LEHRPULS · COMPLIANCE

LehrPuls — Vendor Security Self-Assessment (HECVAT Lite structure)

Product: LehrPuls 1.21.1 · **Vendor:** Dr. Florian Hollomey, Rohr 17, 8413 Ragnitz, Austria · **Contact:** office@lehrpuls.com · **Date:** November 8, 2026

This document answers the question areas of the Higher Education Community Vendor Assessment Toolkit (HECVAT) Lite, published by EDUCAUSE, for LehrPuls. The question texts below are paraphrased from the publicly known section structure of HECVAT Lite; they are not a copy of the EDUCAUSE spreadsheet. Institutions that require the original HECVAT spreadsheet can transfer the answers given here; we will complete the official form on request.

Reading guide. LehrPuls is a desktop application. The instructor's laptop is the server; participants' answers are stored only on that laptop. The vendor hosts no customer data. For that reason most questions about vendor-hosted data, data centers and multi-tenancy are answered **"N/A — no vendor-hosted data"**, each with the reason. The only vendor-operated components are (a) the website lehrpuls.com (downloads, license shop, update manifest), (b) the relay server relay.lehrpuls.com, which forwards end-to-end encrypted messages when participants are not on the instructor's network, and (c) the customer database for license purchases. Where evidence is available on request, the answer says so.

1. Company Overview

ID	Question	Answer	Explanation
COMP-01	Legal name and address of the vendor	Dr. Florian Hollomey, Rohr 17, 8413 Ragnitz, Austria	Registered sole trader (Austrian trade license, GISA number 18954647; VAT ID ATU46352806). Member of the Austrian Economic Chamber, Styria.
COMP-02	Product name and version assessed	LehrPuls 1.21.1 (macOS and Windows) with relay server and website	Released November 6, 2026.
COMP-03	Describe the product	Live questions in the lecture hall. The instructor runs the desktop application; it starts a small web server on the laptop. Participants open a page in their smartphone browser (QR code or room code) and answer. Results are shown on the projector and stored on the laptop. Optional: online route through a relay server with end-to-end encryption.	See the Data-Flow Statement for details.
COMP-04	Number of employees	One person (owner-operated)	Development, support and operations are carried out by the owner.
COMP-05	Years in business / product history	LehrPuls 1.0 was released in September 2026 (first public release 11 September 2026). It is developed by an instructor at an Austrian university of applied sciences and has been in use there since September 2026.	
COMP-06	Does the product process, store or transmit institutional data?	Process: yes, on the institution's own devices. Store: on the instructor's device only. Transmit through vendor systems: only end-to-end encrypted through the relay, if the institution chooses the online route.	The vendor never holds institutional data in readable form.

ID	Question	Answer	Explanation
COMP-07	Data classification of information handled	Student responses, names or student IDs (if the instructor chooses a join mode with names), course lists, questions and results. Depending on jurisdiction these can be education records (FERPA) or personal data (GDPR).	All of it stays on the instructor's device; see section 5.
COMP-08	Is a third party involved in delivery of the service?	Hetzner Online GmbH (server hosting for lehrpuls.com and the relay, EU data center); Paddle.com Market Limited (reseller/merchant of record for online purchases); oja.at (e-mail hosting).	Section 6.
COMP-09	Have you completed a HECVAT before?	No. This is the first self-assessment, structured after HECVAT Lite.	
COMP-10	Do you have cyber-liability insurance?	No. The vendor hosts no customer data from the application; the relay carries ciphertext only.	

