Checklist: Hoe voldoe ik als school aan de nieuwe privacy-wet?

Vanaf 25 mei 2018 gaat de nieuwe wet AVG in. Dat betekent dat elke organisatie, (niet alleen in het onderwijs), zijn privacy-beleid kritisch tegen het licht dient te houden en dient aan te passen. Dit document is een praktische vertaling van hoe je als school zijnde goed voorbereid bent op de regels en plichten die je als school hebt met deze nieuwe wet. Ook vind je een handige checklist van items die je niet moet vergeten bij bepaalde momenten, zoals het aanmelden van een nieuwe leerling.

Algemene teaminformatie

- Uitgangspunt is dat jij alleen gegevens mag verwerken die je ook daadwerkelijk nodig hebt. Dat betekent in de praktijk dat je alleen toegang hebt tot de gegevens van leerlingen die direct onder jouw verantwoordelijkheid vallen. Denk hierbij aan het LAS, maar ook andere (software)-programma's waar leerlinggegevens in staan. De IB'er mag zodoende formeel gezien geen toegang hebben tot alle groepen binnen het LAS, maar slechts tot de leerlingen die, vanwege zorgbehoefte, (mede) onder haar verantwoordelijkheid vallen.
- Elke ouder heeft het recht om op elk moment toegang te vragen tot het (digitale) dossier van zijn/haar eigen kind. Houd er dus ook rekening mee bij de wijze van registreren en datgene wat je vermeldt in het dossier.
- Data waarop leerlinggegevens zijn vermeld, of waarop gegevens staan die direct aan betrokken personen bij de school gerelateerd zijn, mogen de school niet verlaten. Fysieke documenten worden opgeslagen in af te sluiten kasten/ruimtes en digitale documenten mogen niet op mobiele datadragers (zoals usb-sticks en externe harde schijven) worden opgeslagen.
- Vermoeden van datalek? Je bent verplicht dit bij je bestuur te vermelden. Als het goed is, hebben zij hiervoor een meldformulier. Een vermoeden kan genoeg zijn om een melding te maken; er is een protocol gemaakt waar in staat hoe hiermee wordt omgesprongen.
- Plaats geen foto's op eigen (privé) sociale media accounts en maak goede afspraken over de schoolbrede accounts. Met name over het plaatsen van foto's en naamsvermeldingen.

Communicatie

- Besteed jaarlijks (bijvoorbeeld in de eerste nieuwsbrief van het schooljaar) uitgebreid aandacht aan hoe de school er alles aan doet om privacy zo goed mogelijk te waarborgen. Dit kan eenvoudig met een overzichtje aan maatregelen die je aan de hand van dit document besluit te nemen.
- Vermeld op de website geen personen die betrokken zijn bij de school met naam en toenaam, tenzij dat strikt noodzakelijk is. Leerlingen worden hooguit bij voornaam vernoemd.
- Vermeld wél op je website hoe je als school omspringt met privacy en waar de geïnteresseerde betrokkenen documentatie kunnen vinden die (vaak) op stichtings- of bestuursniveau zijn vastgesteld.
- Een ouder geeft bij de aanmelding al dan niet toestemming voor het publiceren van beeldmateriaal. Per gebruikt medium moet een ouder apart kunnen kiezen of daarvoor wel of geen toestemming wordt verleend.
- Een ouder moet elk jaar actief gewezen worden op het feit om eerder gegeven toestemming in te trekken of te herzien.
- Bedenk je wanneer je je naam vermeld. Op uitingen namens de school is het niet altijd nodig om naam en toenaam van jou of je collega's te vermelden. 'Juf Lisette' is privacytechnisch sterker dan 'Lisette van Haperen'.

- Bedenk goed hoe je privacy-gevoelige gegevens, zoals namen en contactgegevens, vermeldt in documenten die op de website worden geplaatst. Denk daarbij bijvoorbeeld aan de nieuwsbrief.
- Verspreid geen lijsten waarop (persoonsgebonden) gegevens staan van andere ouders/verzorgers, bijvoorbeeld van klasgenoten. Ook niet wanneer hier in het verleden toestemming door de ouders voor is verleend.

Nieuw schooljaar

- ◯ Informeer ouders over de wijze waarop de school omspringt met privacy (afsluiten dossiers, beveiligde computers, beleidskeuzes bestuur). Elk schooljaar opnieuw!
- ◯ Wijs ouders op het beleidsdocument wat gepubliceerd is op de website van de school of de stichting.
- ◯ Bekijk intern: wie heeft toegang tot welke gegevens? Klopt dit nog? Zijn er wellicht personeelsleden niet meer werkzaam of hebben zij een andere functie gekregen? Daarop moet dan actie worden ondernomen.
- ◯ Laat ouders hun gegevens controleren, zodat eventuele aanpassingen kunnen worden doorgegeven. Hierop kun je thans aangeven dat zij de toestemming voor publicaties kunnen herzien. Dit kan op elk moment, maar je bent verplicht als school om de ouder hier jaarlijks actief op te wijzen.

