

Bijlage 2: Beveiligingsbijlage

Behorende bij verwerkersovereenkomst lesmateriaal onder de merknaam Proeftuin en/of Grondstof en/of LEF en/of Blauwdruk, van LesLab Holding B.V.

Versie: 20-5-2025

LesLab Holding B.V. 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 LesLab Holding B.V. 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;
- LesLab heeft geen formeel aangewezen coördinator informatiebeveiliging. Meldingen van beveiligingsincidenten of datalekken kunnen worden gericht aan: info@leslab.nl

Deze mailbox wordt actief gemonitord door het kernteam van LesLab. Indien nodig wordt afgestemd met technische partners of de betreffende school.

- 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/.

Aanvulling bij self-assessment: meerdere domeinen, uniforme softwareomgeving

Deze self-assessment is gezamenlijk uitgevoerd door LesLab en subverwerker Paqt B.V., op basis van de EduBIV-richtlijn. Er is geen externe auditor betrokken geweest.

De beoordeling is uitgevoerd op het domein <https://mijnproeftuin.nl/login>. Dit domein maakt gebruik van dezelfde softwarestack, infrastructuur en beveiligingsarchitectuur als de andere onderliggende platforms van LesLab, waaronder mijn-lef.nl, grondstofloopbaan.nl, blauwdrukburgerschap.nl, en eventuele andere subdomeinen.

Alle domeinen draaien op één uniforme softwareomgeving, met identieke rechtenstructuren, databasearchitectuur, hosting, logging en back-upsystemen. Daardoor zijn de uitkomsten van de assessment representatief voor alle bij deze overeenkomst betrokken leeromgevingen.

Toetsvorm	Self-assessment
Uitvoerder toets	PAQT b.v. in samenwerking met LesLab
Inlogpagina	<ul style="list-style-type: none"> https://mijnproeftuin.nl/login (https://mijnproeftuin.nl/login (representatief voor alle domeinen met uniforme software))
BIV-classificatie	<p>BIV-classificatie: Beschikbaarheid = M, Integriteit = L/M, Vertrouwelijkheid = H</p> <p><i>Toelichting:</i> Deze inschatting is gebaseerd op de EduBIV-richtlijn en gangbare AVG-interpretaties voor digitale leermiddelen.</p> <ul style="list-style-type: none"> Beschikbaarheid = M: De applicatie ondersteunt lessen en verwerking van opdrachten, maar tijdelijke uitval heeft geen directe gevolgen voor veiligheid of toetsing. Integriteit = L/M: Leerlingen voeren zelf gegevens in (zoals antwoorden en keuzes) en kunnen deze tot goedkeuring aanpassen. Er is zelden sprake van definitieve registraties die bij vergissingen onherstelbare schade veroorzaken. Vertrouwelijkheid = H: De omgeving bevat persoonsgegevens van leerlingen en docenten (zoals naam, e-mailadres, school en inloggegevens), waarvoor passende toegangsbescherming vereist is. <p>LesLab Holding B.V. is formeel hoofdverwerker en draagt zorg voor organisatorische borging van de beveiliging, zoals contractbeheer, verwerkersovereenkomsten en privacy-by-design.</p> <p>De technische verwerking van persoonsgegevens – inclusief hosting, beveiliging, datatransport en opslag – is volledig uitbesteed aan subverwerker Paqt B.V., die ISO 27001-gecertificeerd is.</p> <p>Deze rolverdeling sluit aan bij artikel 28 van de AVG en is vastgelegd in de bijbehorende subverwerkersovereenkomst.</p>

Categorie	Maatregelen	Compliance	Uitleg
Beschikbaarheid	Ontwerp	Voldaan	De technische omgeving is redundant opgezet door ISO 27001-gecertificeerde subverwerker.
	Capaciteit beheer	Voldaan	Schaalbaarheid is ingericht en bewaakt via monitoring en capaciteitsbeheer.
	Onderhoud	Voldaan	Onderhoud wordt gepland buiten schooltijden en volgens change management-procedure.
	Testen	Voldaan	Technische updates worden getest; volledige herstelprocedures worden in samenwerking met subverwerker Paqt periodiek geëvalueerd en getest.
	Monitoring	Voldaan	Uptime, serverbelasting en verdachte patronen worden proactief gemonitord.
	Herstel	Voldaan met kanttekening	Back-ups worden dagelijks gemaakt; herstel is getest, maar failover-procedure wordt Q4 2025 herzien.
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	Gebruikersacties (zoals antwoorden of aanpassingen) worden automatisch gelogd en gekoppeld aan account-ID's en tijdstempels.
	Backup	Voldaan	Er worden dagelijkse versleutelde back-ups gemaakt met een retentie van 30 dagen. Opslag vindt plaats in een apart datacluster.
	Application controls	Voldaan	De applicatie hanteert invoervalidaties, rolgebaseerde toegang en controle op manipulatie.
	Onweerlegbaarheid	Voldaan met kanttekening	Er is geen digitale ondertekening van