2. Documentation

ID	Question	Answer	Explanation
DOCU-01	Do you have a documented information security policy?	No formal, board-approved policy document. Security requirements are documented in the engineering documents: relay protocol specification, release checklist with mandatory tests, test checklist (including accessibility and platform checks).	A one-person vendor; the documents named are maintained in the product repository.
DOCU-02	Are policies reviewed regularly?	The release checklist and test checklist are reviewed and extended with every release (roughly every two to three weeks in 2026).	
DOCU-03	Do you have a privacy policy, and is it publicly available?	Yes: https://lehrpuls.com/privacy.html (English) and https://lehrpuls.com/datenschutz.html (German), version of November 5, 2026.	
DOCU-04	Do you have license terms / terms of service?	Yes: https://lehrpuls.com/license-terms.html	
DOCU-05	Is there an accessibility conformance report?	Yes: VPAT/ACR, published at https://lehrpuls.com/compliance.html	
DOCU-06	Is there technical documentation for IT departments?	Yes: silent installation (`/S /AllUsers` , `/S /CurrentUser`), environment variables for data folder, relay address and read-only interface lock, network requirements; manual chapter 11 and the "For IT" section of https://lehrpuls.com/help.html. A German step-by-step guide for IT departments exists and is shared on request.	
DOCU-07	Do you provide a data-flow diagram?	Yes: Data-Flow Statement at https://lehrpuls.com/compliance.html	

3. Application / Service Security

ID	Question	Answer	Explanation
APPL-01	Architecture and technology stack	Desktop application: Rust (Tauri 2) with a Vue 3/Quasar user interface in the operating system's web view; embedded HTTP/WebSocket server (axum); SQLite database. Participant app: Vue 3 single-page application served by the laptop (or, in online mode, by the relay). Relay: Rust (axum, tokio-tungstenite), stateless. Website: static HTML.	
APPL-02	Is the application multi-tenant?	N/A — no vendor-hosted data. Each installation is a separate program on a separate device with its own database file. The relay forwards opaque ciphertext for concurrent rooms; it cannot read any of it.	

ID	Question	Answer	Explanation
APPL-03	Does the application encrypt data in transit?	Local Wi-Fi route: HTTP on the local network (private IP address of the laptop, port 8712–8715); no TLS certificate can be issued for a private, room-dependent address. Online route: TLS (HTTPS/WSS) to the relay **and** end-to-end encryption of all content with AES-256-GCM; the key is in the URL fragment (`#k=…`), which browsers never send to a server. Update check and website: HTTPS. Read-only interface: HTTP on 127.0.0.1 by default; the instructor must explicitly enable network access after a warning that the connection is unencrypted.	The manual explains the "Not secure" label of the local route to participants (section 5.6): no passwords, no accounts, data stays in the room.
APPL-04	Does the application encrypt data at rest?	No application-level encryption of the SQLite database. The database lives in the user's profile (macOS: Application Support; Windows: `%APPDATA%` /the folder set by IT), protected by operating-system permissions; full-disk encryption (FileVault, BitLocker) is the institution's control. The license file is written with owner-only permissions (0600). The read-only interface stores only a SHA-256 hash of its access key. Files the relay holds temporarily are AES-256-GCM ciphertext.	The vendor recommends device encryption through the institution's standard endpoint policy.
APPL-05	Are secure coding practices followed?	Rust for all server-side and desktop logic (memory safety); automated test suites for application (`cargo test`), relay (`cargo test` , integration test for payload opacity and error paths) and user interfaces; Clippy and ESLint are mandatory before each release. Inputs from participants are validated on the laptop (size limits, type checks, content/extension match for uploaded files; executable and macro-enabled files are not accepted).	
APPL-06	Is there a vulnerability disclosure or bug reporting channel?	office@lehrpuls.com. No bug bounty program.	
APPL-07	Does the application use third-party components, and how are they tracked?	Yes (Rust crates, npm packages). Versions are pinned in `Cargo.lock` and `package-lock.json` . No scheduled automated dependency vulnerability scan is in place; dependencies are reviewed and updated with each release.	See section 13.
APPL-08	Does the application have any remote-access or telemetry functions?	No telemetry, no crash reporting, no analytics. The only automatic outbound connection is the update check (one HTTPS GET of `https://lehrpuls.com/latest.json` at startup and at a configurable interval, User-Agent `LehrPuls/<version>` , no device or license identifier), which can be switched off.	Verified in the application source.
APPL-09	Can the application be deployed with restricted features?	Yes. Environment variables: `LEHRPULS_DATA_DIR` (data folder), `LEHRPULS_RELAY_URL` (relay address, for a self-hosted relay), `LEHRPULS_API_SPERRE=1` (locks the read-only interface). Update check can be disabled per installation.	
APPL-10	Code signing	macOS: Developer ID signed and notarized. Windows: Authenticode signature, publisher "Dr. Florian Hollomey". SHA-256 checksums of installers are published on the download page.	
APPL-11	Local server exposure	The session server listens on the laptop only while a session runs (TCP 8712, fallback 8713–8715). It serves the participant page and WebSocket. Inbound connections are accepted from the local network only during a session; there is no listener otherwise. A second instance of the program does not open a port (file hand-off via a local mailbox file).	

