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: 6-11-2026, geldt vanaf de overstap naar het eigen platform

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 uitgevoerd door LesLab, voor het eigen platform, 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	LesLab Holding B.V. (Rogier van Essen, directeur)
Inlogpagina	• https://mijnproeftuin.nl/login (https://mijnproeftuin.nl/login (representatief voor alle domeinen met uniforme software)
BIV-classificatie	BIV-classificatie: Beschikbaarheid = M, Integriteit = L/M, Vertrouwelijkheid = H Toelichting: Deze inschatting is gebaseerd op de EduBIV-richtlijn en gangbare AVG-interpretaties voor digitale leermiddelen. 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. LesLab Holding B.V. is formeel hoofdverwerker en draagt zorg voor organisatorische borging van de beveiliging, zoals contractbeheer, verwerkersovereenkomsten en privacy-by-design. De technische verwerking vindt plaats op het eigen platform van LesLab, bij subverwerker Scaleway SAS (Parijs), die ISO/IEC 27001:2022-gecertificeerd is. LesLab beheert de inrichting zelf; die ligt vast als code en verandert alleen na goedkeuring. Deze rolverdeling sluit aan bij artikel 28 van de AVG en is vastgelegd in de verwerkersovereenkomst met Scaleway.

Categorie	Maatregelen	Compliance	Uitleg
Beschikbaarheid	Ontwerp	Voldaan	Database, containers en beheertaak draaien op een afgeschermd privénetwerk bij Scaleway; de database is niet vanaf internet bereikbaar. Valt een container uit, dan start Scaleway hem vanzelf opnieuw.
	Capaciteit beheer	Voldaan	De containers schalen mee met de drukte, binnen een vaste bovengrens die past bij de database. Vóór de overstap is getest met een hele school die tegelijk inlogt.
	Onderhoud	Voldaan	Onderhoud wordt gepland buiten schooltijden. Elke wijziging gaat via een goedgekeurd voorstel en kan met één handeling worden teruggedraaid.
	Testen	Voldaan	Elke wijziging wordt eerst getest op een aparte testomgeving met verzonnen gegevens. Het terugzetten van een reservekopie is getest op 27 oktober 2026.
	Monitoring	Voldaan	Fouten, drukte en beschikbaarheid worden bewaakt in Cockpit van Scaleway; waarschuwingen gaan automatisch naar de beheerders van LesLab.
	Herstel	Voldaan met kanttekening	Elke zes uur een reservekopie bij Scaleway in Parijs, en elke nacht een eigen versleutelde kopie van LesLab in Amsterdam, zodat herstel ook kan als Parijs uitvalt. Herstel is getest op 27 oktober 2026. Herstel naar een willekeurig tijdstip biedt Scaleway niet; het

			herstelpunt is ten hoogste zes uur oud, en bij uitval van heel Parijs ten hoogste een dag.
Integriteit	Herleidbaarheid (gebruikers)	Voldaan	Gebruikersacties (zoals antwoorden of aanpassingen) worden automatisch gelogd en gekoppeld aan account-ID's en tijdstempels.
	Backup	Voldaan	Scaleway maakt elke zes uur een reservekopie, 14 dagen bewaard, in Parijs. Daarnaast maakt LesLab dagelijks een eigen kopie, versleuteld met een sleutel van LesLab, 30 dagen bewaard en in die tijd niet te wissen, in Amsterdam.
	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)	Voldaan	Logboeken van platform en database staan in Cockpit van Scaleway, met zo min mogelijk persoonsgegevens, en worden 7 dagen bewaard. Bij fouten en afwijkend gedrag gaan automatisch waarschuwingen naar de beheerders.
	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	Gebruikers zien alleen wat bij hun rol hoort. Dat wordt in de database zelf afgedwongen en bij elke wijziging getest met een vaste proef. Beheerders gebruiken tweestapsverificatie.
	Fysieke toegang	Voldaan	De datacenters worden beheerd door Scaleway en haar onderaannemers. Scaleway is ISO/IEC 27001:2022-gecertificeerd. LesLab heeft geen eigen servers. Voor regels rond beveiliging bij LesLab zelf, zie het intern beveiligingsbeleid hieronder.
	Netwerk toegang	Voldaan	De database en de beheertaak zijn alleen bereikbaar via het privénetwerk. Het platform is van buiten alleen bereikbaar via HTTPS/TLS.
	Scheiding omgevingen	Voldaan	Test en productie zijn gescheiden omgevingen; de testomgeving bevat alleen verzonnen gegevens.
	Transport en fysieke opslag	Voldaan	Al het verkeer is versleuteld (TLS). De database is versleuteld op de schijf; de eigen reservekopie is versleuteld met een sleutel van LesLab.
	Logging	Voldaan	Activiteiten worden

			gelogd in Cockpit van Scaleway; automatische waarschuwingen bij fouten en afwijkend gedrag.
	Omgaan met kwetsbaarheden	Gedeeltelijk voldaan	Beveiligingsupdates van de onderliggende diensten verzorgt Scaleway; de eigen software wordt bij elke bouw bijgewerkt. Een penetratietest door een externe partij is nog niet uitgevoerd.

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 beveligingsincident, 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 het eigen platform, in Box.com en, voor kennis zonder persoonsgegevens, in GitHub, telkens met toegangscontrole.
- Documentdeling vind 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 managmentassistente 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.

Wijzigingen ten opzichte van versie 20-5-2025

- De self-assessment gaat over het eigen platform van LesLab bij Scaleway, niet meer over de omgeving van de softwareleverancier.
- Reservekopieën: elke zes uur bij Scaleway in Parijs, plus dagelijks een eigen versleutelde kopie van LesLab in Amsterdam.

- Kwetsbaarheden: een externe penetratietest is nog niet uitgevoerd; dat staat er nu eerlijk.
- Documentopslag: het eigen platform, Box en GitHub in plaats van de omgeving van de softwareleverancier.

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/.