Wanneer je met privacy aan de gang gaat, kom je al gauw uit bij de term verwerkersovereenkomst. Wat houdt dit in?

De AVG maakt onderscheid tussen twee partijen: de verwerkingsverantwoordelijke en de verwerker. De verwerkingsverantwoordelijke is degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. De verwerker is de partij die ten behoeve van/in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het hangt dus af van de feitelijke situatie wie de verwerkingsverantwoordelijke is.

Is de onderwijsinstelling de verwerkingsverantwoordelijke? Wat betekent dat?

In de praktijk zal in veel gevallen de onderwijsinstelling dan ook te benoemen zijn als verwerkingsverantwoordelijke. Het belang van het onderscheid tussen verwerkingsverantwoordelijke en verwerker ligt in het verschil in verplichtingen en verantwoordelijkheden die beide kwalificaties met zich mee brengen. Zo hebben verwerkingverantwoordelijken bijvoorbeeld een verantwoordingsplicht om aan te tonen dat zij aan de AVG voldoen.

De verwerker en de verwerkingsverantwoordelijke dienen bepaalde afspraken vast te leggen. De verwerkersovereenkomst is de overeenkomst tussen verantwoordelijke en verwerker, waarin wordt vastgelegd hoe de verwerker met de persoonsgegevens moet omgaan.In de verwerkersovereenkomst worden zaken als de aansprakelijkheid, bewaartermijnen, rechten en verplichtingen en alle informatie omtrent de verwerking vastgelegd. Als een verwerkingsverantwoordelijke persoonsgegevens laat verwerken door een verwerker, is altijd een verwerkersovereenkomst tussen beide partijen verplicht. Beide partijen zijn ervoor verantwoordelijk dat de verwerkersovereenkomst wordt afgesloten.

Waar moet ik op letten bij een verwerkersovereenkomst?

Een aantal tips waar de onderwijsinstelling zelf, voorafgaand aan de beoordeling, naar kan kijken:

- Bekijk of er wordt voldaan aan de eisen van art. 28 AVG;
- Op grond van art. 28 AVG dient je binnen de verwerkersovereenkomst tenminste de volgende zaken af te spreken:
    - het onderwerp en de duur van de verwerking;
    - het doel en de aard van de verwerking;
    - het soort persoonsgegevens waarop de verwerkersovereenkomst betrekking heeft;
    - de categorieën van verwerking van de betreffende betrokkenen;
    - de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Wanneer een verwerkersovereenkomst in de vorm van een convenant van toepassing is, let dan op het volgende:

- Wordt dit convenant in zijn geheel, zonder verwijderingen, toevoegingen of beperkingen gebruikt?
- Indien één of meerdere artikelen uit dit convenant niet van toepassing zijn, wordt dit dan in de verwerkersovereenkomst nadrukkelijk vermeld met motivatie van waarom is afgeweken van het convenant?

Je komt waarschijnlijk ook de term DPIA tegen. Wat is een DPIA en wanneer is dit verplicht?

Wanneer een verwerking van persoonsgegevens een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dan moet de onderwijsinstelling een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren. Zo'n DPIA moet in principe voorafgaand aan de invoering van de verwerking plaatsvinden. Echter, in het kader van de implementatie van de AVG moeten onderwijsinstellingen ook alle huidige processen die een hoog risico kunnen inhouden voor de rechten en vrijheden van natuurlijke personen door middel van een DPIA beoordelen.

Een DPIA onderzoekt en beoordeelt de effecten van een nieuwe verwerking. Te denken valt aan een project m.b.t. medische gegevens (bijvoorbeeld over allergieën bij leerlingen), het gebruik van beveiligingscamera's op het schoolterrein, een nieuw HR-systeem of nieuw leerlingvolgsysteem software. Een DPIA brengt verhoogde beveiligingsrisico's in kaart, die onderwijsinstellingen vervolgens op basis van deze rapportage kunnen minimaliseren.

