Stappenplan informatieveiligheid

Informatieveiligheid is een geheel van maatregelen dat ervoor zorgt dat alle informatie (in digitale en papieren vorm) binnen de onderwijsinstelling beschermd is tegen risico's en bedreigingen. Informatieveiligheid heeft als doel de continuïteit van de informatie en informatievoorziening te waarborgen en de mogelijke gevolgen van een informatieveiligheidsincident tot een aanvaardbaar, vooraf bepaald niveau te beperken.

Binnen informatieveiligheid kan je drie belangrijke kwaliteitsaspecten onderscheiden:

- **B**eschikbaarheid: informatie moet toegankelijk zijn wanneer nodig.
- **I**ntegriteit: informatie en verwerkingsmethoden bevatten zo min mogelijk fouten.
- **V**ertrouwelijkheid: informatie is alleen toegankelijk voor degenen die daartoe bevoegd zijn.

Privacy gaat onder meer over de bescherming van persoonsgegevens. Hoe je moet omgaan met persoonsgegevens is vastgelegd in een wet, nl. de privacywet. In april 2016 is de Europese Algemene Verordening Gegevensbescherming (AVG of GDPR) goedgekeurd. Op 25 mei 2018 wordt de huidige privacywet vervangen door deze nieuwe Europese Verordening die strengere regels bevat.

Hoewel informatieveiligheid en privacybeleid twee verschillende processen zijn, kunnen ze niet los van elkaar gezien worden. Wanneer de term informatieveiligheid wordt gebruikt, wordt hiermee meestal ook privacybeleid bedoeld, zoals ook in het vervolg van het document.

Op de gezamenlijke studiedag "privacybescherming in het onderwijs" op donderdag 16 november 2017 werden een aantal praktische handgrepen aangereikt om een goed beveiligingsplan op te stellen. Hieronder vind je een aantal checklists die je helpen met het opstellen van een goed beleid op basis van de presentaties. De presentaties zijn terug te vinden op OVSG extranet (of op de website van VVSG.

In een eerste instantie is het belangrijk om te sensibiliseren, te categoriseren en te documenteren. Het onderstaande stappenplan helpt je met deze taken. Samen met de informatieveiligheidsconsulent of Data Protection Officer (DPO) van je schoolbestuur kan je verder een Plan-Do-Check-Act cyclus voor je onderwijsinstelling opstellen.

Sensibilisering

Alle onderstaande stappen zullen alleen maar waarde hebben als **iedereen** (poetspersoneel, conciërge, leerkrachten, leerlingen, directeur, ouders, cursisten …) van de onderwijsinstelling hieraan meewerkt. Daarom is het heel belangrijk om een sensibiliseringsplan op te stellen. Betrek hierbij de informatieveiligheidsconsulent van je schoolbestuur (gemeentebestuur)!

Mogelijke acties:

- Betrek leerkrachten.
  - ✓ Laat bijvoorbeeld zelf nagaan welke gegevens ze gebruiken, als deze gegevens privacygevoelig zijn en of dit eigenlijk wel nodig is. Je kan dit eenvoudig doen door de leerkrachten bv. een paar weken lang in de agenda te laten opschrijven welke gegevens, foto's … ze gebruiken.
  - ✓ Laat de leerkrachten zelf voorstellen doen.
- Peer-to-Peer: wissel goede tips en trucs uit. Niet alleen binnen de school maar ook in de scholengemeenschap, scholen onderling, schoolbestuur …
- Maak informatieveiligheid bespreekbaar: plaats op elk overleg een item op de agenda.
- Communiceer met iedereen: ouders, grootouders, poetspersoneel, vrijwilligers …

Deze stap is de belangrijkste stap van het volledige proces. ***Informatieveiligheid is een zaak van iedereen***. Het mag niet leiden tot een papieren dossier (= *planlast*), maar het is een bewustmakingsproces zodat iedereen op een natuurlijke manier waakt over de veiligheid van de kinderen of personeel (= *zorg*).

Behandel het proces informatieveiligheid als een goede huisvader of huismoeder.

Beleid

Beleid wordt gemaakt door de gemeente.