			leeractiviteiten, maar audittrails bevatten voldoende metadata voor herleidbaarheid.
	Herleidbaarheid (technisch beheer)	Gedeeltelijk voldaan	Logbestanden zijn beschikbaar en worden bewaard, maar er is nog geen koppeling aan een geautomatiseerde meldprocedure.
	Controle integriteit	Voldaan	Bij opslag en overdracht worden integriteitscontroles uitgevoerd op basis van hashes. Er zijn geen incidenten gemeld waarbij data onbedoeld is gewijzigd.
	Onweerlegbaarheid (toepassing)	Voldaan	De applicatie toont bewerkingsgeschiedenis bij eindopdrachten; gebruikers kunnen niet ongemerkt gegevens wijzigen na goedkeuring.
Vertrouwelijkheid	Levenscyclus gegevens	Voldaan met kanttekening	Leerlinggegevens worden automatisch verwijderd na afloop van de bewaartermijn. Pro-actief gegevens verwijderen door een school is (nog) niet mogelijk.
	Logische toegang	Voldaan	Alleen geautoriseerde gebruikers hebben toegang tot specifieke gegevens; beheerders maken gebruik van 2FA via Toegang.org.
	Fysieke toegang	Voldaan	De datacenters van de subverwerker (of diens onderaannemers) voldoen aan ISO 27001 en beschikken over fysieke beveiligingsmaatregelen conform die norm. Voor regels rond beveiliging bij LesLab zelf, zie bijlage 2.4
	Netwerk toegang	Voldaan	Alleen verbindingen vanaf goedgekeurde IP-ranges zijn toegestaan;

			alle verkeer verloopt via HTTPS/TLS.
	Scheiding omgevingen	Voldaan	Ontwikkel-, test- en productieomgevingen zijn logisch en fysiek van elkaar gescheiden.
	Transport en fysieke opslag	Voldaan	Alle data wordt versleuteld tijdens transport én bij opslag (AES-256); fysieke dragers zijn beveiligd.
	Logging	Voldaan	Activiteiten worden gelogd en bewaard, automatische notificaties bij afwijkend gedrag
	Omgaan met kwetsbaarheden	Voldaan	Beveiligingsupdates worden tijdig uitgerold op basis van CVSS-scores. Er vindt jaarlijks een penetratietest plaats.

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

LesLab Holding B.V. 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, gecrasht 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 ons team, in beginsel per email contact opnemen met de contactpersoon van de Onderwijsinstelling die is vermeld in bijlage 4. Bij die communicatie zal er één teamlid worden aangewezen als aanspreekpunt voor het geval de Onderwijsinstelling contact wil opnemen over een beveiligingsincident en/of Datalek. De specifieke contactgegevens van deze persoon worden verstrekt bij het melden van het beveiligingsincident, maar deze persoon is indirect te bereiken via info@leslab.nl.

Intern beveiligingsbeleid – LesLab (kantooromgeving)

Hoewel LesLab geen verwerkingen uitvoert op fysieke servers of met lokaal opgeslagen leerlingdata, zijn er wel passende maatregelen genomen om de kantooromgeving en werkplekken te beveiligen tegen onbevoegde toegang of onzorgvuldig gebruik.

1. Fysieke toegang

- Het kantoor is alleen toegankelijk voor medewerkers van LesLab.
- Bezoekers worden altijd begeleid door een medewerker en hebben geen toegang tot werkplekken of devices.

2. Werkplekbeveiliging

- Medewerkers werken met laptops die zijn beveiligd met wachtwoord of biometrische toegang.
- Werkplekken worden vergrendeld bij het verlaten van de ruimte of bij langdurige afwezigheid.
- Er geldt een clean-deskbeleid: geen gevoelige documenten of apparaten blijven onbeheerd achter.

3. Documentopslag

- Digitale documenten worden uitsluitend opgeslagen in de cloudomgeving van Paqt en Box.com met toegangscontrole.
- Documentdeling vindt plaats op een need-to-know-basis.
- Er zijn geen fysieke documenten met gevoelige gebruikersinformatie. Gevoelige bedrijfsinformatie wordt bewaard op kantoor in een afgesloten kast waar alleen de directie en managementassistente toegang toe heeft.

4. Netwerk en software

- Medewerkers gebruiken uitsluitend zakelijke apparaten en beveiligde WiFi-verbindingen.
- Automatische updates en antivirussoftware zijn standaard geconfigureerd en worden gecontroleerd door Mr. Orange, de softwareleverancier.

5. Beveiligingsbewustzijn

- Incidenten of beveiligingszorgen worden intern besproken en geëscaleerd via info@leslab.nl.
- Medewerkers worden actief betrokken bij het naleven van dit beleid en aangesproken op onzorgvuldigheden.

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/>.