Hoe ziet een DPIA eruit? Dit is staat er in een DPIA:

Volgens de AVG bevat de DPIA ten minste:

1. Een systematische beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die de verwerkingsverantwoordelijke aanvoert.
2. Een beoordeling van de noodzaak en evenredigheid van de verwerkingen in relatie tot de doeleinden.
3. Een beoordeling van de risico's voor de privacy van de betrokken onderwijsdeelnemers en medewerkers als gevolg van de onder 1 benoemde verwerking.
4. De beoogde maatregelen om de privacyrisico's te beperken (waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie).

Een DPIA uitvoeren kan een flinke klus zijn. Het is daarom de moeite waard om bij DPIA's van grote leveranciers of systemen samen op te trekken. Dit is bijvoorbeeld gebeurd bij Microsoft. In opdracht van de Rijksoverheid zijn de afgelopen jaren verschillende DPIA's uitgevoerd op een aantal Microsoftproducten. De uitkomsten van die DPIA's hebben geleid tot aanbevelingen die ook gelden voor het onderwijs. Ook bij de DPIA van Google is er door verschillende partijen samen opgetrokken.

Hoe kies ik welk bedrijf veilig omgaat met mijn gegevens?

Uit de ontwikkelingen rondom de Google-software voor onderwijs kunnen een aantal conclusies getrokken worden. Sectoren als het onderwijs zouden zich ten eerste af moeten vragen tot op welke hoogte zij afhankelijk willen zijn van één bedrijf voor al hun onlinediensten. Deze techbedrijven koppelen vaak al hun diensten aan elkaar onder het mom van 'gebruikersgemak en veiligheid'.

Als een systeem eenmaal geïmplementeerd is, is het vaak een zeer kostbaar en tijdrovend proces om over te stappen naar een ander proces. Een kritische houding bij de aanschaf van een softwarepakket is daarom essentieel. Daarnaast is het belangrijk dat onderwijsinstellingen de controle houden over hun dataverzameling. Zeker gelet op het feit dat het vaak gaat om minderjarige personen en gevoelige gegevens, bijvoorbeeld over hun gezondheid. Het hebben van een privacybeleid is een eerste stap, maar het daadwerkelijk naleven van dat beleid blijkt in de praktijk soms lastiger te zijn dan gedacht. Onderwijsinstellingen moeten niet alleen kritisch nadenken over privacy, maar daar ook voortdurend zelf actief mee bezig zijn. Dat voorkomt achteraf veel problemen.

Sinds corona is het voor veel onderwijsinstellingen een bekend begrip; online proctoring. Wat is online proctoring?

Online proctoring wordt ook wel “surveilleren op afstand” genoemd en maakt het mogelijk om online tentamens af te nemen door middel van software. Er zijn grofweg drie verschillende soorten proctoring software te onderscheiden:

1. De eerste variant is live proctoring waarbij iemand live tijdens het examen meekijkt en toezicht houdt. Dit kun je vergelijken met de situatie van fysieke surveillance op locatie, alleen zit de surveillant nu niet in dezelfde ruimte, maar houdt hij vanaf afstand toezicht op studenten door middel van camerabeelden. Gebeurt er iets ontoelaatbaars? Dan kan de surveillant direct ingrijpen;
2. De tweede variant houdt in dat er camerabeelden, audiofragmenten of logs worden opgeslagen, die vervolgens na het tentamen kunnen worden bekeken. Bij deze vorm kan pas achteraf worden geconstateerd of er sprake is van fraude;
3. De laatste variant is geautomatiseerde proctoring waarbij de software een deel van de fraudedetectie overneemt. De software geeft aan waar mogelijk fraude heeft plaatsgevonden. Om vast te stellen dat er inderdaad sprake is van fraude kunnen de opgenomen beeld- en audiofragmenten vervolgens achteraf worden gecontroleerd. Er is dus altijd een menselijke controle

Mag een onderwijsinstelling tijdens corona gebruik maken van proctoring software?