Om in orde te zijn met de nieuwe wetgeving, moeten een aantal documenten aangepast worden zoals het schoolreglement, arbeidsreglement, privacyverklaring, ICT policy, informatieveiligheidsplan, …

De wet is pas van toepassing op 25 mei 2018. Ter voorbereiding heeft OVSG reeds een aantal richtlijnen opgenomen in de modelreglementen.

In de nabije toekomst zullen nog meer diverse modellen ter beschikking gesteld worden via OVSG extranet. Volg de nieuwsbrieven van VVSG en OVSG.

Organisatie

Ieder schoolbestuur is verplicht om een informatieveiligheidsconsulent of DPO aan te stellen. Aangezien onderwijs een gemeentedienst is, is het schoolbestuur verantwoordelijk voor de informatieveiligheid voor zijn onderwijsinstellingen (scholen, CVO, DKO, CLB). Dit betekent niet dat de onderwijsinstelling geen verantwoordelijkheid draagt wat informatieveiligheid betreft! Het opzettelijk niet naleven of het negeren van de instructies of wetgeving kan ervoor zorgen dat een directeur of personeelslid zelf verantwoordelijk wordt gesteld.

Om de informatieveiligheidsconsulent of DPO te helpen, werd met de Vlaamse Toezichtcommissie (VTC) afgesproken om een aanspreekpunt aan te stellen binnen de onderwijsinstellingen. Elk schoolbestuur ontving hierover een gezamenlijke brief vanuit VVSG en OVSG.

Er kunnen eventueel meerdere aanspreekpunten worden aangesteld afhankelijk van het doel. Voorbeeld: voor beleid kan de directeur of de administratieve medewerker belast met personeelszaken fungeren al aanspreekpunt, terwijl voor het technische luik de ict-coördinator deze taak op zich neemt.

Checklist

- ☐ Is er binnen de onderwijsinstelling een aanspreekpunt aangesteld (eventueel gedeelde opdracht)? Is die persoon gekend bij de personeelsleden?
- ☐ Is er al een gesprek geweest met de informatieveiligheidsconsulent of DPO van het schoolbestuur? Ter voorbereiding kan de vragenlijst gebruikt worden die ter beschikking is gesteld door VVSG en OVSG (extranet OVSG).
- ☐ Maakt het aanspreekpunt deel uit van een actief overlegplatform binnen het schoolbestuur?

Overzicht gegevens

De directeur van de school is verantwoordelijk voor de diverse toegangen tot de toepassingen en gegevens. Foto's zijn ook gegevens!

Checklist

- ☐ **Maak een lijst van alle gegevens** die gebruikt worden in de onderwijsinstelling:
  - ⇨ Welke gegevens zijn er aanwezig?
    Deze lijst kan als uitgangspunt gebruikt worden voor het verder opmaken van het dataregister (classificatie). Voor meer informatie hierover, contacteer de informatieveiligheidsconsulent of DPO van het schoolbestuur.
    - Publieke gegevens: mag buiten de onderwijsinstelling/schoolbestuur
    - Interne gegevens: mag alleen binnen de onderwijsinstelling/schoolbestuur ("bedrijfsgevoelig")
    - Privacy gegevens? Persoonsgegevens zoals naam, adres, resultaten, kenmerken,foto's …
    - Gevoelige gegevens? Bijvoorbeeld ziekte, geloof, contact met strafrechter …
    - Gegevens van minderjarigen?
    - Waar worden de gegevens bewaard? Op papier, op computer, in de Cloud, op externe dragers, website, sociale media …?
  - ⇨ Hoelang worden de gegevens bewaard? Tip: ga eerst na of er wettelijke bewaartermijnen zijn voor het bewaren van gegevens. Indien de termijn afwijkt van de wettelijk termijn, motiveer waarom deze gegevens langer worden bewaard. Indien er geen bewaartermijn is, hanteer dan het principe "niet langer bewaren dan noodzakelijk" (waarbij je die noodzaak ook duidt).
  - ⇨ Wie heeft toegang (ook fysiek!) tot de gegevens? En welke toegang krijgen ze tot de gegevens (lezen, aanpassen …)?
  - ⇨ Hoe worden de gegevens beschermd zodat enkel diegene die recht heeft op toegang ook toegang krijgt?
  - ⇨ Indien van toepassing: hoe worden de gegevens intern (binnen de school of het schoolbestuur) uitgewisseld?

