Bijlage 2

Beveiligingsbijlage

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.

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 licentieinformatie. Zij kunnen onder meer zien voor welke studenten een digitaal leermiddel is geactiveerd.	Administratieve handelingen in het kader van de werking van leermiddelen en licenties. Ondersteuning van de eindgebruiker.
Analisten / deskundigen op het gebied van ontwikkeling van lesmateriaal hebben toegang tot geanonimiseerde sets van resultaten van gebruik van leermiddelen, eventuele problemen/fouten bij gebruik	Analyse van het lesmateriaal, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van adaptief lesmateriaal, opsporing en verbetering van fouten in de werking van het digitale leermiddel.
IT-databasebeheerders hebben toegang tot de databases.	De handelingen van IT-databasebeheerders zijn gericht op 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

- Instruct B.V. beschikt over een actief informatiebeveiligingsbeleid.
- Instruct B.V. 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.
- Instruct B.V. heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.

- Instruct B.V. 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.

Beveiliging en continuïteit van de middelen, het netwerk, de server en de applicatie

Instruct B.V. heeft het Certificeringsschema gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor haar digitale leermiddelen.
(zie www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/)

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden

Toetsvorm	Self-assessment		
Uitvoerder toets	Instruct BV, alle productmanagers		
BIV-classificatie	**B**eschikbaarheid=2 **I**ntegriteit=2 **V**ertrouwelijkheid=2		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	**Voldaan**	
	Business continuity	**Voldaan**	
	Ontwerp	**Voldaan**	
	Monitoring	**Voldaan**	
	Testen	**Voldaan**	
	Software	**Voldaan**	
	Actuele dreigingen	**Voldaan**	
Integriteit	Herleidbaarheid (gebruikers)	**Voldaan**	
	Backup	**Voldaan**	
	Application controls	**Voldaan**	
	Onweerlegbaarheid	**Voldaan**	
	Herleidbaarheid (technisch beheer)	**Voldaan**	
	Controle integriteit	**Voldaan**	
	Onweerlegbaarheid	**Voldaan**	
	Actuele dreigingen	**Voldaan**	
Vertrouwelijkheid	Levenscyclus gegevens	**Niet voldaan**	**#1**
	Logische toegang	**Voldaan**	
	Fysieke toegang	**Voldaan**	
	Netwerk toegang	**Voldaan**	
	Scheiding omgevingen	**Alternatief**	**#2**
	Transport en fysieke opslag	**Niet voldaan**	**#3**
	Logging	**Voldaan**	
	Toetsing	**Voldaan**	
	Actuele dreigingen	**Voldaan**	

#1: De gegevens in de digitale leeromgevingen worden nu nog blijvend bewaard. Vanaf 4e kwartaal 2018 worden de gegevens automatisch drie jaar na laatste activiteit van de gebruiker verwijderd.
#2: In de testomgeving wordt een kopie van de productiedata gebruikt. Elke nieuwe kopie wordt vanaf medio 2018 geanonimiseerd.
#3: Instruct hanteert geen encryptie van fysieke opslag.

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 Instruct B.V. worden regelmatig gecontroleerd op veiligheid. Daarnaast voorziet het beveiligingsbeleid van Instruct B.V. in interne processen om kwetsbaarheden te identificeren.

Rapportage

Instruct B.V. actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via het privacystatement.
In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Instruct B.V. via mail: instruct@instruct.nl of telefoon: 0172 – 650983.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

- De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

  Instruct B.V. monitort 24/7 haar dienstverlening en heeft de in Bijlage 2 opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een Datalek worden beoordeeld door het **meldpunt datalek Instruct**, deze analyseert of sprake kan zijn van een Datalek.

- De wijze waarop informatie wordt gedeeld:

  Wanneer zich een Datalek voordoet zal Instruct B.V. met de verwerkersverantwoordelijke onderwijsinstelling in beginsel zonder onredelijke vertraging in overleg treden, na vaststelling dat sprake is van een Datalek.

- Instruct B.V. 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 Instruct B.V. 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

Deze bijlage is voor het laatst bijgewerkt op 14 mei 2018.

Deze privacy bijsluiter 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://ww.privacyconvenant.nl.