Aandachtspunten medewerkers AVG

Inleiding

Vanaf 25 mei 2018 geldt voor alle EU-inwoners dezelfde bescherming van persoonsgegevens ongeacht waar hun gegevens zijn opgeslagen in Europa of buiten Europa. De wet 'Algemene verordening gegevensbescherming' (AVG of GDPR in het Engels) is een vervanging van de nationale wetten die nu in de verschillende EU lidstaten gelden.
De AVG gaat strenger om met privacy dan de verschillende nationale wetten op dat terrein.
Onderwijsorganisaties zijn op bestuursniveau verplicht om de informatiebeveiliging en privacy (IBP) te regelen. Onderdeel daarvan is het aanstellen van een functionaris voor gegevensbescherming (FG) die als interne toezichthouder belast is met de controle en handhaving van de IBP.

Binnen het regelen van de IBP is er een onderscheid te maken tussen twee elementen:

1. **De technische kant.**
2. **De gedragskant.**

Bij de technische kant moet je denken aan:

- Technische inrichting van ICT-systemen, zoals "wie mag wat lezen en/of muteren in bv Somtoday"
- Wie heeft welke rechten om welke documenten in te zien?
- Regelingen waarbij duidelijk wordt dat de juiste toestemmingen zijn verkregen om bepaalde gegevens te verwerken en/of beeldmateriaal te gebruiken.
- Verwerkingsovereenkomsten met externe ICT-beheerders en softwareleveranciers.
- Het goed verdelen van de taken en bevoegdheden over de mensen die een sturende rol hebben op dit terrein.
- Het instellen van het Meldpunt dataprivacy (Meldpuntdataprivacy@altenacollege.nl. Dit meldpunt zal het centrale aanspreekpunt worden voor alle dataprivacy gerelateerde zaken, zoals het melden van beveiligingsincidenten en inzageverzoeken.

Bij de gedragskant kun je denken aan:

- Goed omgaan met vertrouwelijke gegevens vraagt van iedereen die daarmee werkt bewustwording en passend gedrag.

Hieronder wordt deze gedragskant uitgewerkt in een aantal aandachtspunten

- Het automatisch doorsturen van schoolmail naar privémail is reeds gestopt. Check dus met regelmaat je schoolmail en houdt schoolmail en privémail maximaal gescheiden.
- Zet bij een mail naar meerderen van wie je niet zeker weet dat ze elkaars e-mailadres kennen de e-mailadressen altijd in de BCC en niet in AAN of de CC.
- Laat je computer nooit ingelogd en/of onvergrendeld achter.
- Als je schoolbestanden op een privédevice (computer, tablet of smartphone) hebt staan waarin persoonlijke gegevens van leerlingen, ouders of collega's staan, zorg dan voor een goede scheiding tussen schoolbestanden en privébestanden èn zorg dat het betreffende device goed beveiligd is, zodat anderen er niet bij kunnen.
  Let hier bv ook op als je thuis een computer deelt met anderen uit het gezin. Zorg er dan voor dat jouw mailomgeving en bestanden alleen door jouzelf geraadpleegd kunnen worden en dat jouw gedeelte dus met een persoonlijk wachtwoord is beveiligd.
  Je loopt hier het minste risico als je bestanden met persoonlijke gegevens niet lokaal, maar alleen in je persoonlijke en beveiligde cloud-omgeving zet.