- ⇨ Indien van toepassing: hoe worden de gegevens extern (buiten de school of het schoolbestuur) uitgewisseld?
- ⇨ Waarom worden de gegevens verzameld? Wettelijk, algemeen of vitaal belang, contractueel of andere?
- ⇨ Waarvoor worden de gegevens gebruikt (leerlingenadministratie, personeelsadministratie, opvolging …)?

☐ **Maak een lijst van alle toepassingen** en noteer de volgende gegevens:

- ⇨ wie kent de rechten toe? “Wie kan wat” en “Wie ziet wat”?
- ⇨ is er een procedure indien een personeelslid uit dienst gaat of een andere functie krijgt? Wie is hiervoor verantwoordelijk?

Controleer of de gegevens up-to-date zijn. Indien dit niet zo is, verwijder alle oude gegevens.

Hou niet meer gegevens bij dan nodig (**dataminimalisatie)**. Vernietig gegevens die niet nodig zijn of waarvan het bijhouden ervan niet verantwoord kunnen worden.

Toestemmingen

In deze stap worden de toestemmingen gecontroleerd.

Indien de gegevens wettelijk nodig zijn, van algemeen/vitaal belang zijn of nodig zijn binnen een afgesloten contract, dan hoef je geen toestemming te vragen. Je mag de gegevens echter niet langer bijhouden dan noodzakelijk!

Het krijgen van toestemming is ook van toepassing op websites, sociale media, nieuwsbrieven …

Hoe een toestemming vragen?

- Gebruik duidelijke en klare taal.
- Er moet vermeld worden waarom de gegevens worden verzameld en wat er met de gegevens zal gebeuren. Je kan de gegevens niet voor andere doeleinden gebruiken dan deze waarvoor je toelating hebt gekregen.
- In de tekst moet opgenomen worden hoe de gegevens kunnen opgevraagd worden en hoe ze hun gegevens kunnen (laten) wijzigen.
- Vermeld ook het recht om vergeten te worden. Het kan zijn dat je voor bepaalde redenen, bijvoorbeeld wettelijke redenen, de informatie van een persoon niet kan/mag verwijderen. Neem dit op in de tekst.
- Geen kleine letters! Er moet een actieve handeling gebeuren!

  Voorbeeld:

  Niet OK: ☒ inschrijving schoolnieuwsbrief

  Wel OK: ☐ vink aan indien je de schoolnieuwsbrief wenst te ontvangen

  Zorg ook voor opt-out: op ieder moment moet het abonnement op de schoolnieuwsbrief ongedaan kunnen worden.

- Wat de toelating van minderjarigen betreft kan je twee situaties onderscheiden:

  - ✓ Wanneer “diensten van de informatiemaatschappij” rechtstreeks aan kinderen worden aangeboden (bv. sociale media en apps), is de GDPR van toepassing en is de toestemming van de ouders of voogd enkel nodig indien het kind jonger is dan 16 jaar.

- ✓ Wanneer de diensten van de informatiemaatschappij niet rechtstreeks aan kinderen worden aangeboden, geven de ouders of voogd toelating indien het gaat over minderjarige jongeren. Niettemin mogen minderjarige jongeren zelf hun toestemming geven indien ze beschikken over “voldoende onderscheidingsvermogen”. Dit betekent dat de jongere bekwaam is om autonome beslissingen te nemen. Dit kan meestal vanaf een leeftijd tussen 12 en 14 jaar. Indien een minderjarige blijk geeft over voldoende onderscheidingsvermogen en verantwoordelijkheidszin te beschikken, is het raadzaam dat hij samen met zijn ouders of voogd toestemming geeft. Vanaf 18 jaar beslissen de jongeren zelf.

Checklist

- ☐ Maak een lijst van alle gegevens waarvoor toelating nodig is. Zorg voor een document.
- ☐ Maak een lijst van alle toelatingen: inventariseer centraal.