Uitstapjes

- ◯ Zorg dat je documentatie (o.a. lijsten met contactgegevens van ouders) liefst digitaal bij je hebt, maar in elk geval niet verspreidt. Ook niet met ouders die als begeleiding meegaan.
- ◯ Breng ouders vooraf op de hoogte van de manier waarop jullie op dat moment bereikbaar zijn.
- ◯ Vanzelfsprekend de gangbare veiligheidsvoorwaarden bij het maken van een uitstapje: goede begeleiding, eventueel hesjes, herkenbaarheid en goede afspraken met de leerlingen.

Nieuwe leerling

- ◯ Geef de ouders bij de aanmelding per medium de keuze of hij/zij al dan niet toestemming geeft om beeldmateriaal van het kind te plaatsen. Denk hierbij aan de website, de schoolgids, sociale media die op school gebruikt worden, ouderportaal-apps, nieuwsbrief en posters voor bijvoorbeeld de open dag.
- ◯ Duid bij het inschrijfformulier waarvoor je de gegevens nodig hebt waar je om vraagt. Volgens de wetgeving mag je alleen de gegevens vragen die je echt nodig hebt om het onderwijs op jullie school te kunnen verzorgen. Tip: Wellicht heeft je LAS een standaard ‘bijsluiter/disclaimer’ met tekst en uitleg over de invulvelden.

Vertrekkende personeelsleden (ook vrijwilligers)

- ◯ Registreer nu alvast waar teamleden allemaal toegang toe hebben. Inlogcodes tot data, zoals het LAS, maar ook leerlingsoftware en bijvoorbeeld de website van de school.
- ◯ Vertrekt een teamlid? Stel hem dan vooraf op de hoogte per wanneer de toegang tot bovengenoemde systemen ontnomen wordt, zodat hij tijdig zijn eigen materialen kan veiligstellen. Het kopiëren van leerlinggegevens naar eigen systemen is daarbij uiteraard niet toegestaan.
- ◯ Stel de netwerkleverancier (indien van toepassing) op de hoogte dat een teamlid gaat vertrekken of is vertrokken, zodat zij ook gepaste acties kunnen ondernemen.
- ◯ Haal het betreffende teamlid uit het LAS van de school.

De AVG: wat kan echt niet meer?
Een opsomming van zaken die je écht zou moeten veranderen of aanpassen op het moment dat ze bij jou op school of in de klas voorkomen:

- Klassenlijsten op het prikbord, zichtbaar aan de muur, achter het vluchtplan of in de klassenmap. Kortgezegd mogen deze niet zomaar toegankelijk zijn voor iedereen die de school binnen loopt. Hetzelfde geldt voor alle andere fysieke documentatie waarop de gegevens van leerlingen staan, ook al gaat het hierbij 'slechts' om voor- en achternaam.
- Nu we het toch over die klassenmap hebben: een lijstje met wachtwoorden en inlogcodes hoort daar ook niet. Tip: heb je tegenwoordig erg handige apps voor, zodat je nog maar één wachtwoord hoeft te onthouden.
- En over wachtwoorden gesproken: zorg dat je wachtwoord tenminste hoofdletters, kleine letters en cijfers bevat. En nee; niet Welkom01 of iets dergelijks.
- Leerlingdossiers in open kasten; deze moeten afsluitbaar zijn. De dossiervorming vindt bij voorkeur digitaal plaats, en alles wat toch op papier moet, moet af te sluiten zijn.
- USB-sticks waarop leerlinggegevens staan. Bij voorkeur verdwijnen alle usb-sticks uit de school, maar als het alleen een usb-stick met wat kleurplaten en werkbladen is, is daar natuurlijk niet zoveel mis mee.
- Groepsapps of -chats met ouders zijn ook niet wenselijk. Het middel is te openbaar en ouders worden min of meer verplicht om deel te nemen, omdat zij anders informatie missen.
- Het printen of kopiëren van privacy-gevoelige gegevens, zoals dossiers of rapporten op afstand. Het gevaar is namelijk dat je deze 'vergeet' uit de printer te halen en ze daarmee voor iedereen letterlijk voor het oprapen liggen. Tip: zorg voor een inlogcode op het apparaat.
- Privé-apparaten (computers/tablets) gebruiken die niet in het netwerk van de school opereren. Onveilig en een verantwoordelijkheid die je als medewerker neemt voor zowel het apparaat als de gegevens die het bevat.
- Zelf foto's plaatsen op je eigen sociale media-accounts van leerlingen op school.

