansluiten op OSO.

Deze punten zijn:

1. Weet waar privacy over gaat
2. Sluit met iedere leverancier die persoonsgegevens verwerkt, een verwerkingsovereenkomst
3. Informeer ouders over de omgang met persoonsgegevens van hun kinderen en uitwisseling via OSO
4. Zorg voor inzage of toestemming voor uitwisseling van leerlinggegevens via OSO
5. Zorg voor afspraken bij overdracht van het overstapdossier (dataminimalisatie)
6. Beveilig door de school verwerkte persoonsgegevens.

☐ Weet waar privacy over gaat (samenvatting)

Privacy draait om het beschermen van een ieders privéleven, het beschermen van persoonsgegevens (die informatie die “iets” over “iemand” zegt) is daar onlosmakelijk mee verbonden.

Juridisch kader verwerken persoonsgegevens

Het Europees parlement stemde in 2016 in met de **Algemene Verordening Gegevensbescherming** (AVG). Deze nieuwe wetgeving sluit aan op technologische ontwikkelingen en globalisering en is sinds 25 mei 2018 van kracht. Dat betekent dat er vanaf die datum nog maar één privacywet geldt in de hele Europese Unie (EU). De (huidige) Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.
Als de AVG van toepassing is, hebben organisaties die persoonsgegevens verwerken meer verplichtingen. Er wordt in de AVG meer nadruk gelegd op de verantwoordelijkheid van organisaties zelf om de AVG na te leven én om te kunnen aantonen dat zij zich aan de AVG houden.

De AVG kent drie belangrijke rollen:

1. De ‘**verwerkingsverantwoordelijke**’ (in de Wbp de ‘verantwoordelijke’) stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Het gaat hier om de persoon of instantie die formeel en juridisch het initiatief neemt tot het verzamelen van persoonsgegevens en daarvoor ook verantwoordelijk is. In het onderwijs is dit vaak de directie of het bestuur van de rechtspersoon waar de school onder valt: het bevoegd gezag.

   Voor de leesbaarheid van deze publicatie gebruiken we het begrip ‘school’. Hiermee bedoelen we eigenlijk de verwerkingsverantwoordelijke: ‘het bevoegd gezag waar de betreffende school onder valt’.

2. De **‘verwerker’** (in de Wbp de ‘bewerker’ genoemd) verwerkt de persoonsgegevens namens de verwerkingsverwerkingsverantwoordelijke.
   Dit is bijvoorbeeld een aanbieder van leermiddelen of een leverancier van een leerlingadministratie-systeem (LAS). De verwerker handelt in opdracht van de verwerkingsverwerkingsverantwoordelijke en mag *alleen* verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt.

3. De ‘**betrokkene’** is de persoon over wie de persoonsgegevens gaan: in het onderwijs is dit meestal de leerling, maar persoonsgegevens kunnen natuurlijk ook iets over medewerkers zeggen.

Uitgangspunt van de AVG is dat het bevoegd gezag, als verwerkingsverantwoordelijke, eindverantwoordelijk is voor de privacy van leerlingen. De verwerkingsverantwoordelijke is verplicht om volgens de wet te handelen en daarbij behoorlijk en zorgvuldig te werk gaan. De wet biedt scholen gelukkig genoeg ruimte om persoonsgegevens te gebruiken: binnen de kaders van de wet is er veel mogelijk.

Scholen hebben de regie op wat er gebeurt met de persoonsgegevens. Dit mag *niet* worden overgelaten aan een verwerker (‘leverancier’). Die verantwoordelijkheid houdt ook in dat scholen ouders en leerlingen volledig moeten informeren over het gebruik van persoonsgegevens én hoe ouders gebruik kunnen maken van hun rechten. Dit kan bijvoorbeeld op basis van gegevens van leveranciers.