Leveranciers

Met de softwareleveranciers moeten er afspraken worden gemaakt indien er persoonsgegevens worden verwerkt. Naar Nederlands model zullen ook de Vlaamse softwareleveranciers kunnen intekenen op een intentieverklaring. Via deze intentieverklaring laten de softwareleveranciers weten dat ze alles in het werk zullen stellen om te voldoen aan de nieuwe regelgeving. Er zal een model verwerkersovereenkomst ter beschikking worden gesteld die de softwareleveranciers zullen ondertekenen.

Via de nieuwsbrieven van VVSG en OVSG zal je op de hoogte worden gehouden.

Je kan echter binnen de onderwijsinstelling al voorbereidend werk uitvoeren:

Checklist

- ☐ Maak een lijst van alle softwarepakketten die binnen de onderwijsinstelling worden gebruikt, ook de apps (al dan niet gratis).
- ☐ Duid aan welke toepassingen of apps privacy(gevoelige) gegevens verzamelen, bewerken …
- ☐ Verzamel alle contracten van alle toepassingen en apps die privacy(gevoelige) gegevens verzamelen, bewerken …
- ☐ Ga na welke toepassingen (of apps) privacygegevens bewaren in niet EU-landen (indien mogelijk) of beheerd worden door niet EU-bedrijven.

Data Protection Impact Assessment (DPIA)

Een DPIA of een gegevensbeschermingseffectbeoordeling (GEB) is verplicht als er een verhoogd risico aanwezig is. De Privacycommissie heeft een aanbeveling geschreven wanneer een DPIA nodig is: https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_NL.pdf

Concreet voor onderwijs:

Er is geen DPIA nodig voor je cursistenadministratiesysteem indien voldaan aan aanbeveling nummer 7.

> *"7. verwerkingen van persoonsgegevens verricht door onderwijsinstellingen met het oog op het beheer van hun relaties met hun leerlingen of studenten in het kader van hun onderwijsopdrachten, voor zover de verwerking alleen betrekking heeft op persoonsgegevens betreffende potentiële, huidige en gewezen leerlingen of studenten van de betrokken onderwijsinstelling en er geen personen worden geregistreerd op grond van gegevens verkregen van derden en alleen in het kader van de toepassing van een wets- of verordeningsbepaling aan derden worden meegedeeld en niet langer worden bewaard dan nodig voor het beheer van de relatie met de leerling of student."*

Er is geen DPIA nodig voor je personeelsadministratie en boekhouding op voorwaarde dat voldaan is aan de aanbevelingen 1 t.e.m. 3.

> *"1. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op gegevens welke noodzakelijk zijn voor de **loonadministratie** van personen in dienst van of werkzaam ten behoeve van de verantwoordelijke voor de verwerking wanneer de gegevens uitsluitend worden gebruikt voor die loonadministratie, alleen worden meegedeeld aan de ontvangers die daartoe gerechtigd zijn en niet langer worden bewaard dan nodig voor de doeleinden van de verwerking;*
>
> *2. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op de **administratie van het personeel** in dienst van of werkzaam ten behoeve van de verantwoordelijke voor de verwerking, voor zover deze verwerking geen betrekking heeft op gegevens betreffende de gezondheid van de betrokken persoon, noch op gevoelige of gerechtelijke gegevens in de zin van de artikelen 9 en 10 van de AVG of op gegevens die een beoordeling van de betrokken persoon tot doel hebben en de verwerkte persoonsgegevens niet langer worden bewaard dan nodig voor de personeelsadministratie en alleen in het kader van de toepassing van een wets- of verordeningsbepaling of indien nodig voor de verwezenlijking van de doelstellingen van de verwerking aan derden worden meegedeeld;*
>
> *3. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op de boekhouding van de verantwoordelijke voor de verwerking wanneer de gegevens uitsluitend worden gebruikt voor die boekhouding, de verwerking alleen betrekking heeft op personen van wie de gegevens noodzakelijk zijn voor de boekhouding en de persoonsgegevens niet langer worden bewaard dan nodig voor de doeleinden van de verwerking en de verwerkte persoonsgegevens alleen aan derden worden meegedeeld in het kader van de toepassing van een wets- of verordeningsbepaling of wanneer de mededeling noodzakelijk is voor de boekhouding;"*