4. Authentication, Authorization and Accounting

ID	Question	Answer	Explanation
AAAI-01	Does the product support SSO (SAML, OIDC, CAS)?	N/A — there are no user accounts. The instructor's identity is the operating-system login; participants join a session with a room code (plus, at the instructor's choice, a pseudonym, a name, or name and student ID verified against the course list).	

ID	Question	Answer	Explanation
AAAI-02	Password policy, MFA	N/A — no passwords exist anywhere in the product.	
AAAI-03	Role-based access control	The instructor has full control of their own data on their own device. Participants can only answer the currently open question. The read-only interface (if enabled) grants read-only access with a bearer key.	
AAAI-04	How is the read-only interface protected?	Off after installation. When enabled, a random 32-byte key (`lp_…`) is generated; only its SHA-256 hash is stored; the key expires after at most 90 days and can be revoked at any time. Default scope 127.0.0.1 only; default output anonymized (no participant names). Reads use a separate read-only database connection, so writes are technically impossible through this path.	Verified in the application source.
AAAI-05	How is the relay room protected against takeover?	A host token (random secret held by the cockpit) is needed to act as host of a room; while a host is disconnected its room code stays reserved for that token (default 180 days, configurable, at most 366). Participants cannot become host.	Relay protocol specification section 2.
AAAI-06	Audit logging of user actions	N/A — single-user desktop application; the instructor's actions are their own. The relay logs no payload and no user action; its access log (web server) holds IP address and request path for at most 90 days.	
AAAI-07	License activation	License keys are ed25519-signed tokens issued by the vendor; the application verifies the signature offline with the embedded public key. There is no activation server, no hardware binding, no phone-home. The token contains product, licensee name, e-mail, license type, purchase date and the major version it covers.	Verified in the application source.

5. Data Protection and Data Handling

ID	Question	Answer	Explanation
DATA-01	Where is institutional data stored?	On the instructor's device: one SQLite file (`lehrpuls.db`) plus media files in the user's data folder. Institutions can point the data folder to a managed location (for example a OneDrive folder of the institution's tenant) with `LEHRPULS_DATA_DIR` .	No copy exists at the vendor.
DATA-02	Does the vendor have access to institutional data?	No. There is no remote access, no support tunnel and no backup at the vendor.	
DATA-03	Data in transit through vendor systems	Only in online mode: end-to-end encrypted frames (AES-256-GCM, key never sent to the server) pass through relay.lehrpuls.com. The relay sees room code, connection metadata (IP address, timing, sizes) and ciphertext. Files attached to answers or question images are stored on the relay as ciphertext for the duration of the session, at most 12 hours after the last access, and deleted when the session is ended.	Relay source; protocol section 5.
DATA-04	Data retention and deletion	Determined by the instructor: deletion period per course (automatic deletion of sessions after N days), trash with configurable retention, manual deletion. Sample privacy notice for participants is built into the product. The vendor retains nothing from sessions. Relay usage statistics are counts only (per hour and per ended session: numbers of connections, devices, joins, messages, bytes), with no codes, addresses or identifiers.	
DATA-05	Is data anonymized or pseudonymized?	At the instructor's choice: anonymous sessions, pseudonyms, names, or name plus student ID. Export and read-only interface are anonymized by default. Export protection with a minimum group size for aggregated statistics exists.	
DATA-06	Data return at end of contract	N/A — the data was never with the vendor. Instructors export their data at any time (XLSX, CSV, JSON raw data; `.lpx` exchange files; PDF reports) and the database is a standard SQLite file.	
DATA-07	Data residency	Institutional data: on the institution's devices. Vendor systems (website, relay, customer database): Hetzner Online GmbH, data center in the EU. Online purchases: Paddle (United Kingdom; EU adequacy decision).	
DATA-08	Which personal data does the vendor process about institutional staff?	Only for license purchase and support: name, e-mail, institution, billing address, license type, seat count, optionally VAT number and purchase order number. Legal basis and retention are stated in the privacy policy (invoices seven years, Austrian tax law).	