- Dat geldt ook als je via een App op een privé-device schoolmail kunt lezen. Leen zo'n device ook niet uit aan anderen. Als je schoolmail op je telefoon of tablet raadpleegt en/of bestanden van school op je telefoon of tablet hebt staan, zet dan een beveiliging op je telefoon cq tablet.
- Als je schoolbestanden met persoonsgegevens op een usb-stick of externe harddisk zet, zorg dan dat deze met een wachtwoord beveiligd is en beperkt deze tot het minimum. Dus zeker niet op een usb-stick o.i.d. zonder wachtwoord.
  Verwijder de informatie als je deze niet meer nodig hebt.
- Als extra beveiliging is het zeer aan te bevelen om bestanden met persoonlijke gegevens van een wachtwoord op dat bestand te voorzien. Als je dan geheel per ongeluk zo'n bestand als bijlage bij een mail voegt, kunnen ontvangers er niets mee.
- Ga zorgvuldig om met persoonsgegevens van mensen (leerlingen, ouders, collega's). Voorkom het 'rondzwerven' van bestanden met persoonsgegevens op verschillende gegevensdragers.
- Verstrek geen school e-mailadressen aan mensen buiten school; de enige uitzondering is dat aan leerlingen en hun ouders de e-mailadressen van hun docenten en begeleiders mogen worden verstrekt.
- Laat geen printjes op de printer achter waar persoonlijke gegevens op staan.
- Verwijder interne en vertrouwelijke documenten van je bureau bij het voor langere tijd verlaten van je bureau.
- Als je een beveiligingsincident (een gebeurtenis die kan leiden tot een datalek) of een datalek (het verloren raken van persoonsgegevens) veroorzaakt of bemerkt, meldt dat dan meteen, hetzij rechtstreeks aan de rector, hetzij via het Meldpunt.
  Mocht er onbedoeld een datalek optreden (i.c. er komen persoonlijke gegevens van leerlingen, personeelsleden of ouders terecht bij mensen voor wie die gegevens niet bestemd zijn) dan moeten we snel beoordelen of dit datalek dermate ernstig is dat we het moeten melden bij de autoriteit persoonsgegevens. Daar zit een tijdsklem op van 72 uur, dwz 3 volledige dagen.
  Dit betekent dat een eventueel datalek altijd snel gemeld moet worden bij de AVG-commissie. Dus niet eerst het een paar dagen aanzien of er ergens roering ontstaat, dan wel of het stil blijft. We zijn als school namelijk strafbaar als we niet (tijdig) melden in situaties waarin dat wel moet.
- Vanaf 2018- 2019 moet iedereen een token gebruiken om in te loggen in SOMtoday. Het handigste is een soft-token = een App op een mobiele telefoon of tablet. Maar een hardtoken = een klein apparaatje kan ook. Wie een hardtoken wil, dient dit bij Regina aan te geven.
- Het educatieve netwerk wordt zo ingesteld dat iedereen automatisch na een half jaar een nieuw wachtwoord moet kiezen. Bij SOMtoday kan dit niet automatisch ingesteld worden, maar het advies is hier het wachtwoord te wijzigingen zodra je daartoe gedwongen wordt in het educatieve netwerk.
- Er is een geactualiseerd protocol Social Media, dat nu als apart document wordt gebruikt. Het is het op onze situatie toegespitste modelprotocol van Verus.
- Wees je er van bewust dat leerlingen ouder dan 16 jaar of ouders van kinderen onder de 16 jaar inzage in hun eigen gegevens kunnen vragen. Persoonlijke werkaantekeningen vallen hier niet onder, maar alles wat in een dossier wordt opgeslagen of gegevens die aan anderen worden verstrekt vallen daar wel onder.
- Overdracht van gegevens over vertrekkende leerlingen naar andere scholen (VO, VSO, MBO, HBO, Universiteit) gebeurt zo veel mogelijk via OSO (= het gecertificeerde landelijke systeem voor overdracht van leerlinggegevens). Hiervoor dienen de ouders ook toestemming te geven. Er worden geen onversleutelde gegevens over leerlingen via e-mail verzonden.
  Bij een eventuele mondelinge warme overdracht wordt zorgvuldig omgegaan met vertrouwelijke gegevens over of van de leerling.
- Als documenten met persoonlijke gegevens niet meer nodig zijn en/of niet langer bewaard mogen worden, zorg dan voor een goede vernietiging van de deze documenten.

Bestemd voor:
- medewerkers

Te plaatsen op:
- personeelsportaal