Bijlage B

TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

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 (gepseudonimiseerde) 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

- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- VO-digitaal N.V. heeft een proces ingericht en gedocumenteerd 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.

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.
- Er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen (SSL). De uitwisseling van persoonsgegevens aan derden in opdracht van de onderwijsinstelling vindt versleuteld plaats.

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

Bewerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via http://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 verantwoordelijke onderwijsinstelling door of namens VO-digitaal N.V. in beginsel binnen 24 uur na ontdekking van het 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 28-08-2016.

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, 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://ww.privacyconvenant.nl.