Bijlage 2

BEVEILIGINGSBIJLAGE

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

I. Toegang tot persoonsgegevens

VO-digitaal N.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/helpdesk 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.	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 (waaronder auteurs) 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 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. Maatregelen om persoonsgegevens te beschermen tegen misbruik

Organisatie van informatiebeveiliging en communicatieprocessen

- VO-digitaal beschikt over een actief informatiebeveiligingsbeleid.
- VO-digitaal 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.
- VO-digitaal heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers (zowel intern als extern) 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.

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

VO-digitaal heeft het Certificeringsschema (zie https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/) gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy. 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	VO-digitaal, Robin van Rootseler		
BIV-classificatie	Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=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	voldaan	
	Logische toegang	voldaan	
	Fysieke toegang	voldaan	

	Netwerk toegang	voldaan	
	Scheiding omgevingen	voldaan	
	Transport en fysieke opslag	Alternatieve maatregel	De gegevens worden door subverwerker True niet encrypted opgeslagen. De subverwerker is zelf ISO27001 gecertificeerd en heeft uitgebreide controls geïmplementeerd als het aankomt op de fysieke toegang tot het datacenter.
	Logging	voldaan	
	Toetsing	voldaan	
	Actuele dreigingen	voldaan	

III. Maatregelen om zwakke plekken te identificeren

De systemen van VO-digitaal N.V. zijn gecontroleerd op veiligheid door een extern bedrijf met expertise op het gebied van digitale veiligheid. Daarnaast voorziet het beveiligingsbeleid van VO-digitaal N.V. in interne processen om kwetsbaarheden te identificeren en op te lossen.

Rapportage

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

In het getal dat u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met VO-digitaal N.V. via 0316 820993.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

- *De wijze waarop monitoring en identificatie van Datalekken plaatsvindt*

VO-digitaal N.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 de security officer van VO-digitaal N.V., die analyseert of sprake kan zijn van een Datalek.

- *De wijze waarop informatie wordt gedeeld:*

Wanneer zich een Datalek voordoet, wordt de verwerkersverantwoordelijke onderwijsinstelling door of namens VO-digitaal N.V. in beginsel zonder onredelijke vertraging na vaststelling dat er 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.

- *VO-digitaal N.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 VO-digitaal N.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 03-04-2018.

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, 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.