Technische en organisatorische beveiligingsmaatregelen Learnbeat

Learnbeat, een product van Dedact BV, is een digitale leeromgeving voor het onderwijs waarbij persoonsgegevens worden verwerkt. In het 'Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen' is tussen aanbieders en de onderwijssectorraden vastgelegd dat een onderwijsinstelling in juridische zin de 'verantwoordelijke' is voor de verwerking van persoonsgegevens. Daardoor hebben en houden onderwijsinstellingen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt. Dedact BV is een 'bewerker', die uitvoering geeft aan de opdracht van een onderwijsinstelling. De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.

Bij het gebruik en de levering van Learnbeat zijn gegevens nodig die te herleiden zijn tot personen (zoals leerlingen). Dedact BV spant zich in deze persoonsgegevens zo goed mogelijk te beveiligen, en neemt hiervoor zowel technische als organisatorische beveiligingsmaatregelen. De afspraken die hiervoor gelden, zijn vastgelegd in de Bewerkersovereenkomst van Dedact BV. Dit document vormt een onlosmakelijk onderdeel van de Bewerkersovereenkomst. In dit document wordt specifieke informatie gegeven over Learnbeat en de genomen technische en organisatorische beveiliginsmaatregelen.

A. Omschrijving van de maatregelen zoals bedoeld in artikel 7.2

Bewerkersovereenkomst

I Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Dedact BV 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 de accountinformatie van de leerling en docent (voornaam, achternaam, gebruikersnaam, school, klas/groep, licentie-informatie). Medewerkers van de klantenservice hebben toegang tot de account van de leerling en docent om een specifieke vraag te beantwoorden of probleem te kunnen oplossen.	Verstrekken van gebruikersnamen en wachtwoorden aan docenten en leerlingen, eenmalig aan het begin van het schooljaar. Ondersteunen van docenten en leerlingen bij het gebruik van Learnbeat en het oplossen van problemen rondom gebruik, licenties, etc. Bij het loggen van problemen in andere systemen wordt het probleem algemeen omschreven. Administratieve handelingen ten behoeve van activatie en facturatie.
Analisten / deskundigen / redacteurs / uitgevers op het gebied van ontwikkeling van lesmateriaal hebben indien nodig toegang tot geanonimiseerde sets van resultaten van gebruik van leermiddelen voor het oplossen van eventuele problemen, fouten bij gebruik en het verkrijgen van inzicht in het gebruik van het lesmateriaal. In sommige gevallen is toegang tot de account van de leerling of docent noodzakelijk om een specifieke vraag te beantwoorden of probleem te kunnen oplossen.	Analyse van het lesmateriaal, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van het lesmateriaal en het adaptieve algoritme. Oplossen van onvolkomenheden in het lesmateriaal in zijn algemeenheid of specifieke gebruikers in het bijzonder.
IT- & databasebeheerders hebben toegang tot de centrale databases en back-ups van deze databases. Daarnaast hebben ontwikkelaars toegang tot de account van leerlingen of docenten met een specifiek probleem of vraag voor replicatie of analyse.	De handelingen van de IT- & databasebeheerders zijn gericht op beschikbaarheid, continuïteit en optimalisatie van ICT-systemen.

II 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

- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Dedact BV heeft een proces ingericht en gedocumenteerd voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Dedact BV stimuleert bewustzijn ten aanzien van privacy en 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.

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 omgevingen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie. Wijzigingen in applicaties worden getest op kwetsbaarheden voordat deze in productie worden genomen.
- Op systemen worden periodiek de laatste (beveiligings-)patches geïnstalleerd op basis van patchmanagement. Penetratietests en vulnerability assessments worden periodiek uitgevoerd.
- Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan. Medewerkers hebben hierdoor geen toegang tot de wachtwoorden van gebruikers.
- Er wordt voor alle gegevensuitwisseling gebruikt gemaakt van versleutelde verbindingen (https).

III Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

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

B. Rapportage (artikel 7.4 van de Bewerkersovereenkomst)

Bewerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via https://www.learnbeat.nl. In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Dedact via support@dedact.nl.

C. Contactgegevens

Dedact BV

3e Binnenvestgracht 23k

2312 NR LEIDEN

+31 (0)20-7009854

privacy@dedact.nl

D. Versie

Versie 1.1 voor het laatst aangepast op 24-10-2016

Deze bijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen -, een initiatief van de PO-Raad, VO-raad, de verschillende betrokken ketenpartijen (GEU, KBb-e en vDOD), het ministerie van Onderwijs, Cultuur en Wetenschappen en het ministerie van Economische Zaken.