Dit document wordt opgesteld om de nodige verduidelijking te geven aan het directieteam alsook aan het schoolbestuur.

GDPR kort uitgelegd

Vanaf 25/05/2018 gaat de nieuwe **A**lgemene **V**erordening **G**egevensbescherming (**G**eneral **D**ata **P**rotection **R**egulation) in voege. Concreet wil dit zeggen dat de toezichthouder (Privacycommissie/CPBL) vanaf dan (hoge) boetes kan opleggen terwijl dat voorheen nog niet mogelijk was.

De GDPR is er gekomen om bedrijven (en dus ook scholen) meer te laten nadenken over de manier waarop omgesprongen wordt met persoonsgegevens[1] en hoe deze beschermd worden. Privacy by default en Privacy by design is iets wat we vaak zien terugkomen in de teksten omtrent GDPR.

Belangrijk om weten is dat de directie steeds de eindverantwoordelijkheid draagt omtrent alle dataverwerking. Het aanspreekpunt informatieveiligheid (AIV) zorgt voor een duidelijke vertaling naar de directie en heeft enkel een adviserende rol. Er kan binnen de school een CEL informatieveiligheid opgericht worden om continu toe te zien op de opstelling en opvolging van het beleid en de procedures. Deze cel draagt echter geen verantwoordelijkheid.

Wat wordt van ons verwacht

Aangezien wij als school veel omgaan met persoonsgegevens moeten wij er op toezien dat deze gegevens op een correcte manier worden **opgevraagd**, **opgeslagen**, **gebruikt** en **gearchiveerd**.

Om aan te tonen hoe we dit doen (want bij een incident zal dit van ons verwacht worden) moeten we een register aanmaken waarin we o.a. volgende zaken bewaren:

- overzicht van fysieke en logische toegangen tot persoonsgegevens (wie kan wat)
- inschatting van de risico's bij nieuwe projecten
- oplijsten van de gegevens die we verzamelen (en waarom we deze verzamelen)
- indien van toepassing de toestemming van het data subject (leerling/ouders van leerling) om zijn gegevens te bewaren...

Verder wordt er van ons ook verwacht dat wij nagaan of de partners waarmee we als school samenwerken voor de dataverwerking (data processors: Google [G Suite], Microsoft [Office365], Smartschool, Informat, Wisa…) GDPR compliant zijn (dus voldoen aan de Europese wetgeving). Data hoeft (om GDPR compliant te zijn) niet noodzakelijk binnen de EU bewaard te worden.

Als er zich een datalek voordoet (account leerkracht gehackt, USB-stick **met persoonsgegevens** verloren/gestolen, computer van de directeur is gestolen…) is de school verplicht dit te melden aan de toezichthouder (een lek wordt niet per se beboet, het niet melden ervan **wel**). Lekken worden steeds door de Data Protection Officer (DPO)[2] (als die er is) gemeld.

[1] Persoonsgegevens zijn alle gegevens die gebruikt kunnen worden om personen te identificeren en/of informatie die betrekking heeft tot deze personen (al dan niet gevoelige informatie).
[2] KathOndVla heeft aangegeven dat scholen geen DPO dienen te hebben. Een aanspreekpunt informatieveiligheid (AIV) volstaat. Sommige schoolbesturen zullen er echter toch voor opteren om met een DPO te werken.

Wat wij alvast kunnen doen

In bijlage is een document toegevoegd met 24 quick wins[3]. Heel veel van deze zaken zijn mits een kleine (gezamenlijke) inspanning relatief vlug te realiseren.

Waar moeten wij als school zo op letten (een korte indicatieve opsomming):

- persoonsgegevens moeten zowel fysiek als logisch voldoende afgeschermd worden.
    - overzicht van logische en fysieke toegang
      sleutelplan, kasten niet zomaar open laten staan, documenten niet op de printer kunnen blijven liggen...
- persoonsgegevens efficiënt en correct archiveren (gegevens niet langer bewaren dan nodig, maar **minstens** zo lang als wettelijk bepaald dus er **moet** een termijn bepaald worden).
- we moeten enkel gegevens verzamelen die we effectief nodig hebben. Om gegevens op te vragen waar we wettelijk gezien geen nood aan hebben (er zijn uitzonderingen) moeten we steeds de ondubbelzinnige toestemming vragen aan het datasubject (leerling/ouder, wettelijke leeftijd is nu 16j maar kan nog verlagen).
- personeel blijvend sensibiliseren en correct leren omgaan met de gegevens waar zij toegang toe hebben.
- duidelijke **procedures** en **beleid** opstellen:
    - hoe geven we toegang tot gegevens en hoe ontnemen we deze? Wat bij leerkrachten die tijdelijk elders aangesteld zijn? Hoe maken we het werkbaar voor interimarissen?
    - gebruikt het personeel een sterk wachtwoord? Voor wie gaan we dubbele authenticatie verplichten? Zijn ze zich bewust van de risico's? Niet alleen op school maar ook thuis?
    - op welke plaatsen mogen persoonsgegevens bewaard worden?

Actieplan

In het kort hieronder ons voorlopig **actieplan**:

- Opmaken van een register omtrent de dataverwerking op school.
    - welke data verzamelen we?
    - waarvoor gebruiken we die?
    - er is een wettelijke grond of noodzaak om deze gegevens te gebruiken of hebben we hiervoor toestemming nodig?

  Momenteel wordt ervoor gekozen om af te wachten wat KathOndVla/schoolbestuur aan modeldocumenten hieromtrent zal voorzien.
- Aanpassingen aan het schoolreglement met enkele belangrijke toevoegingen omtrent GDPR.
- Collega's sensibiliseren (al dan niet met een verplichte opleiding) > dit is iets dat best jaarlijks terugkeert.
- Wachtwoordenbeleid uitwerken (gebruik password managers [zo weinig mogelijk], **geen** wachtwoorden opschrijven)
- Het gebruik van cloudtoepassingen stevig onder de loep nemen.
  Persoonlijke dropbox/google drive/onedrive verbieden
  > verhuis naar G Suite / O365.
- Oprichten van een interne cel informatieveiligheid. Deze cel zou ter voorbereiding van GDPR een paar keer moeten samenkomen om de stand van zaken en planning op te volgen. Daarna zou deze 1 of 2x per jaar moeten samenkomen om de stand van zaken verder op te volgen en toe te zien op de opvolging van het beleid.

[3] https://docs.google.com/document/d/16h4Uy2vHQFFogslwFOBAVYf_qwvtohfHeL5q2kZdurc/edit?usp=sharing