Verwerkersovereenkomst Zien! 4.0 november 2022
Bijlage 2: beveiligingsbijlage

Versie 4.0, november 2022

Burgemeester Jamessingel 2
2803 PD GOUDA
KvK 81749481
info@gouwe-academie.nl
www.gouwe-academie.nl

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

A. Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking

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

Gouwe Academie hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke gegevens, zoals in de tabel hieronder aangegeven. Geautoriseerde 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 school(bestuur) toegang tot persoonsgegevens.	Opsporen van oorzaken van foutsituaties om deze te herstellen en herhaling te voorkomen.

De accounts van deze medewerkers zijn voorzien van sterke wachtwoorden.

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.

Verwerker past de volgende technische en organisatorische maatregelen toe om de Persoonsgegevens te beschermen:

- Toegang tot (productie)platformen is beperkt tot een kleine groep medewerkers die daar beheerwerkzaamheden moeten uitvoeren. Alle toegang tot (productie)platformen vinden plaats met persoonlijke accounts die via een aanvullend beveiligingsplatform (KeyHub) beveiligd zijn tegen oneigenlijk gebruik. Daarbij wordt alle toegang tot de platformen gelogd.
- Het technische platform is ondergebracht in een hostingcentrum dat ISO 9001 en 27001:2013 gecertificeerd is.
- De gegevensdrager (database) is fysiek gescheiden van het platform waarmee de eindgebruikers communiceren (de webserver). De gegevensdrager heeft geen directe verbinding met het Internet.
- Al het transport van gegevens vindt plaats over beveiligde verbindingen (SSL). Dit geldt ook voor koppelingen met andere systemen waarbij TLS 1.2 als standaard wordt gesteld.
- Geautoriseerde gebruikers krijgen toegang tot het systeem via persoonlijke accounts die door de scholen (de Verantwoordelijke) beheerd worden. Daarbij wordt aan elk account een rol gekoppeld die aangeeft welke Persoonsgegevens het account mag zien.
- Een geautoriseerde gebruiker met een rol heeft alleen toegang tot de groep en leerling gegevens als hij/zij daar daadwerkelijk aan gekoppeld zit. Een docent heeft bijvoorbeeld standaard alleen toegang tot de leerlingen binnen de lesgroepen waar hij/zij les aan geeft.
- Persoonlijke accounts worden middels een combinatie van gebruikersnaam/wachtwoord beveiligd.

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.

- Verwerker voert continu (minimaal één keer per maand) controles uit op eventuele kwetsbaarheden in de door haar gebruikte infrastructuur en softwarecomponenten van derden, en werkt deze waar nodig bij.

- Verwerker laat eigen medewerkers regelmatig het systeem toetsen op kwetsbaarheden en herstelt deze waar nodig.

B. 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. Verwerker gebruikt hiervoor in beginsel het 'Certificeringsschema informatiebeveiliging en privacy ROSA' (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.

Toetsvorm	Self-assessment
Uitvoerder toets	Educator B.V., Emil van den Berg, Lead engineer
Inlogpagina	https://start.start.zienvooronderwijs.nl
BIV-classificatie	Beschikbaarheid = L, Integriteit = M, Vertrouwelijkheid =H

Categorie	Maatregelen	Compliance	Uitleg
		[Voldaan/ Niet voldaan/ Alternatieve maatregel]	[Bij "Niet voldaan" aangeven hoe/wanneer dit wordt gecorrigeerd. Bij "Alternatieve maatregel" deze beschrijven.]
Beschikbaarheid	Ontwerp	Voldaan	
	Capaciteit beheer	Voldaan	
	Onderhoud	Voldaan	
	Testen	Voldaan	
	Monitoring	Voldaan	
	Herstel	Voldaan	
Integriteit	Herleidbaarheid (gebruikers)	Gedeeltelijk voldaan	Mogelijk maken wijzigingen terug te draaien Leerkrachtlijst: voldaan. Leerlinglijst: niet voldaan. Plannen: niet voldaan.
	Back-up	Voldaan	
	Application controls	Voldaan	
	Onweerlegbaarheid	Gedeeltelijk voldaan	Logging als een gebruiker gegevens wijzigt. Leerkrachtlijst: voldaan. Leerlinglijst: niet voldaan Plannen: niet voldaan.
	Herleidbaarheid (technisch beheer)	Voldaan	
	Controle integriteit	Voldaan	
	Acute dreigingen	Gedeeltelijk voldaan	Er is sprake van detectie van verdacht verkeer, maar niet voldaan op automatische detectie.
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan	
	Logische toegang	Voldaan	
	Fysieke toegang	Voldaan	
	Netwerktoegang	Voldaan	

Categorie	Maatregelen	Compliance	Uitleg
	Scheiding omgevingen	Voldaan	
	Transport en fysieke opslag	Voldaan	
	Logging	Niet voldaan.	Monitoren wanneer de logging wordt ingezien. Intentie is om dit in 2024 te realiseren.
	Omgaan met kwetsbaarheden	Voldaan	

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

Verwerker 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 zal Verwerker 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 welk onderdeel van de beveiliging heeft het betrekking, 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 Persoonsgegevens versleuteld, gehasht etc. waren;
- de groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen;
- wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor de groep(en) Betrokkene(n);
- de hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens 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 een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Verwerker in beginsel per e-mail contact met elkaar opnemen via onderstaande contactgegevens, dan wel de contactgegevens zoals opgenomen in Bijlage 4.

	Contactpersoon bij beveiligingsincidenten/Datalekken	Contactgegevens (e-mail en telefoonnummer)
Verwerker	Dhr. C.M. Codee	C.M.Codee@driestar-educatief.nl, (0182) 540333
Verwerker (bij afwezigheid)	Dhr. A.M. Vollmuller	a.m.vollmuller@gouwe-academie.nl (0182) 540333
Onderwijsinstelling		

Bijlage 2 (Beveiligingsbijlage) maakt 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 op www.privacyconvenant.nl.