Er is **wel** een DPIA nodig voor volgsystemen, zorgsystemen …

> *"12. wanneer de verwerking ertoe strekt om de kennis, prestaties, vaardigheden of mentale gezondheidstoestand van leerlingen te registeren en de evolutie ervan op te volgen, met name aan de hand van leerlingvolgsystemen, ongeacht of deze leerlingen zich in het primair, secundair, tertiair of universitair onderwijs bevinden."*

Checklist

- ☐ Maak een lijst van alle gegevens/toepassingen voor de administratie van leerlingen of cursisten.
- ☐ Maak een lijst van alle gegevens/toepassingen nodig voor de administratie van het personeel.
- ☐ Maak een lijst van alle gegevens/toepassingen nodig voor de boekhouding.
- ☐ Maak een lijst van alle gegevens/toepassingen die nodig zijn om kennis, prestaties, vaardigen of mentale gezondheidstoestand van leerlingen te registreren en de evolutie er van op te volgen.
- ☐ Overloop bovenstaande 4 lijsten met de informatieveiligheidsconsulent of DPO van je schoolbestuur en maak een actieplan op.

Operationeel

Om een goed privacybeleid te kunnen voeren zijn er ook een aantal operationele acties nodig. Er moeten enerzijds acties genomen worden door de IT, maar anderzijds is de fysieke beveiliging eveneens een onderdeel van een goede informatiebeveiligingsplan.

Fysieke beveiliging

Wat de fysieke beveiliging betreft, moeten de volgende punten gecontroleerd worden:

- De toegang tot beveiligde ruimtes (waarin zich persoonsgegevens bevinden of gebruikt/bewerkt worden) moet strikt beperkt worden tot de bevoegde personen. Dit geldt ook voor serverrooms die beveiligde gegevens bevatten. Er moet hiervan een logfile worden bijgehouden. De verantwoordelijke (directeur) moet hierop regelmatig controle houden.
- De gepaste maatregelen moeten genomen worden om schade door brand, wateroverlast, explosie, dieren … kortom elke vorm van natuurlijke of door mensen veroorzaakte calamiteiten te vermijden. Voorbeelden:
  - ✓ De gepaste branddetectie en brandblusapparatuur voorzien en de werking ervan op geregelde tijdstippen controleren.
  - ✓ Opslagmedia voor back-ups niet bewaren in de beveiligde serverruimte.

Checklist

- ☐ Overloop bovenstaande lijst met het aanspreekpunt preventieadviseur arbeidsveiligheid van de onderwijsinstelling.

IT handboek

Het IT-handboek bevat een overzicht van alle configuraties en procedures met betrekking tot de IT.

Checklist

- ☐ Documenteer de volgende procedures:
  - ⇨ Anti-malware software: log de meldingen
  - ⇨ Firewall
  - ⇨ Back-ups: controle en test
  - ⇨ Logging: wat en hoe?
  - ⇨ Ontdubbeling netwerk: administratief netwerk, schoolnetwerk. Ook scheiding van de Wifi-netwerken (publiek, school)!

- ⇨ Cryptografische sleutels indien nodig
- ⇨ Netwerkplan: kabels + beveiliging (gesloten patchkasten!)

☐ Servicedesk
- ⇨ Bijhouden meldingen van veiligheidsincidenten (hacken, diefstal toestellen …)
- ⇨ Melden privacy inbreuken
- ⇨ Procedure bij uit dienst zetten van apparatuur

Eigen softwareontwikkeling

Indien de onderwijsinstelling eigen software ontwikkelt waarin persoonsgegevens verwerkt worden, dan moet je dit zeker aftoetsen bij de informatieveiligheidsconsulent of DPO van je schoolbestuur.

Checklist

☐ Maak een lijst van alle toepassingen die zijn ontwikkeld of zullen worden ontwikkeld en die privacygegevens verwerken.
☐ Contacteer de informatieveiligheidsconsulent of DPO van je schoolbestuur.