BIJLAGE 2: BEVEILIGINGSBIJLAGE

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

I. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

(Groepen van) medewerkers die toegang hebben tot welke Persoonsgegevens:	Handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.
Medewerkers van Uitgeverij Essener hebben toegang tot het overzicht van de deelnemende scholen, de naam en het e-mailadres van de opgegeven schoolbeheerders, docenten en het aantal afgenomen licenties.	Administratieve handelingen in het kader van het aanmaken, bewerken en verwijderen van scholen, licenties en schoolbeheerders.
IT-databasebeheerders en softwareontwikkelaars hebben toegang tot de software en de databases.	De handelingen zijn gericht op de ontwikkeling en het onderhoud van de ICT-systemen.
Schoolbeheerders	Schoolbeheerders kunnen mutaties aanbrengen in persoonsgegevens van leerlingen en docenten op hun school alsook opgeven welke klassen deelnemen aan de digitale lesomgeving.
Docenten	Docenten kunnen mutaties aanbrengen in persoonsgegevens van leerlingen Docenten hebben inzicht in de antwoorden en resultaten van de leerlingen waar ze les aan geven. Ook kunnen ze de persoonsgegevens van leerlingen wijzigen.

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

- Uitgeverij Essener beschikt over een actief informatiebeveiligingsbeleid.
- Uitgeverij Essener 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.
- Uitgeverij Essener heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Uitgeverij Essener 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.

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

Uitgeverij Essener 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	Uitgeverij Essener		
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	Alternatieve maatregel	Per augustus voorziet het systeem in geautomatiseerde monitoring (en alarmering) van ongeautoriseerde veranderderende programmeercodes.
	Onweerlegbaarheid	voldaan	
	Herleidbaarheid (technisch	voldaan	

	beheer)		
	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 Logging	Alternatieve maatregel	De gegevens worden door subverwerker Exonet niet encrypted opgeslagen. De subverwerker is zelf ISO9001, ISO27001 en NEN7510 gecertificeerd en heeft uitgebreide maatregelen geïmplementeerd als het aankomt op de fysieke toegang tot het datac*en*ter.
	Toetsing	voldaan	
	Actuele dreigingen	voldaan	

Rapportage

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via https://www.essener.nl/privacy
In het getal dat u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met Uitgeverij Essener via 075 621 72 91 en info@essener.nl

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

Uitgeverij Essener 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 Uitgeverij Essener die analyseert of sprake kan zijn van een Datalek.

De wijze waarop informatie wordt gedeeld

- Wanneer zich een Datalek voordoet zal Uitgeverij Essener met de verwerkersverantwoordelijke onderwijsinstelling in beginsel zonder onredelijke vertraging in overleg treden, na vaststelling dat sprake is van een Datalek. Afhankelijk van de situatie, kan ook informatie worden gedeeld

via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten.

- 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.

Uitgeverij Essener 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 Uitgeverij Essener 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.

In geval van een (vermoeden van) beveiligingsincident en/of Datalek, kan Onderwijsinstelling contact opnemen met: Uitgeverij Essener, 075 621 72 91 en info@essener.nl

De contactpersoon voor Verwerker is: Maayke Bongenaar

Versie 2.2: 4-6-2018

Deze Beveiligingsbijlage 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://www.privacyconvenant.nl