Beveiligingsbijsluiter - Bijlage 2 bij de Verwerkersovereenkomst Noordhoff Uitgevers

Technische en organisatorische beveiligingsmaatregelen

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

Noordhoff Uitgevers 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 leerlingen een digitaal leermiddel is geactiveerd. De klantenservice heeft geen inzage in leerresultaten van 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 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

- Noordhoff Uitgevers heeft een privacy- en beveiligingsbeleid vastgesteld waarin de verschillende rollen worden omschreven. Belangrijk zijn onderstaande rollen.
- Noordhoff Uitgevers heeft een functionaris voor de gegevensbescherming, die hoofdzakelijk verantwoordelijk is voor het informeren en adviseren van Noordhoff Uitgevers over haar verplichtingen uit hoofde van de AVG en houdt toezicht op naleving. De verantwoordelijkheden van deze functionaris (DPO) staan beschreven in het hiervoor bestemde beleid van Infinitas.
- De Corporate Security Officer (CSO) is verantwoordelijk voor het beveiligingsbeleid van Infinitas.
- Infinitas heeft per dochteronderneming en per rechtsgebied een lokale privacycontactpersoon ("Privacy Contact") benoemd, die de taak heeft van directies van dochterondernemingen in samenwerking met de DPO het privacybeleid en de procedures van de entiteit uit te voeren en te ontwikkelen.

- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Noordhoff Uitgevers heeft een proces ingericht voor omgang met (en communicatie over) informatiebeveiligingsincidenten (datalek procedure).

Medewerkers

- Met alle medewerkers zijn in hun arbeidsvoorwaarden geheimhoudingsverklaringen overeengekomen.
- Noordhoff Uitgevers 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.

Fysieke beveiliging en continuïteit van de middelen

Noordhoff heeft het Certificeringsschema gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor haar producten waarop het Privacy Convenant ziet.

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

Toetsingskader versie 1.2. behorende bij het Certificeringsschema Informatiebeveiliging en Privacy ROSA

Toetsvorm	Self-assessment May 2018		
Uitvoerder toets	Infinitas Learning Holding B.V., Raymond van Koulil, security officer securityofficer@infinitaslearning.com voor Noordhoff Uitgevers B.V.		
BIV-classificatie	Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=2		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	Voldaan.	
	Business continuity	Alternatieve maatregel	De oplossingen van Noordhoff worden gehost op virtuele platformen, waarvan onderliggende hardware volledig redundant is.
	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	Niet voldaan.	Externe verbindingen maken gebruik van encryptie (https), maar interne verbindingen niet in alle gevallen.
	Logging	Voldaan.	
	Toetsing	Voldaan.	
	Actuele dreigingen	Voldaan.	

- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf. Er is een toegangsprotocol opgesteld. Toegang wordt bovendien geregistreerd.
- 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 back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.
- De locaties waar gegevens worden verwerkt zijn beveiligd door middel van sloten, alarmsystemen en videobewaking en worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's. Noordhoff Uitgevers beschikt over bedrijfscontinuïteitsplannen waarin uitwijklocaties zijn opgenomen.

Netwerk-, server- en applicatiebeveiliging en onderhoud

- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- De digitale leermiddelen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie (DTAP). Wijzigingen in applicaties worden getest op kwetsbaarheden voordat deze in productie worden genomen.
- Op systemen worden periodiek de laatste (beveiligings)patches geïnstalleerd op basis van patchmanagement.
- Gegevens die binnen applicaties worden verwerkt zijn geclassificeerd op risico's.
- Penetratietests en vulnerability assessments worden periodiek uitgevoerd.
- Niet (meer) gebruikte informatie wordt verwijderd.
- Op wachtwoorden zijn cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- Er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van de onderwijsinstelling vindt versleuteld plaats.

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 Noordhoff Uitgevers worden periodiek gecontroleerd op veiligheid. Daarnaast voorziet het beveiligingsbeleid van Noordhoff Uitgevers in interne processen om kwetsbaarheden te identificeren.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

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

Noordhoff Uitgevers monitort 24/7 haar dienstverlening en heeft maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een inbreuk in verband met persoonsgegevens worden beoordeeld door de Corporate Security Officer en functionaris voor gegevensbescherming van Noordhoff Uitgevers, die analyseert of sprake kan zijn van een inbreuk in verband met persoonsgegevens, het type inbreuk en of dit een inbreuk betreft die valt onder haar rol als verwerker of haar rol als verwerkingsverantwoordelijke.

- *De wijze waarop informatie wordt gedeeld:*

Wanneer zich een inbreuk in verband met persoonsgegevens voordoet ten aanzien van persoonsgegevens die Noordhoff Uitgevers verwerkt als verwerker, wordt de verwerkingsverantwoordelijke door of namens Noordhoff Uitgevers binnen 24 uur na vaststelling dat sprake is van een inbreuk 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.

- *Noordhoff Uitgevers deelt de volgende informatie aan verwerkingsverantwoordelijken wanneer zich een inbreuk in verband met persoonsgegevens 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 Noordhoff Uitgevers een (eerste) melding van een inbreuk in verband met persoonsgegevens doen bij de autoriteit. De verwerkingsverantwoordelijke wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

Versie

Deze bijlage is voor het laatst bijgewerkt op 2 juli 2018.

Deze privacy bijsluiter maakt deel 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 over het privacybeleid van Noordhoff Uitgevers is te vinden op www.noordhoffuitgevers.nl/privacy.