☐ Maak afspraken met leveranciers: sluit verwerkingsovereenkomsten

Voor en door de uitwisseling van leerlingdossiers via OSO is het nodig om persoonsgegevens uit te wisselen met uitgevers en andere leveranciers (verwerkers). Belangrijk is dat er met elk van deze verwerkers – voor de uitwisseling van de persoonsgegevens – juridische afspraken worden gemaakt over wat de verwerker wél en niet mag met de persoonsgegevens. Deze afspraken worden vastgelegd in een overeenkomst dat we een **verwerkingsovereenkomst** noemen. Zo'n verwerkingsovereenkomst is wettelijk verplicht.
Het belangrijkste uitgangspunt is dat de verwerker alleen verwerkingen uitvoert in opdracht van de school, dit wordt ook vastgelegd in de verwerkingsovereenkomst. De leverancier mag de ontvangen persoonsgegevens niet voor iets anders gebruiken, doorverkopen of bijvoorbeeld contact opnemen met de ouders om bijvoorbeeld reclame te maken voor extra lesmateriaal. Soms nemen verwerkers zelf het initiatief om een verwerkingsovereenkomst op te stellen, maar de school blijft verantwoordelijk voor de aanwezigheid en inhoud van de verwerkingsovereenkomst.

In 2015 hebben de PO-Raad, VO-raad, uitgevers (GEU), softwareleveranciers (vDOD) en distributeurs van digitaal leermateriaal (KBb-e) het convenant 'Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen' ondertekend. Alle leveranciers die bij deze partijen zijn aangesloten, leveren op dit moment gezamenlijk zo'n 95 procent van alle beschikbare producten voor scholen. Dit convenant zorgt ervoor dat de scholen de regie hebben over wat er gebeurt met de gegevens die worden verwerkt bij het gebruik van digitale leermiddelen. Het convenant concretiseert hiermee veel verplichtingen voor scholen die voortvloeien uit de AVG. Op deze manier worden scholen ontzorgt: het helpt ze bij het maken van de juiste afspraken met hun verwerkers.

Bij het convenant hoort een '**Model Verwerkingsovereenkomst**'. Hierin maakt de school met de leverancier afspraken over welke verwerkingen de leverancier in opdracht van de school doet en welke persoonsgegevens hiervoor gebruikt worden. In de verwerkingsovereenkomst staat ook welke beveiligingsmaatregelen de leverancier treft om de veiligheid van de door hem verwerkte persoonsgegevens te waarborgen. Deze afspraken zijn juridisch afdwingbaar. Alle leveranciers die het convenant 'Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen' hebben ondertekend, zijn verplicht om deze Model Verwerkingsovereenkomst te gebruiken. Afwijken van dit model kán, maar is niet wenselijk. Eventuele aanpassingen moeten dan ook in een extra bijlage gemotiveerd worden. Door ondertekening van de verwerkingsovereenkomst bekrachtigen de school en de leverancier dat zij zich aan de afspraken houden die in het convenant staan beschreven.

De huidige 3.0-versie uit maart 2018 kent een verbreding van de eerdere afspraken ten aanzien van leerling- en schooladministratiesystemen. De bij het convenant behorende model verwerkingsovereenkomst 3.0 bevat naast een verbreding ook een aan de laatste ontwikkelingen bijgewerkte tekst, mede in verband met de wettelijke regeling over melding van datalekken.

Bij de Model Verwerkingsovereenkomst hoort een bijlage, de '**privacybijsluiter'**. Hierin leggen de school en leverancier vast met welk doel de verwerking van persoonsgegevens plaatsvindt, wat de dienstverlening van de leverancier omvat en wat de producteigenschappen van de dienst zijn. Daarnaast staat er beschreven welke categorieën persoonsgegevens de leverancier verwerkt. De leverancier vult de privacybijsluiter in. De school gaat na of alles klopt en besluit uiteindelijk om wel of niet akkoord te gaan met de voorgestelde afspraken.

Een nadere uitleg van het convenant en de Model Verwerkingsovereenkomst is te lezen in de Aanpak IBP van Kennisnet (https://kn.nu/ibponderwijs)

OSO en verwerkingsovereenkomst

Voordat er gebruik kan worden gemaakt van OSO, moet de school een verwerkingsovereenkomst hebben gesloten met de leverancier die zorgt voor de uitwisseling via OSO. Partijen dienen hierbij gebruik te maken van de 'Model Verwerkingsovereenkomst'.

☐ Informeer ouders over het gebruik van OSO

De school is verplicht om de ouders goed te informeren hoe er wordt omgegaan met de persoonsgegevens van leerlingen. Met betrekking tot het gebruik van OSO kan de school dit doen door bijvoorbeeld door:

- In het privacybeleid van de school in algemene bewoordingen uit te leggen dat OSO wordt gebruikt (bijvoorbeeld in het **privacyreglement** en/of beleidsdocument privacy). Ook kan op het inschrijfformulier, of tijdens de informatieavond voor groep 8 op het gebruik van OSO worden ingegaan. Deze informatie wordt (ook) in de schoolgids en/of op de website opgenomen.

