

## Bijlage 2 Beveiligingsbijlage

(Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst)

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

De Basisacademie 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 en op welke school deze leerlingen zitten. | Ondersteuning van de eindgebruiker<br>Administratieve handelingen in het kader van de werking van leermiddelen en licenties.  |
| Deskundigen, analisten en redacteurs hebben ten behoeve van verbetering van de kwaliteit van het leermiddel toegang tot resultaten van gebruik van leermiddelen.   | Activiteiten gericht op optimalisatie van het lesmateriaal.<br>Alle handelingen zijn geanonimiseerd   |
| Trainers/onderwijskundig begeleiders hebben toegang tot resultaten op school- en/of klasniveau ten behoeve van maatwerkondersteuning van docenten/schoolmanagement.  | Activiteiten gericht op onderwijskundig-didactische instructie, training en begeleiding op verzoek van de school.   |
| IT-databasebeheerders en ontwikkelaars hebben toegang tot de databases   | Analyse van lesmateriaal, opsporing en verbetering fouten in de werking van het digitale leermiddel ondersteuning van de eindgebruiker, reset van leerlingresultaten op verzoek van de docent |

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

## Medewerkers

Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt. Uitgeverij Basisacademie 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

De Basisacademie heeft het Certificeringsschema (zie [https://www.edustandaard.nl/standaard\\_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/](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 SCORE. Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

| Toetsvorm                | Self-assessment  |  |   |
|--------------------------|--|--|---|
| Uitvoerders toets        | Emmia B.V.: Mark Siebeler, directeur en Basisacademie B.V.: Marijke Tiemersma, directeur |  |   |
| BIV-classificatie        | 3-2-2  |  |   |
| Categorie                | Maatregelen  | Compliance   | Uitleg  |
|                          |  | [Voldaan/<br>niet voldaan/<br>alternatieve<br>maatregel] | Bij niet voldaan<br>aangeven<br>hoe/wanneer dit<br>wordt gecorrigeerd. Bij<br>alternatieve maatregel<br>deze beschrijven] |
| <b>Beschikbaarheid</b>   | Overbelasting  | Voldaan: niveau 2  |   |
|                          | Business continuity  | Voldaan: niveau 2  |   |
|                          | Ontwerp  | Voldaan: niveau 2  |   |
|                          | Monitoring   | Voldaan: niveau 2  |   |
|                          | Testen   | Voldaan: niveau 2  |   |
|                          | Software   | Voldaan: niveau 2  |   |
| <b>Integriteit</b>       | Actuele dreigingen   | Voldaan: niveau 2  |   |
|                          | Herleidbaarheid (gebruikers)   | Voldaan: niveau 1  |   |
|                          | Backup   | Voldaan: niveau 2  |   |
|                          | Application controls   | Voldaan: niveau 2  |   |
|                          | Onweerlegbaarheid  | Voldaan: niveau 1  |   |
|                          | Herleidbaarheid (technisch<br>beheer)  | Voldaan: niveau 2  |   |
|                          | Controle integriteit   | Voldaan: niveau 1  |   |
| <b>Vertrouwelijkheid</b> | Onweerlegbaarheid  | Voldaan: niveau 1  |   |
|                          | Actuele dreigingen   | Voldaan: niveau 2  |   |
|                          | Levenscyclus gegevens  | Voldaan: niveau 2<br>Per 2 jaar                          |   |
|                          | Logische toegang   | Niet voldaan   | Wordt schooljaar<br>2018-2019 uitgevoerd<br>door Emmia  |
|                          | Fysieke toegang  | Voldaan: niveau 2  |   |
|                          | Netwerk toegang  | Voldaan: niveau 2  |   |
|                          | Scheiding omgevingen   | Niet voldaan   | Wordt schooljaar<br>2018-2019 uitgevoerd<br>door Emmia  |

|  |                             |                   |                             |
|--|-----------------------------|-------------------|-----------------------------|
|  | Transport en fysieke opslag | Voldaan: niveau 2 |                             |
|  | Logging                     |                   | Wordt uitgevoerd door Emmia |
|  | Toetsing                    | Voldaan: niveau 1 |                             |
|  | Actuele dreigingen          | Voldaan: niveau 1 |                             |

### 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 Basisacademie worden vanaf 2018 jaarlijks gecontroleerd op veiligheid. Daarnaast voorziet het beveiligingsbeleid van Basisacademie in interne processen om kwetsbaarheden te identificeren.

#### Rapportage

De Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via <https://www.basisacademie.nl>. En indien nodig via SCORE.

In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van de Basisacademie B.V. via [info@basisacademie.nl](mailto:info@basisacademie.nl) of telefonisch via 058 2501656.

#### Informereren over Datalekken en/of incidenten met betrekking tot beveiliging

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

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

- **De wijze waarop informatie wordt gedeeld**

Wanneer zich een Datalek voordoet, wordt de verwerkersverantwoordelijke onderwijsinstelling door of namens de Basisacademie 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 media kanalen en/of officiële distributeurs en/of handelsagenten.

Voor vervolgvragen of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk via de in de Privacy Bijsluiting opgenomen gegevens.

- **Uitgeverij Basisacademie 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 de Basisacademie 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 25 mei 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>.*