BIJLAGE 2: BEVEILIGINGSBIJLAGE

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 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.

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.

Driestar Educatief hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens, zoals in de tabel hieronder aangegeven. Geauthoriseerde medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Medewerkers en gegevens:	Handelingen:
Helpdesk heeft waar nodig in opdracht van het samenwerkingsverband toegang tot persoonsgegevens.	Opsporen van oorzaken van foutsituaties om deze te herstellen en herhaling te voorkomen.

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

- Driestar Educatief beschikt over een actief informatiebeveiligingsbeleid. Driestar Educatief heeft een security officer om risico's rond de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die toezien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Driestar Educatief heeft procedures ingericht voor de behandeling van en communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers zijn geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Driestar Educatief 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

Driestar Educatief heeft het Certificeringsschema van Edu-K gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor Kindkans (https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/). Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Toetsvorm	Asssessment door softwareleverancier		
Uitvoerder toets	Educator B.V., Emil van den Berg, Lead engineer		
BIV-classificatie	Beschikbaarheid=1, Integriteit=2, Vertrouwelijkheid=3		
Categorie	**Maatregelen**	**Compliance**	**Uitleg**
Beschikbaarheid	Overbelasting	Voldaan	
	Business continuity	Voldaan	
	Ontwerp	Voldaan	
	Monitoring	Voldaan	
	Testen	Voldaan	
	Software	Gedeeltelijk voldaan	Verouderde techniek (frameworks) wordt momenteel vervangen .
	Actuele dreigingen	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Gedeeltelijk voldaan	Mogelijk maken wijzigingen terug te draaien; hier wordt nog niet aan voldaan.
	Backup	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Gedeeltelijk voldaan	Logging als een gebruiker gegevens wijzigt; hier wordt nog niet aan 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	Voldaan	
	Logging	Gedeeltelijk voldaan	Monitoren wanneer de logging wordt ingezien; hier wordt nog niet aan voldaan.
	Toetsing	Gedeeltelijk voldaan	Toetsing wordt uitgevoerd bij vervangen van verouderde frameworks.
	Actuele dreigingen	Gedeeltelijk voldaan	Inbouwen van automatische detectie van verdacht netwerkverkeer; is nog niet gedaan.

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.

Het informatiebeveiligingsbeleid van Driestar Educatief voorziet in interne processen om kwetsbaarheden te identificeren.

Rapportage

Driestar Educatief actualiseert haar beveiligingsmaatregelen voortdurend en informeert gebruikers via de gebruikelijke kanalen binnen Kindkans over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik.

In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Kindkans.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

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

Driestar Educatief 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 Driestar Educatief, die analyseert of sprake kan zijn van een Datalek. Indien er sprake is van een Datalek wordt de binnen Driestar Educatief gehanteerde datalekprocedure gevolgd.

- *De wijze waarop informatie wordt gedeeld:*

Wanneer zich een Datalek voordoet, wordt de verwerkersverantwoordelijke door of namens Driestar Educatief zonder onredelijke vertraging na vaststelling dat sprake is van een Datalek per e-mail geïnformeerd.

Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden opgenomen met de helpdesk van Kindkans via de in de Privacy Bijsluiter opgenomen gegevens.

- *Driestar Educatief 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 Driestar Educatief 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.

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: [contactgegevens helpdesk/servicedesk voor beveiligingsincidenten]

Naam: < dhr. C.M. Codee>

E-mail: < C.M.Codee@driestar-educatief.nl >

Tel.: < 0182 540333 >

Bij afwezigheid:

Naam: < dhr. A.M.Vollmuller >

E-mail: < A.M.Vollmuller@driestar-educatief.nl >

Tel.: <0182-540333 >

Informeren over Datalekken

Er is een procedure over het informeren in geval van datalekken met betrekking tot beveiliging, en bevat de volgende punten voor zover bekend bij Verwerker:

- De wijze waarop monitoring en identificatie van datalekken plaatsvindt,
- De wijze waarop informatie wordt gedeeld:
  - Op welke manier (via e-mail);
  - Aan wie gericht (contactpersonen en contactgegevens);
  - Met wie kan (bij vervolgacties) contact worden opgenomen.
- Informatie die in ieder geval over een datalek gedeeld moet worden
  - 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 datalek;
  - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
  - Benoemen van betrokkenen die gevolgen kunnen ondervinden van het datalek, en de mate waarin;
  - De omvang van de groep betrokkenen;
  - Het soort gegevens dat door het datalek wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).