- Bij uitwisselingen van leerlinggegevens, zoals bij de uitwisseling via OSO, dienen de ouders vooraf geïnformeerd te worden over hoe de uitwisseling plaatsvindt.

☐ Zorg voor inzage of toestemming voor de uitwisseling met OSO

Primair onderwijs: inzage

Voor de uitwisseling van het OKR tussen de basisschool en de nieuwe school (po of vo), is geen toestemming van ouders nodig. Ze kunnen dus ook geen bezwaar maken tegen de uitwisseling van het OKR: de school moet het OKR hoe dan ook uitwisselen.
Wel moeten de ouders inzage krijgen in het OKR, voordat deze wordt uitgewisseld. Professionele indrukken van leraren kunnen niet gecorrigeerd worden, maar bezwaren en opmerkingen van de ouders moeten wel opgenomen worden in het OKR. De school moet de gegeven inzage ook vastleggen. Dit kan op verschillende manieren:

- Bewaar een kopie van de brief aan de ouders.
- Maak een verslag van het gesprek tussen de leraar en de ouders.
- Registreer de datum (en tijd) van de (mondeling) gegeven toestemming.
- Plaats na het gesprek met de ouders een vinkje bij ‘inzage’ in de LAS.

Door dit schriftelijk vast te leggen in het leerlingdossier, maakt de school controleerbaar dat de wettelijke informatieplicht is nageleefd.

Na enige discussie in de Tweede Kamer, is besloten om in het primair onderwijs een (centrale) eindtoets in te voeren en om scholen te verplichten voor 1 maart het schooladvies te geven omtrent het volgen van aansluitend voortgezet onderwijs. Het schooladvies maakt formeel deel uit van het OKR en daarom hebben ouders dus alleen recht tot inzage in dit schooladvies. Het uitwisselen van het OKR en het schooladvies tussen de po-school en de vo-school is verplicht. Ook wanneer de ouders het hier niet mee eens zijn.

Voortgezet onderwijs: toestemming

Anders dan op de basisschool, moet een middelbare school voor de uitwisseling van een OKR (of andersoortig overstapdossier) wél toestemming hebben van de ouders. Deze toestemming is nodig voor de uitwisseling van het OKR tussen de vo-school en een nieuwe school (vo, mbo of hoger onderwijs). Ouders moeten natuurlijk ook inzage hebben gehad voordat ze toestemming kunnen geven voor een uitwisseling.

Ouders kunnen in dit geval wel bezwaar maken tegen de uitwisseling van die informatie: bij bezwaar tegen de uitwisseling kan de school uiteraard het gesprek met de ouders aangaan, maar zonder toestemming mag het OKR niet worden uitgewisseld.

De school die het OKR uitwisselt, moet een verklaring van toestemming van de ouders in de administratie bewaren. Dit is een wettelijke verplichting. Door gebruikt te maken van een schriftelijke toestemming, kan de school altijd aantonen dat er toestemming voor uitwisseling is gegeven.

Inzage, toestemming en OSO

Bij het gebruik van OSO, hebben de leveranciers afgesproken dat er wordt gecontroleerd of de school in de administratie wel het veld ‘inzage’ of ‘toestemming’ heeft ingevuld. Er wordt (nog) gecontroleerd of er een geldige datum is ingevoerd. Op deze manier dwingt het systeem dus af dat de school bewust het veld inzage of toestemming heeft ingevuld.

☐ Dataminimalisatie: niet meer persoonsgegevens dan nodig

Wat is dataminimalisatie?

Bij beveiliging wordt geregeld dat er niet meer mensen toegang tot bepaalde persoonsgegevens dan strikt noodzakelijk. Voorbeeld: een conciërge die ouders moet kunnen bellen in geval van ziekte, heeft geen toegang nodig tot cijfers of het leerlingbegeleidingssysteem. Een intern begeleider zal juist wel toegang moeten hebben tot die informatie of zelfs tot medische informatie. De gehele leerlingenadministratie toegankelijk maken voor alle medewerkers, lijkt een snelle en praktische oplossing maar de AVG vraagt scholen om verder te denken en om de toegang te beperken tot de personen die de informatie nodig hebben. Zo wordt er ook wel gesproken over een ‘autorisatiematrix’: wie heeft toegang nodig tot welke persoonsgegevens?

