

Bijlage 2: Beveiligingsbijlage

Behorende bij verwerkersovereenkomst (digitale) leermiddelen en educatieve diensten, van Blink Educatie VO BV

Versie: 01-08-2022

Blink Educatie VO BV heeft, overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst passende technische en organisatorische maatregelen genomen om de verwerking van persoonsgegevens aantoonbaar te beveiligen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

1. Maatregelen die Blink Educatie VO BV heeft genomen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.

- Een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
- Een systeem van autorisatie waardoor enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie;
- Er is een coördinator informatiebeveiliging die de risico's omtrent de verwerking van persoonsgegevens inventariseert, het beveiligingsbewustzijn stimuleert, voorzieningen controleert en maatregelen treft die zien op naleving van het informatiebeveiligingsbeleid. Deze coördinator is bereikbaar op het volgende emailadres: privacy@blink.nl
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid;
- Er is een proces ingericht voor communicatie over informatiebeveiligingsincidenten;
- Met medewerkers worden geheimhoudingsverklaringen afgesloten en worden informatiebeveiligingsafspraken gemaakt;
- Het bewustzijn, opleiding en training ten aanzien van informatiebeveiliging wordt gestimuleerd.

2. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden, zoals beschreven in het Certificeringsschema informatiebeveiliging en privacy ROSA. Zie: https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/.

Toetsvorm	Self assessment		
Uitvoerder toets	Thomas van der Slot, Developer, Blink Educatie VO BV		
Inlogpagina	https://docent.blinknederlands.nl , https://leerling.blinknederlands.nl , https://docent.plot26.nl , https://leerling.plot26.nl , https://docent.saga.nl https://leerling.saga.nl , https://docent.wired.nl , https://leerling.wired.nl		
BIV-classificatie	Beschikbaarheid = Hoog Integriteit = Midden Vertrouwelijkheid = Midden		
Categorie	Maatregelen	Compliance	Uitleg
Beschikbaarheid	Ontwerp	voldaan	
	Capaciteit beheer	niet voldaan	Er is nog geen actieve signalering om extra resources toe te wijzen. Dit vindt plaats door periodieke monitoring bij issues.
	Onderhoud	voldaan	
	Testen	niet voldaan	Er is nog geen planning om regressie- en loadtesten in te voeren.
	Monitoring	voldaan	
	Herstel	niet voldaan	Er is een 'Warm Standby' aanwezig. Nieuwe infrastructuur kan gelijk in gebruik genomen worden, maar vergt nog wel enkele handelingen. Herstel van de dienst duurt tot op heden maximaal 24 uur, dit wordt in schooljaar 2022-2023 verbeterd.
Integriteit	Herleidbaarheid (gebruikers)	niet voldaan	In het schooljaar 2022-2023 is gepland om inzicht en herleidbaarheid in wijzigingen (logging) te verbeteren.

	Backup	niet voldaan	In het schooljaar 2022-2023 is de implementatie van een periodieke controle van de integriteit van de back-up (logging) ingepland.
	Application controls	voldaan	
	Onweerlegbaarheid	niet voldaan	Inlogactiviteit wordt gelogd, maar wordt nog niet periodiek gecontroleerd. In het schooljaar 2022-2023 wordt dit opgepakt.
	Herleidbaarheid (technisch beheer)	voldaan	
	Controle integriteit	niet voldaan	Er is nog geen planning om secure software development guidelines en een structurele controle van de integriteit van de configuratie en software toe te passen.
	Onweerlegbaarheid (toepassing)	niet voldaan	In schooljaar 2022-2023 is gepland om de inlogactiviteit (technisch beheer) te gaan loggen.
Vertrouwelijkheid	Levenscyclus gegevens	voldaan	
	Logische toegang	niet voldaan	Er is nog geen planning voor de implementatie van twee-factor authenticatie voor beheerdersrollen.
	Fysieke toegang	voldaan	
	Netwerk toegang	voldaan	
	Scheiding omgevingen	niet voldaan	Er is nog geen planning voor de anonimisering van productiedata in testomgevingen
	Transport en fysieke opslag	voldaan	
	Logging	niet voldaan	Voor het schooljaar 2022-2023 staat een project gepland om de logging te verbeteren.
	Omgaan met kwetsbaarheden	voldaan	

3. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Blink Educatie VO BV heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zullen wij de verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- De kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk, samenvatting van de inbreuk waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (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 de inbreuk;
- Hoe de inbreuk is ontdekt;
- De maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- Of de bij de inbreuk betrokken gegevens versleuteld, gehasht etc. waren;
- Benoemen van groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep Betrokkenen;
- Wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor betrokkene(n);
- De hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere gegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van) beveiligingsincident en/of Datalek zal onze coördinator informatiebeveiliging, in beginsel per email contact opnemen met de contactpersoon van de Onderwijsinstelling die is vermeld in bijlage 4. De coördinator informatiebeveiliging is tevens aanspreekpunt voor het geval de Onderwijsinstelling contact wil opnemen over een beveiligingsincident en/of Datalek. De coördinator informatiebeveiliging is bereikbaar op het volgende mailadres: privacy@blink.nl

Paraaf



Onderwijsinstelling

Verwerker

Deze bijlage is opgezet volgens het branche-specifieke format van MEVW en vormt een integraal onderdeel van de bijbehorende verwerkersovereenkomst. Verwerkersovereenkomst en de bijlagen daarbij maken onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (MEVW, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>.