Bijlage 2

Beveiligingsbijlage portal **AMN Insight**

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.

AMN Systems 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 licentie informatie. Zij kunnen onder meer zien voor welke onderwijsdeelnemers 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

- AMN Systems BV beschikt over een actief informatiebeveiligingsbeleid.
- AMN Systems BV 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.
- AMN Systems BV heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers zijn geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- AMN Systems BV 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

AMN Systems BV 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 voor de digitale leermiddelen. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Toets vorm	ISO 27001		
Uitvoerder toets	Lloyd's Register Nederland BV		
BIV-classificatie	Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=3		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	Voldaan	Zie ISO 27001 certificering
	Business continuity	Voldaan	Zie ISO 27001 certificering
	Ontwerp	Voldaan	Zie ISO 27001 certificering
	Monitoring	Voldaan	Zie ISO 27001 certificering
	Testen	Voldaan	Zie ISO 27001 certificering
	Software	Voldaan	Zie ISO 27001 certificering
	Actuele dreigingen	Voldaan	Zie ISO 27001 certificering
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	Zie ISO 27001 certificering
	Backup	Voldaan	Zie ISO 27001 certificering
	Application controls	Voldaan	Zie ISO 27001 certificering
	Onweerlegbaarheid	Voldaan	Zie ISO 27001 certificering
	Herleidbaarheid (technisch beheer)	Voldaan	Zie ISO 27001 certificering
	Controle integriteit	Voldaan	Zie ISO 27001 certificering
	Onweerlegbaarheid	Voldaan	Zie ISO 27001 certificering
	Actuele dreigingen	Voldaan	Zie ISO 27001 certificering

Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	Zie ISO 27001 certificering
	Logische toegang	Voldaan	Zie ISO 27001 certificering
	Fysieke toegang	Voldaan	Zie ISO 27001 certificering
	Netwerk toegang	Voldaan	Zie ISO 27001 certificering
	Scheiding omgevingen	Voldaan	Zie ISO 27001 certificering
	Transport en fysieke opslag	Voldaan	Zie ISO 27001 certificering
	Logging	Voldaan	Zie ISO 27001 certificering
	Toetsing	Voldaan	Zie ISO 27001 certificering
	Actuele dreigingen	Voldaan	Zie ISO 27001 certificering

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 AMN Systems BV worden [periodiek] gecontroleerd op veiligheid door Lloyd's Register Nederland BV. Daarnaast voorziet het beveiligingsbeleid van AMN Systems BV 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 www.amn.nl

In het geval dat u een beveiligingsrisico constateert, dan verzoeken wij u contact op te nemen met de helpdesk van AMN Systems BV via 026 3557344.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

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

AMN Systems BV 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 coördinator voor informatiebeveiliging van AMN Systems BV, die analyseert of er sprake kan zijn van een Datalek.

- *De wijze waarop informatie wordt gedeeld:*

Wanneer zich een Datalek voordoet, wordt de verwerkersverantwoordelijke onderwijsinstelling door of namens AMN Systems BV in beginsel zonder onredelijke vertraging 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 mediakanalen 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.

- AMN Systems BV *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 AMN Systems BV 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 3-5-2018

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.