In het geval van een overdracht van een OKR of overstapdossier, is er door de wetgever in een apart besluit vastgelegd wat de school mag uitwisselen. Er mag niet meer worden uitgewisseld dan strikt noodzakelijk is voor het leren en begeleiden van de leerling op de nieuwe school. Het uitgangspunt is niet om zo min mogelijk gegevens uit te wisselen: de oude school mag niet het gehele leerlingdossier (ongezien) doorsturen, maar alleen die gegevens die men relevant vindt voor de nieuwe school. Dit noemen we ‘**selectief uitleveren**’. Hierbij gaat het om een specifieke set gegevens die de docent/directeur (van de oude school) heeft geselecteerd. Het systeem dat de uitwisseling faciliteert, moet hierin dus voorzien. Er kan niet worden uitgewisseld met ‘één druk op de knop’; de latende school moet selecteren welke gegevens verzonden moeten worden. Dit sluit aan bij het wettelijke uitgangspunt van dataminimalisatie.

OSO en dataminimalisatie

Om te voorkomen dat iedere leerlingadministratie andere ‘velden’ en definities gebruikt in het uit te wisselen leerlingdossier, is er een gegevensstandaard ontwikkeld: de **OSO-gegevensset**. Hierdoor maken alle leveranciers en scholen gebruik van een standaard set met gegevens. In deze OSO-gegevensset van Edustandaard staat welke gegevens wel en niet gebruikt mogen worden bij de overdracht aan een andere school.

OSO maakt gebruik van de standaard **OSO-gegevensset.** Daarmee wordt er voorkomen dat er onbedoeld teveel of onjuiste gegevens worden uitgewisseld. Met de leveranciers, die zijn aangesloten bij OSO, wordt overleg gevoerd om het voor alle scholen mogelijk te maken om in de verschillende administratiesystemen zelf de velden te kiezen die wel (of juist niet) uitgewisseld mogen worden. Dit ‘selectief uitleveren’ sluit volledig aan bij het wettelijk uitgangspunt van dataminimalisatie.

☐ Beveilig de gegevens

Zorgvuldig omgaan met persoonsgegevens vraagt om een goede beveiliging. Scholen zijn wettelijk verplicht om persoonsgegevens te beveiligen tegen risico's zoals verlies, onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens.

De AVG gaat ervan uit dat persoonsgegevens beveiligd zijn volgens de ‘stand van de techniek’. Het gaat daarbij om algemeen geaccepteerde en toegepaste organisatorische en technische beveiligingsnormen. Dit geldt voor de school (de verwerkersverwerkingsverantwoordelijke), maar de school moet deze eis ook opleggen aan de leveranciers (de verwerkers).

Ook bij OSO is aan beveiliging gedacht: de uitwisseling van gegevens vindt plaats via de LAS-leverancier van de school. Iedere leverancier, die OSO wil gebruiken, moet OSO-gecertificeerd zijn en dus voldoen aan de eisen is van OSO. Hiermee zorgt OSO voor een bepaalde minimum set aan beveiligingsmaatregelen waar iedere leverancier aan moet voldoen. Hierdoor wisselen (de leveranciers van) de scholen met elkaar het overstapdossier digitaal én veilig uit.

Uitzondering

Bij uitwisselingen tussen scholen en bijvoorbeeld **samenwerkingsverbanden** (in het kader van Passend Onderwijs) gelden er beperkingen. Zo heeft het ministerie van OCW met de Tweede Kamer bepaald dat de uitwisseling tussen een school en een samenwerkingsverband altijd op individuele basis gebeurt. Het gaat daarbij maar om één leerling. Daarom is besloten dat samenwerkingsverbanden géén PGN of BSN toepassen om een dossier aan te duidden. Digitale uitwisselingen tussen samenwerkingsverbanden en scholen geschiedt dus aan de hand van bijvoorbeeld geboortedatum en naam of via OSO met een tijdelijke sleutel verstuurd kan worden.