ID	Question	Answer	Explanation
DATA-09	Backups	Institution's responsibility (standard endpoint backup; the manual recommends Time Machine or the institution's backup and describes the "Back up database" function). Vendor systems: the website is static and reproducible from the repository; the customer database (contact and order data only) is backed up by the vendor; details on request. The relay has no data to back up except room reservations.	
DATA-10	FERPA / GDPR roles	The institution (or the instructor) is the controller. The vendor is not a processor for session data, because it never receives it. For the relay, the vendor operates a forwarding service that handles ciphertext and connection metadata; the privacy policy describes this. No data processing agreement is required for the desktop application; a Data-Flow Statement is provided for the privacy office.	

6. Third Parties

ID	Question	Answer	Explanation
THRD-01	List third parties with access to institutional data	None.	Hetzner hosts servers that see only encrypted relay traffic and web server logs; Paddle processes purchases, not institutional data.
THRD-02	Subprocessors for vendor systems	Hetzner Online GmbH (hosting, EU, processor under Art. 28 GDPR for web server logs and the customer database); Paddle.com Market Limited (reseller for online purchases; independent controller for payment data); oja.at (e-mail hosting, Austria).	
THRD-03	Third-party scripts on the website	None on content pages (no analytics, no cookies, no embedded fonts). Paddle's `paddle.js` loads only after the buyer clicks "Pay online" on the order page.	
THRD-04	Third-party code in the product	Open-source libraries (Rust crates and npm packages) compiled into the product; no third-party services called at runtime except the vendor's own update manifest and relay.	

7. Consulting / Professional Services

ID	Question	Answer	Explanation
CONS-01	Are on-site or remote consulting services offered?	No consulting services. Support by e-mail. Documentation (manual, step-by-step guides, IT guide) is provided.	
CONS-02	Does vendor staff need access to institutional systems?	No.	

8. Business Continuity and Disaster Recovery

ID	Question	Answer	Explanation
BCPL-01	Business continuity plan	No formal plan document. The product works without any vendor system: installed copies, licenses (offline verified) and data on the institution's devices continue to work if the vendor's servers or business cease. The relay can be self-hosted from the published source (`relay/` , Docker and systemd deployment files) and selected with `LEHRPULS_RELAY_URL` .	
BCPL-02	Recovery time and recovery point objectives for vendor systems	Relay: stateless; a restart loses only live connections, which reconnect automatically, and room reservations are persisted. No formal RTO/RPO commitments. Website: static files, redeployable within minutes from the repository.	
BCPL-03	Impact on the institution if the vendor service is unavailable	Local Wi-Fi route unaffected. Online route unavailable until the relay is back; hybrid sessions continue for devices on the room network.	

9. Change Management

ID	Question	Answer	Explanation
CHNG-01	Is there a documented change and release process?	Yes: the release checklist (German) defines, for every release, the test run on macOS and Windows, code and documentation reviews, a mandatory package check, release gate, build, signing/notarization, upload order (update manifest last) and rollback procedure.	
CHNG-02	How are customers informed about changes?	Release notes per version at https://lehrpuls.com/whats-new.html; the application shows a notice when a new version exists (if the update check is enabled). Updates are never installed automatically.	
CHNG-03	Can the institution control update timing?	Yes. Updates are manual installs; IT can disable the update notice and distribute installers with its own tooling.	

