Vlaamse overheid

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens

Richtlijnen bij gebruik van digitale middelen in onderwijs[1]

voor directies en personeel van Vlaamse onderwijsinstellingen

Waarom: het risico

Wat de bescherming van gegevens van leerlingen en personeel betreft, is er het risico dat de informatie die opgenomen wordt in de toepassingen ooit verspreid raakt en dat dit de vermelde personen, maar eventueel ook andere betrokken personen, in verlegenheid en zelfs in moeilijkheden brengt. Dit blijkt ondermeer uit de regelmatige meldingen van inbreuken (datalekken) bij de VTC door onderwijsinstellingen.

Voor wie: alle personeelsleden

De richtlijnen gelden voor directie, ondersteunend personeel, onderwijzend personeel, onderhoudsploeg,...

Stagiairs en interimarissen vormen een risicogroep die nauw moet opgevolgd worden.

Vooraf

Sluit telkens een overeenkomst = PROCEDURE

De AVG[2] verplicht je om een overeenkomst te sluiten met de leverancier, specifiek voor wat betreft de verwerking van persoonsgegevens. Die moet voldoen aan de vereisten van de AVG. Maak gebruik van het model dat de onderwijskoepels hebben gemaakt[3].

Kijk uit met niet-Europese providers = MET WIE

Niet-Europese leveranciers achten zich mogelijk niet gebonden door de Europese beschermingsregels en je bent minder zeker van de wettelijke bescherming. Er is ook het risico van toegang die gegeven

[1] We denken hierbij onder andere aan de diensten die geleverd worden in het kader van leerlingen, cursisten- en personeelsadministratie, leerlingvolgsystemen, pakketten voor financieel beheer, maar ook aan aanbieders van educatief lesmateriaal en elektronische leeromgevingen (ook voor de CLB's).
[2] De Algemene Verordening Gegevensbescherming (ook *GDPR* genoemd).
[3] Te vinden op https://www.privacyinonderwijs.be/

kan worden aan niet-Europese overheidsdiensten zonder dat je dat weet. Daarom moeten er extra veiligheidsmaatregelen genomen worden zoals encryptie van de gegevens.

De informatie: de persoonsgegevens.

Beperk de inhoud wat informatie over personen betreft = WAT

Het is soms nodig om meer uitgebreide en gedetailleerde informatie bij te houden voor probleemdossiers, vooral waar er discussies mogelijk zijn met ouders of andere opvoedingsverantwoordelijken.
Het moet wel een bewuste beslissing zijn en geen automatisme om van iedereen alles bij te houden wat ooit nodig of interessant zou kunnen zijn.

Iedereen heeft een inzagerecht (met het recht op een kopie) wat informatie over hemzelf betreft. Hou daar rekening mee.

Vermijd dat de leerlingen of de ouders zich gelabeld en gestigmatiseerd voelen.

Noteer zo weinig mogelijk over derden en noem die bij voorkeur niet bij naam. Leerlingen en ouders/ kunnen nog verwachten dat er informatie over hen wordt bijgehouden (via het schoolreglement en privacyverklaringen op de website van de school of bij de aanbieder van het platform), maar voor derden wordt er waarschijnlijk niet aan de transparantieplicht voldaan.

Schrijf alleen de echt nodige informatie op en communiceer meer mondeling met collega's.

Stel bewaartermijnen in = HOELANG

De algemene richtlijn is dat informatie verwijderd wordt zodra die niet meer nodig is. Dat zou volgens de principes van *privacy by design* en *privacy by default*[4] automatisch binnen een duidelijk bepaalde termijn moeten gebeuren. De regel is dat informatie die niet wettelijk vereist is, niet langer wordt bijgehouden (in het systeem) als de leerling de school verlaten heeft. Dit geldt zowel voor de onderwijsinstelling als voor de leverancier.

Toegang tot de informatie

Beperk de toegang tot de informatie = WIE

Geef de medewerkers enkel de toegangen tot de informatie die ze nodig hebben.

In principe moet de leverancier van het platform een fijnmazig rechtenbeheer ingebouwd hebben. De directeur of de door hem of haar aangeduide persoon kent die rechten toe[5].

[4] Dit betekent: in het vroegste stadium van het ontwerp de technische en organisatorische maatregelen treffen die nodig zijn om privacy en gegevensbescherming vanaf het begin te waarborgen (*„gegevensbescherming door ontwerp"*) en dat standaard persoonsgegevens worden verwerkt met het hoogste niveau van privacybescherming zodat persoonsgegevens standaard niet toegankelijk zijn voor een onbeperkt aantal personen (*„gegevensbescherming door standaardinstellingen"*).
[5] Ook volgens de principes van *privacy by design* en *privacy by default,* zodat alles standaard dicht staat in het begin.

Kies voor multifactor authenticatie = HOE

Gebruik niet alleen een login en wachtwoord[6] om toegang te krijgen tot het systeem. Multifactor authenticatie houdt de combinatie van minstens 2 verschillende van de volgende elementen in, zodat kwaadwillige personen moeilijk tegelijk over al die elementen kunnen beschikken:

- iets wat jij alleen weet (een code)

- iets wat jij alleen hebt (een kaart, stick of toestel met een beveiligingscertificaat)

- wat jij alleen bent (meestal via biometrische gegevens[7] als een vingerafdruk)

Wacht niet tot er een hack (of de zoveelste hack door leerlingen bijvoorbeeld) is geweest.

Werk mee met de verdere introductie van het gebruik van de elektronische identiteitskaart.

Controleer de toegang

Je zorgt ervoor dat de toegangen gelogd worden zodat men kan controleren wie wanneer toegang had tot welke gegevens en waarom.

Omgaan met de informatie: zorg dragen voor de persoonsgegevens

Druk niet af

Print de informatie uit de platformen niet als het niet echt nodig is en vernietig de afdruk zodra dat kan op een effectieve manier. Laat zeker niets rondslingeren op bureau's, in lokalen of in niet afgesloten kasten (er wordt regelmatig ingebroken in scholen) en in toegankelijke papierbakken.

Geef de gegevens niet aan derden

Sta gebruik van de informatie over personen voor andere dan de strikte onderwijsdoeleinden niet toe. Ook niet aan de beheerders van de platformen. Die zouden geen toegang tot de data zelf mogen hebben, tenzij voor specifieke helpdesktussenkomsten.

Contacteer je functionaris voor gegevensbescherming als je toch denkt dat er een noodzaak is om persoonsgegevens door te geven. Die kan je begeleiden naar de juiste procedures.

Meer weten? Vragen?

https://overheid.vlaanderen.be/vlaamse-toezichtcommissie

[6] https://safeonweb.be/nl/gebruik-sterke-wachtwoorden

[7] Biometrische gegevens gebruik je niet lichtzinnig: zie https://overheid.vlaanderen.be/standpunt-onderzoeksdossier-nr-2019/02 .