BIJLAGE 2: 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. 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 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 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.

Meer in het bijzonder de uitwerking van de door Bewerker getroffen technische en organisatorische (beveiligings-)maatregelen en de daarbij gehanteerde beveiligingsnorm.

- De softwareontwikkelaar betrachten grote voorzichtigheid bij de ontwikkeling van software. Ontwikkelaars zijn zich zeer bewust van de gevaren van een datalek.
- Met medewerkers (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen.
- Er wordt dagelijks een back-up van de gegevens gemaakt. Bij dataverlies wordt de originele data binnen twee uur hersteld.
- Identificatie, authenticatie en autorisatie en alle overige dataoverdracht vindt enkel plaats middels een versleutelde verbinding.

- 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.

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.

- Jaarlijks wordt een Pentest uitgevoerd t.b.v. van het opsporen van (mogelijke) datalekken.

Rapportage (artikel 7.4 van de Bewerkersovereenkomst

Bewerker rapporteert periodiek met een frequentie van 1 maal per jaar, uiterlijk op 1 augustus aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

- Subbewerkers rapporteren aan Essener over updates of beveiligingsincidenten. De bewerker actualiseert de informatie en informeert contractpartijen en/of gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen.
- Essener communiceert haar maatregelen rondom de technische en organisatorische maatrelen jaarlijks via de privacy bijsluiter. De intentie is om dit samen met de aanschaf van het producten te laten verstrekken (door distributeur). Hierdoor is er geen aparte administratie benodigd t.a.v. bewerkersovereenkomst en privacy bijsluiter en zal de administratieve belasting voor de school en de uitgeverij idealiter minimaal zijn.
- Wet Meldplicht datalekken: Essener heeft een protocol voor datalekken ingericht waarbij er bij calamiteiten. In het geval een beveiligingslek en/of datalek zal Bewerker Verantwoordelijke binnen 24 uur daarover informeren, naar aanleiding waarvan Verantwoordelijke beoordeelt of zij de betrokkenen zal informeren of niet. Verantwoordelijke is en blijft verantwoordelijk voor een eventuele wettelijke verplichting daartoe.
- Updates rondom het privacystatement worden weergegeven op www.essener.nl/privacy.
- In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Essener: 075-6217291, info@essener.nl en support@essener.nl.

Versie 1 (augustus 2017)

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.