10. Datacenter

ID	Question	Answer	Explanation
DCTR-01	Where are the data centers located?	N/A — no vendor-hosted institutional data. Vendor systems run on a Hetzner Online GmbH server in the EU.	
DCTR-02	Physical security certifications of the data center	Hetzner data centers are ISO/IEC 27001 certified (certificate available from Hetzner).	
DCTR-03	Server hardening of the relay	The relay runs as a systemd service with `DynamicUser` , `NoNewPrivileges` , `ProtectSystem=strict` , `PrivateTmp` , a private state directory (mode 0700) and listens on localhost only; Caddy terminates TLS (Let's Encrypt) and proxies to it. Status and usage endpoints answer only to local requests.	Source: `relay/deploy/lehrpuls-relay.service` , `relay/deploy/Caddyfile.relay` .

11. Privacy

ID	Question	Answer	Explanation
PRIV-01	Is personal information collected from students?	By the product on the instructor's device: only what the instructor configures (anonymous, pseudonym, name, or name plus student ID) and the answers given. Not by the vendor.	

ID	Question	Answer	Explanation
PRIV-02	Is data shared with or sold to third parties?	No.	
PRIV-03	Are cookies or tracking used?	The participant app stores a random device identifier and the join state in the browser's `localStorage` so a participant can reload the page or switch devices within a session; no cookies, no tracking. The website sets no cookies.	
PRIV-04	Privacy notice for participants	A sample privacy notice for participants is built into the cockpit (courses page) and can be copied into course materials.	
PRIV-05	Data subject rights	For session data: handled by the institution (controller), which holds the data. For purchase data: office@lehrpuls.com, see privacy policy section 6.	
PRIV-06	Children's data (COPPA)	The product is intended for higher education; it is not directed at children.	

12. Quality Assurance

ID	Question	Answer	Explanation
QUAL-01	Testing before release	Automated unit and integration tests (application, relay, participant app), scripted end-to-end runs with simulated participant devices (up to 500 devices load test), a documented test checklist with several hundred items run on macOS and Windows before each release, accessibility scan with axe-core, and a package check of the signed installers.	
QUAL-02	Defect handling	Findings from a release test run are fixed before the release ("only defect-free releases" rule since November 6, 2026) or documented as deferred in the test report.	
QUAL-03	Support channels and response time	E-mail office@lehrpuls.com. No formal service-level agreement.	

13. Vulnerability Scanning and Patching

ID	Question	Answer	Explanation
VULN-01	Are vulnerability scans or penetration tests performed?	No external penetration test has been performed. Internal checks: Clippy and tests before each release; path traversal and input limits in the relay were reviewed and have regression tests (for example the `/a/` asset path check).	
VULN-02	How quickly are vulnerabilities patched?	No formal commitment. Releases are frequent (several per month in 2026); a security fix would be released as a point release and announced on the "What's new" page.	
VULN-03	Dependency vulnerability monitoring	Not automated; dependencies are reviewed and updated with each release.	A reasonable request from an institution; it can be added (cargo-audit, npm audit) at low cost.
VULN-04	Operating system patching of vendor servers	Hetzner server with Ubuntu 24.04 LTS; security updates are installed automatically every day (unattended-upgrades).	

14. HIPAA

N/A — LehrPuls does not process protected health information and is not intended for clinical use.

15. PCI DSS

N/A — the vendor never sees payment card data. Online payments are processed by Paddle.com Market Limited as merchant of record; purchases by invoice are paid by bank transfer.

Summary for the reviewer

- Student data: never leaves the instructor's device in readable form. No vendor access, no vendor backup, no accounts.
- Vendor systems: static website, license shop (customer data of the buyer only), update manifest (version number only), relay (ciphertext and connection metadata; logs 90 days; counts only for capacity planning).
- Controls the institution keeps: device encryption, endpoint backup, data folder location, update timing, relay choice (public, self-hosted or none), read-only interface lock.
- Evidence available on request: backup schedule of the customer database, Hetzner's ISO/IEC 27001 certificate, the IT guide in German.

Self-assessment by the vendor, November 8, 2026. HECVAT is a trademark of EDUCAUSE; this document uses its section structure and is not an EDUCAUSE-reviewed submission.