**BIJLAGE 2. Algemene technische en organisatorische beveiligingsmaatregelen**

Volgens artikel 28.1 van de AVG doet de verwerkersverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties m.b.t. technische en organisatorische maatregelen bieden zodat persoonsgegevens voldoende beschermd zijn en de rechten van de betrokkene gewaarborgd blijven.

Volgens artikel 32 van de AVG moet de verwerker passende technische en organisatorische maatregelen nemen ter beveiliging van de verwerking van persoonsgegevens.

**In deze bijlage vermelden verwerkers wat hun algemene technische en organisatorische beveiligingsmaatregelen zijn zodat de verwerkingsverantwoordelijke voldoende garanties krijgt inzake beveiliging van persoonsgegevens.**

Eventuele certificeringen:

Audits/derdenverklaringen:

**Algemene omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Verwerkersovereenkomst**

I. Algemene omschrijving van de maatregelen om te waarborgen dat uitsluitend bevoegd personeel toegang heeft tot de verwerking van persoonsgegevens.

> Meer in het bijzonder de uitwerking welke (groepen) medewerkers van de verwerker toegang hebben tot welke persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers mogen uitvoeren met de persoonsgegevens.

Plantyn hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

| Medewerkers en gegevens | Handelingen |
|---|---|
| Medewerkers van de klantenservice en consultants verkrijgen op verzoek van een school toegang tot licentie-informatie. Zij kunnen onder meer zien voor welke leerlingen een digitaal leermiddel is geactiveerd. De klantenservice zal alleen op verzoek van én met uitdrukkelijke toestemming van de leerkracht zicht hebben in de gegevens van de school/leerkracht/leerling, en uitsluitend ter ondersteuning van de eindgebruiker. | Administratieve handelingen in het kader van de werking van leermiddelen, schooladministratiesystemen, bestellingen en licenties.<br><br>Ondersteuning van de eindgebruiker. |
| Analisten/deskundigen op het gebied van ontwikkeling van lesmateriaal hebben toegang tot geanonimiseerde sets van resultaten van gebruik van leermiddelen/schooladministratiesystemen. | Analyse van het lesmateriaal, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van adaptief lesmateriaal, opsporing en verbetering van de kwaliteit van het materiaal. |
| Analyse van het lesmateriaal, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van adaptief lesmateriaal, opsporing en verbetering van de kwaliteit van het materiaal. | De handelingen van IT-databasebeheerders zijn gericht op continuïteit en beheer van ICT-systemen. |

II. Algemene omschrijving van de maatregelen om de persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking.

**Organisatie van informatiebeveiliging en communicatieprocessen**

- Plantyn nv heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Plantyn nv heeft een proces georganiseerd voor communicatie over informatiebeveiligingsincidenten.

**Medewerkers**

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Plantyn nv stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

**Fysieke beveiliging en continuïteit van de middelen**

- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.
- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's. Noordhoff Uitgevers beschikt over bedrijfscontinuïteitsplannen waarin uitwijklocaties zijn opgenomen.

**Netwerk-, server- en applicatiebeveiliging en onderhoud**

- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- De digitale leermiddelen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie. Wijzigingen in applicaties worden getest op kwetsbaarheden voordat ze in productie worden genomen.

- Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd op basis van patchmanagement.
- Gegevens die in applicaties worden verwerkt zijn geclassificeerd op risico's.
- Penetratietests en *vulnerability assessments* worden periodiek uitgevoerd.
- Niet (meer) gebruikte informatie wordt verwijderd.
- Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- Er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van de onderwijsinstelling vindt versleuteld plaats.

III. Algemene omschrijving rond het informatieveiligheidsbeleid en de maatregelen om zwakke plekken te identificeren en aan te pakken ten aanzien van de verwerking van persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de onderwijsinstelling.

De systemen van Plantyn nv worden periodiek gecontroleerd op veiligheid. Daarnaast voorziet het beveiligingsbeleid van Plantyn nv in interne processen om kwetsbaarheden te identificeren.

**Informeren over Inbreuken in verband met persoonsgegevens**

Het informeren in geval van inbreuken in verband met persoonsgegevens en/of incidenten met betrekking tot beveiliging. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de volgende informatie zonder onredelijke vertraging in stappen worden verstrekt.

- Informatie die in ieder geval over een incident gedeeld moet worden zodat de verwerkingsverantwoordelijke aan de meldplicht aan de gegevensbeschermingsautoriteit kan voldoen. De vetgedrukte elementen moeten zeker worden meegedeeld in geval van een inbreuk in verband met persoonsgegevens.
    - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en **aard incident** (hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens).
    - De **oorzaak** van het beveiligingsincident.
    - De **maatregelen** die getroffen zijn om het incident aan te pakken en eventuele/verdere schade te beperken en voorkomen.
    - Benoemen van **betrokkenen** die gevolgen kunnen ondervinden van het incident, en de mate waarin.
    - De **omvang van de groep betrokkenen**.
    - Het **soort gegevens** dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
    - De **omvang van de gegevens**.

- De **waarschijnlijke gevolgen voor de betrokkene**.

**Versie**

Deze bijlage is voor het laatst bijgewerkt op 17 mei 2018.