Bijlage B bij de Bewerkersovereenkomst Instruct B.V.

Technische en Organisatorische Beveiligingsmaatregelen

A. Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

Toegang tot persoonsgegevens

Instruct B.V. 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 hebben toegang tot licentie informatie. Zij kunnen onder meer zien voor welke leerlingen een digitaal leermiddel is geactiveerd, op welke school deze leerlingen zitten en het e-mailadres van de leerlingen. De klantenservice heeft geen inzage in leerresultaten van leerlingen	Administratieve handelingen in het kader van de werking van leermiddelen en licenties. Ondersteuning van de eindgebruiker.
Deskundigen op het gebied van ontwikkeling van lesmateriaal (waaronder auteurs) hebben geen toegang tot resultaten van gebruik van leermiddele	Activiteiten gericht op het ontwikkeling en optimalisatie van lesmateriaal.
Productmanagers hebben toegang tot alle resultaten van gebruik van leermiddelen	Analyse van het lesmateriaal, opsporing en verbetering van fouten in de werking van het digitale leermiddel en ondersteuning van de eindgebruiker.
IT-databasebeheerders en ontwikkelaars hebben toegang tot de databases	De handelingen van IT-databasebeheerders en ontwikkelaars zijn gericht op continuïteit en optimalisatie van ICT-systemen.

B Maatregelen om persoonsgegevens te beschermen tegen misbruik

Organisatie van informatiebeveiliging en communicatieprocessen

- Instruct B.V. beschikt over een actief informatiebeveiligingsbeleid.
- informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- 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 op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- Er worden periodiek backups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze backups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.

Netwerk-, server-en applicatiebeveiliging en onderhoud

- De netwerkomgeving waarbinnen gegevens worden verwerkt is beveiligd. Daarbij worden verkeersstromen gescheiden en versleuteld.
- De digitale leermiddelen waarbinnen persoonsgegevens worden verwerkt worden getest op kwetsbaarheden voordat deze in productie worden genomen.
- Niet (meer) gebruikte informatie wordt verwijderd, ook uit backups.
- Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- De uitwisseling van persoonsgegevens aan derden in opdracht van de onderwijsinstelling vindt versleuteld plaats.

C Maatregelen om zwakke plekken te identificeren

het beveiligingsbeleid van Instruct B.V voorziet in interne processen om kwetsbaarheden te identificeren en op te lossen.

Rapportage

Bewerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via https://www.instruct.nl/

In het geval dat u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met Instruct B.V. via 0172-650983.

Versie

Deze bijlage is voor het laatst bijgewerkt op 17-03-2016.