BIJLAGE 2: BEVEILIGINGSBIJLAGE LEARNBEAT

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

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

Verwerker hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke Persoonsgegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie. Hieronder wordt uitgewerkt welke (groepen) medewerkers van de Bewerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

Groepen van medewerkers en Persoonsgegevens:	Handelingen:
Medewerkers van de klantenservice en accountmanagement hebben toegang tot de accountinformatie van de leerling en docent (voornaam, achternaam, e-mailadres, gebruikersnaam, school, klas/groep, licentieinformatie). 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 / redacteuren / 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	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.

tot de account van de leerling of docent noodzakelijk om een specifieke vraag te beantwoorden of probleem te kunnen oplossen.	
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.

Dedact heeft het Certificeringsschema van Edu-K toegepast als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor Learnbeat. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de toelichting bij eventuele afwijkingen van de standaarden.

Toetsvorm	Self-assessment		
Uitvoerder toets	Dedact BV, Frank van Rest, CTO		
BIV-classificatie	(Beschikbaarheid=3, Integriteit=3, Vertrouwelijkheid=2)		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Voldaan	
	Afhankelijkheden	Voldaan	
	Software	Voldaan	
	Logging/monitoring/testen	Voldaan	
	Actuele bedreigingen	Voldaan	
Integriteit	Herleidbaarheid	Niet voldaan	Implementatie verbeterde logging in de periode juni tot augustus (zomervakantie*) van 2018 waarmee herleidbaarheid gegarandeerd is.
	Functiescheiding	Andere	Toetsscores kunnen niet anders dan door

		maatregel	de applicatie (vanuit een docentrol) aangepast worden.
	Backup	Voldaan	
	Application controls	Voldaan	
	Manual controls	Voldaan	
	Onweerlegbaarheid	Niet voldaan	Implementatie verbeterde logging in de periode juni tot augustus (zomervakantie*) van 2018 waarmee onweerlegbaarheid gegarandeerd is.
	Actuele dreigingen	Alternatieve maatregel	Dagelijkse backups en live-replica database server beschermen de applicatie tegen actuele dreigingen.
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Fysieke toegang	Voldaan	
	Logische toegang	Voldaan	
	Opslag en transport	Voldaan	
	Logging	Niet voldaan	Implementatie verbeterde logging in de periode juni tot augustus (zomervakantie*) van 2018.
	Toetsing	Voldaan	
	Actuele dreigingen	Niet voldaan	Implementatie verbeterde logging in de periode juni tot augustus (zomervakantie*) van 2018 waarmee aan signalering actuele dreigingen voldaan wordt.

* Introductie tijdens de zomervakantie vanwege de impact van de wijziging en het daarmee gepaarde risico van downtime van de applicatie.

Organisatie van informatiebeveiliging en communicatieprocessen

- Verwerker beschikt over een actief informatiebeveiligingsbeleid
- Verwerker heeft een coördinator voor informatiebeveiliging (security officer) 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.

- Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers zijn geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.

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 Verwerker worden periodiek gecontroleerd aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging door Dedact BV. Daarnaast voorziet het beveiligingsbeleid van Verwerker in interne processen om kwetsbaarheden te identificeren.

Rapportage:

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via de inlogpagina van de applicatie, onder de knop ‘privacy’, zie: https://inloggen.learnbeat.nl.

In het geval u beveiligingsrisico’s constateert, verzoeken wij u contact op te nemen met de helpdesk van Verwerker via 020-7009854 of support@learnbeat.nl.

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met:

Learnbeat support
support@learnbeat.nl
020-7009854

De contactpersoon voor Verwerker is:

[contactgegevens Onderwijsinstelling voor beveiligingsincidenten]

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

Verwerker monitort 24/7 haar dienstverlening en heeft de in deze Bijlage opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een Datalek worden beoordeeld door de security officer van Verwerker, die analyseert of sprake kan zijn van een Datalek.

De wijze waarop informatie wordt gedeeld:

Wanneer zich een Datalek voordoet, wordt de Verwerkingsverantwoordelijke onderwijsinstelling door of namens Verwerker in beginsel binnen binnen 24 uur na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten.

Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk via de in de Privacy Bijsluiter opgenomen gegevens.

Verwerker deelt ten minste de volgende informatie wanneer zich een Datalek voordoet:

- De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, 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 eventuele/verdere schade te 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).

Indien een concrete situatie zich daartoe leent, dan kan Verwerker een (eerste) melding van een Datalek doen aan de Autoriteit Persoonsgegevens. De Onderwijsinstelling wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

Versie

versie 1.0
Deze bijlage is voor het laatst bijgewerkt op 25 mei 2018.

Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.