Ja, in ieder geval zolang de tentamens niet volledig op locatie kunnen plaatsvinden en zolang dit *noodzakelijk* is voor het uitvoeren van de publieke taak van de onderwijsinstelling.

Kan ik ook na corona gebruik maken van online proctoring?

Het gebruik van online proctoring biedt veel mogelijkheden om studenten (plaatsonafhankelijk) te toetsen en het onderwijs flexibeler in te vullen. Denk daarbij aan de situatie waarin Nederlandse studenten die tijdelijk in het buitenland studeren toch in Nederland een tentamen kunnen maken, topsporters die vanuit hun trainingskamp een tentamen kunnen maken en een ernstig zieke student die thuis tentamen kan doen. Post corona zal een onderwijsinstelling het gebruik van online proctoring vermoedelijk niet meer kunnen baseren op de grondslag dat dit noodzakelijk is voor haar publieke taak. Het ligt voor de hand dat onderwijsinstellingen in dat geval het gebruik van online proctoring moeten baseren op toestemming van de student (of wettelijke vertegenwoordiger).

Even wat anders: welke privacyregels gelden er voor cameratoezicht in en rond het schoolterrein?

Steeds meer onderwijsinstellingen willen gebruik maken van camera's, bijvoorbeeld om vernielingen of diefstal tegen te gaan. Cameratoezicht maakt echter een grote inbreuk op de privacy van leerlingen, docenten en bezoekers.

Daarom mogen onderwijsinstellingen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Zo zal een onderwijsinstelling moeten beoordelen of zij een gerechtvaardigd belang heeft bij cameratoezicht en of het ook noodzakelijk is om cameratoezicht in te zetten. De onderwijsinstelling zal daarbij een belangenafweging moeten maken tussen de (privacy)belangen van de leerlingen, docenten en bezoekers en het eigen belang op cameratoezicht. Ook moeten onderwijsinstellingen ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Een camera voor het schoolplein mag wel, maar een camera in bijvoorbeeld een toilet of kleedhokje mag niet.

Ook mogen camerabeelden niet langer worden bewaard dan noodzakelijk is.

Mag een onderwijsinstelling ook verborgen camera's ophangen?

Nee, in principe niet, maar er kunnen specifieke omstandigheden zijn waarin een onderwijsinstelling dit toch mag doen. Bijvoorbeeld het geval als de onderwijsinstelling duidelijke vermoedens van bijvoorbeeld diefstal of fraude door leerlingen of docenten heeft. Hiervoor gelden strengere voorwaarden dan voor "normaal" cameratoezicht. Zo zal onder andere een reglement cameratoezicht moeten vermelden wanneer de onderwijsinstelling gebruik kan maken van verborgen camera's en moet de medezeggenschapsraad ook toestemming geven voor het gebruik van verborgen camera's.

Mag een onderwijsinstelling foto's en/of filmpjes plaatsen van de leerlingen op eigen social media kanalen?

Wanneer op een foto een persoon herkenbaar staat afgebeeld, is dat een persoonsgegeven. Het plaatsen van zo'n foto op internet is een 'verwerking van persoonsgegevens' waarop de AVG van toepassing is. Dat betekent dat er toestemming nodig is om foto's te mogen maken en te publiceren. De leerlingen van 16 jaar of ouder moeten hun toestemming geven via een duidelijke, actieve handeling. Dit kan een mondelinge of schriftelijke verklaring of een duidelijke, bevestigende actie van de student zijn. Leg de toestemming vast, zodat de onderwijsinstelling later zou kunnen aantonen dat er geldige toestemming is gegeven. Wanneer een leerling jonger dan 16 jaar is, is de toestemming van de ouder of wettelijk vertegenwoordiger nodig. De toestemming moet aan drie voorwaarden voldoen:

1. De toestemming moet vrij en niet onder druk gegeven zijn.
2. De toestemming moet uitdrukkelijk en ondubbelzinnig zijn verleend.
3. De toestemming kan alleen worden gevraagd voor een specifieke verwerking en een specifiek doel. Bijvoorbeeld om via foto's en video's verslag te doen van een sportdag of schoolreisje

Als de leerling of ouder later zijn toestemming intrekt, dient de foto verwijderd te worden van social media. Daarnaast heeft het de voorkeur om foto's en filmpjes niet op sociale media te publiceren, maar in een beveiligd onderdeel van de website van de onderwijsinstellingen waarop leerlingen of ouders kunnen inloggen

Wat doe je als er data (persoonsgegevens) is gelekt? Welke stappen dient een onderwijsinstelling te zetten als er een datalek heeft plaatsgevonden?