En wat wordt (als het goed is) door de stichting geregeld?

- Benodigde beleidsstukken over IBP, zoals een formeel beleidsplan en een handboek met een praktische inslag.
- Het aanstellen van een manager IBP die toeziet op de naleving en het actueel houden van gemaakte en te maken afspraken.
- Een format voor een risico-analyse op basis waarvan je kunt inschatten of je voldoet aan de privacy-normen.
- Een meldformulier voor het melden van een (vermoeden van) een datalek.
- Een afspraak met de netwerkleverancier over het automatisch vergrendelen van computersystemen na bijvoorbeeld 30 minuten van inactief gebruik.
- Een afspraak met de netwerkleverancier over het loggen van gegevens, het maken van back-ups en het instellen van vertrouwde websites die de school nodig heeft.
- Een alternatief voor usb-sticks, zodat jij veilig in de cloud kunt opslaan en er overal toegang toe hebt.
- Wellicht het allerbelangrijkst: communicatie naar school, medewerkers én ouders over hoe de stichting omgaat met deze wetgeving en de gevolgen daarvan op stichtings-, school en individueel niveau.

Checklist: heb ik alles geregeld?

Afspraken met de teamleden	
	Alle teamleden zijn op de hoogte van het feit dat zij geen usb-sticks of mobiele datadragers gebruiken voor documenten met leerling- of gevoelige informatie.
	Er is in de hele school geen klassenlijst meer te vinden met leerlinggegevens op een plaats die niet kan worden afgesloten (bijvoorbeeld een kast met slot)
	Namens de school worden geen documenten verspreid waarop leerlinggegevens, oudergegevens of gegevens van medewerkers staan zonder dat zij schriftelijk toestemming hebben gegeven.
	Wachtwoorden die niet voldoen aan de afgesproken minimale vereisten, worden aangepast aan dat niveau. (minimaal 8 tekens, min. 1 cijfer, min. 1 hoofdletter)
	Bij een (vermoeden van) een datalek of hack: melding maken bij directeur en meldformulier invullen. Alle medewerkers zijn hiervan op de hoogte.
	Op privé-devices (computers, tablets) worden geen gegevens opgeslagen die op schoolniveau horen te worden opgeslagen.
	Groepsapps worden opgeheven, hiervoor wordt een alternatieve communicatiemogelijkheid aangeboden.
	Mailinglijsten worden altijd verzonden als 'BCC', waardoor ouders elkaars e-mailadressen niet zien.
	Wachtwoorden zijn niet openbaar beschikbaar, bijvoorbeeld in klassenmappen of onder het beeldscherm van de pc.
	Niet namens de school communiceren met privé-emailadressen of op je eigen sociale media-accounts. Ook niet met je eigen 06- of privé-nummer.
Afspraken communiceren naar ouders	
	Ouders hebben te allen tijde de mogelijkheid om gegeven toestemming voor wat betreft foto- en videomateriaal in te trekken en worden hier jaarlijks actief op gewezen.
	Het is niet wenselijk dat ouders beeldmateriaal van klasgenoten van hun kinderen plaatsen op hun sociale media. De school neemt hierin geen verantwoordelijkheid, ook al zijn de foto's op school gemaakt. Wel heeft de school een signalerende functie.
	Wijs ouders ook actief over de vernieuwde (en aangescherpte) wetgeving rondom privacy. De website waarop ze hierover alles kunnen vinden is www.autoriteitpersoonsgegevens.nl.
Afspraken met de netwerkbeheerder	
	Op de printer zit een code/wachtwoord, waardoor de printjes of kopieën er pas uitkomen wanneer ik op het apparaat de code heb ingetoetst.
	Wanneer computers 30 minuten niet gebruikt worden, worden ze automatisch vergrendeld.
	Nagaan of alle personen die niet meer op de school werken of functioneren, uit het systeem zijn gehaald.
	Tot wanneer zijn back-ups beschikbaar en wie kunnen deze opvragen?
Afspraken met andere leveranciers	
	Je website-url beschikt over een SSL-certificaat, waarmee een versleutelde verbinding tot stand wordt gebracht.
	Met uitgevers van alle programma's waarbij leerlinggegevens worden bewerkt of verwerkt wordt een verwerkersovereenkomst aangegaan.
Overig	
	Pas je inschrijfformulier aan; per gebruikt medium kan een ouder apart toestemming geven of deze intrekken. (website, sociale media, schoolgids et cetera)
	Wie hebben er allemaal toegang tot de school, de dossierkast et cetera. Is het nodig om afspraken met verenigingen of gebruikers van het gebouw te herzien?