1. Inhoudelijk beoordelen en onderzoeken van het datalek: in deze stap is het belangrijk om het datalek in kaart te brengen. Om wat voor soort datalek gaat het, wat is de oorzaak van het datalek, wanneer is het datalek ontstaan, wat voor soort gegevens zijn gelekt, hoeveel persoonsgegeven van hoeveel personen zijn er gelekt, van welke groep personen zijn persoonsgegevens gelekt, zijn er maatregelen getroffen om de gelekte persoonsgegevens (deels) ontoegankelijk te maken voor onbevoegden (zoals door versleuteling)? Maak hier een inschatting van de (mogelijke) risico's die het datalek oplevert.
2. Probeer het datalek onmiddellijk te beëindigen en neem maatregelen om de negatieve gevolgen te beperken: bijvoorbeeld door een laptop op afstand te wissen, een bestand offline te halen of een verkeerde ontvanger te vragen om te bevestigen dat de e-mail is verwijderd.
3. Melden datalek aan AP: de hoofdregel is dat een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens (AP). Een uitzondering op deze hoofdregel bestaat wanneer het onwaarschijnlijk is dat de inbreuk gevolgen en een risico voor de betrokkenen veroorzaakt. In dat geval hoeft het datalek niet gemeld te worden aan de AP, maar moet het datalek wel intern worden gedocumenteerd in het datalekregister. Moet het datalek wel gemeld worden? Dan dient dit binnen 72 uur te gebeuren. Deze termijn gaat in nadat de onderwijsinstelling van het (mogelijke) datalek kennis heeft genomen.

Let op: meldt de onderwijsinstelling een datalek ten onrechte niet bij de AP? Dan kan de AP een boete opleggen

4. Melden datalek aan betrokkenen: In sommige gevallen zal een datalek ook aan de betrokkenen (bijvoorbeeld leerlingen, ouders, docenten) moeten worden gemeld. Deze melding dient te worden gedaan wanneer de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Om te bepalen of een datalek een hoog risico oplevert voor de betrokkenen, moet de onderwijsinstelling onder andere kijken of het datalek kan leiden tot fysieke, materiële of immateriële schade voor de betrokkenen. Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.

Tip: als wordt gemeld aan betrokkenen, bewaar het bewijs van die communicatie en neem deze op in het datalekregister

Let op: de AP kan een boete opleggen als een onderwijsinstelling ten onrechte een datalek met een hoog risico verzwijgt voor de betrokkenen.

5. Registratie datalek in datalekregister: een onderwijsinstelling is verplicht om elk datalek intern te registreren in het eigen datalekregister. In dit datalekregister moeten alle belangrijke zaken rondom het datalek worden vermeld (feiten over de inbreuk, zoals de oorzaak van het datalek, de betrokken persoonsgegevens, de gevolgen van de inbreuk en de corrigerende maatregelen die zijn genomen). Dit datalekregister is handig voor de organisatie, maar dient ook als overzicht die de AP kan opvragen in het geval van een controle.

Tip: Het is aan te raden om bij elk inbreuk vast te leggen waarom is besloten om het datalek wel of niet te melden aan de AP en de betrokken personen.

6. Evalueren van het datalek en de genomen maatregelen
7. Datalekprotocol: het is aan te raden om intern een datalekprotocol op te stellen, zodat duidelijk is wie het aanspreekpunt is voor het melden van een datalek en hoe binnen de onderwijsinstelling wordt omgegaan met een datalek