Anhang 1: Technische und organisatorische Maßnahmen (TOM)

GeniusQ – Lernplattform Stand: 13.08.2026

Dieser Anhang beschreibt die technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Art. 32 DSGVO. Die Maßnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten, die im Rahmen der Nutzung der Lernplattform verarbeitet werden. Der Auftragnehmer ist berechtigt, diese TOM zu aktualisieren, sofern dadurch kein niedrigeres Schutzniveau entsteht. Aktualisierte Fassungen ersetzen automatisch diesen Anhang.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zugangskontrolle

- Passwortschutz für alle administrativen und technischen Zugänge
- Multi-Faktor-Authentifizierung für die Verwaltungszugänge bei den eingesetzten Anbietern, namentlich: Hosting und Objektspeicher (Hetzner), Managed-Datenbank (Elestio), KI-Inferenz (AWS), Speicherung der Datensicherungen sowie Domain- und DNS-Verwaltung (IONOS), Quellcode- und Auslieferungsplattform (GitHub) und die eingesetzten KI-Anbieter
- Plattformzugänge (Lernende, Trainer, interne Admins) sind über passwortgeschützte HTTPS-Verbindungen abgesichert
- Zugriff auf alle Systeme ausschließlich über TLS-verschlüsselte HTTPS-Verbindungen
- Rollenbasierte Zugriffskontrolle für alle Plattformnutzer (Lernende, Trainer, interne Admins)

1.2 Berechtigungsmanagement

- Rollenbasierte Zugriffskontrolle (RBAC) mit klar definierten Rollen: Lernende, Trainer, interne Admins
- Vergabe von Berechtigungen strikt nach dem Need-to-know-Prinzip
- Benutzerkonten werden anhand der vom Auftraggeber bereitgestellten E-Mail-Adressen angelegt; jede betroffene Person erhält eine individuelle Einladung per E-Mail mit einem registrierungspflichtigen Einladungscode
- Der Einladungscode ist eindeutig dem Auftraggeber zugeordnet, sodass die Zuordnung von Nutzern zu Mandanten gewährleistet ist
- Nutzer stimmen während der Registrierung den Datenschutzbestimmungen der Plattform zu
- Benutzerkonten werden auf Antrag des Auftraggebers oder des betroffenen Nutzers unverzüglich, spätestens jedoch innerhalb von 7 Werktagen gelöscht
- Regelmäßige Überprüfung interner Admin-Zugänge (mindestens einmal jährlich)

1.3 Vertraulichkeitsverpflichtung

- Alle internen Mitarbeiter und beauftragten externen Dienstleister werden schriftlich auf Vertraulichkeit verpflichtet
- Zugriff auf personenbezogene Daten ist ausschließlich befugten Personen gestattet. Dies gilt für die Datenbank, die Anwendung und die im Objektspeicher abgelegten Medien- und Anhangsdateien gleichermaßen. Der Abruf einer Medien- oder Anhangsdatei ist nur über eine zeitlich befristete, signierte Adresse möglich, die die Anwendung erst nach Prüfung der Berechtigung ausgibt; ohne gültige Signatur wird der Abruf abgewiesen.
- Befugte Personen erhalten nur Zugang zu den Daten, die für ihre Tätigkeit erforderlich sind
- Externe Dienstleister (z. B. Entwickler oder technische Unterstützung), sofern eingesetzt, werden vor Tätigkeitsbeginn schriftlich auf Vertraulichkeit verpflichtet
- Datenschutzrelevante Abläufe werden dokumentiert und regelmäßig überprüft

1.4 Vertraulichkeit und Richtlinien

Der Auftragnehmer hat interne Datenschutzrichtlinien dokumentiert, die den Umgang mit personenbezogenen Daten regeln. Externe Dienstleister und Mitarbeiter werden vor Tätigkeitsbeginn schriftlich auf Vertraulichkeit verpflichtet und über die geltenden Datenschutzanforderungen informiert.

1.5 Sicherheit der Arbeitsstationen (Mobile Arbeit & Home Office)

Da administrative Tätigkeiten auch mobil oder im Home Office durchgeführt werden können, gelten

folgende Schutzmaßnahmen für die Endgeräte des Auftragnehmers: * **Festplattenverschlüsselung:** Alle genutzten Notebooks/PCs sind vollständig verschlüsselt (z. B. BitLocker, FileVault). * **Sperrmechanismus:** Automatische Bildschirmsperre bei Inaktivität. * **Schutz vor Dritteinsicht:** Verwendung von Blickschutzfiltern bei Arbeit in öffentlichen Bereichen; im Home Office ist sichergestellt, dass Unbefugte (z. B. Familienangehörige) keinen Blick auf personenbezogene Daten haben. * **Sicherheitsupdates:** Betriebssysteme und Browser werden automatisch auf dem aktuellen Stand gehalten.

1.6 Bewusst öffentlich zugängliche Inhalte

Nicht signaturpflichtig sind ausschließlich Inhalte, deren Zweck der offene Abruf ist und die keine personenbezogenen Daten enthalten: Logos und Gestaltungsvorgaben der Auftraggeber — auch in E-Mails, die keine befristeten Bildadressen tragen können — sowie Bildmaterial öffentlich eingebundener Widgets.

Die Freigabe erfolgt ausschließlich über eine im System hinterlegte, abschließende Liste von Ablageorten. Ein Upload außerhalb dieser Liste wird stets nicht-öffentlich abgelegt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Übertragungskontrolle

- TLS 1.2+ bei sämtlichen Datenübertragungen
- API-Kommunikation mit externen Anbietern ausschließlich verschlüsselt

2.2 Eingabekontrolle

- Änderungen an personenbezogenen Daten können ausschließlich durch befugte administrative Nutzer vorgenommen werden
- Administrativer Zugriff beschränkt sich auf den Auftragnehmer und ggf. beauftragte Dienstleister
- Technische Maßnahmen (z. B. CSRF-Schutzmechanismen) verhindern unbefugte oder automatisierte Änderungen durch Dritte
- Sicherheitsrelevante administrative Änderungen werden intern dokumentiert
- Passwörter werden ausschließlich gehasht gespeichert

2.3 Sitzungen und Abmeldung

- Eine Sitzung endet spätestens **24 Stunden** nach der Anmeldung.
- Wählt ein Nutzer „angemeldet bleiben", gilt das zugehörige Cookie **7 Tage** und verlängert sich bei jeder Nutzung; es überdauert die Inaktivitäts-Policy nicht.
- Unabhängig davon werden Konten, die länger als **7 Tage** nicht genutzt wurden, beim nächsten Zugriff serverseitig zwangsabgemeldet.
- CSRF-Schutz mit zeitlich begrenzten Tokens
- Sichere Session-Cookies (HTTPS-only, HttpOnly, SameSite)

2.4 Absicherung der Auslieferung im Browser

- **Content-Security-Policy:** Die Plattform liefert eine eng gefasste Policy aus, die das Nachladen und Ausführen von Code fremder Hosts unterbindet. Der Betriebsmodus (Meldebetrieb/ Durchsetzung) ist konfigurierbar; Verstöße werden protokolliert.
- **Keine Fremdressourcen:** Programmbibliotheken und Schriften werden ausschließlich vom eigenen Server ausgeliefert. Ein Abruf bei Drittanbietern – und damit eine Übermittlung von IP-Adressen der Nutzer – findet beim Seitenaufruf nicht statt. Die ausgelieferten Dateien sind über Prüfsummen im Quellcode festgeschrieben.
- **Eingebettete Videos und Karten** externer Anbieter werden erst nach ausdrücklicher Aktivierung durch den Nutzer geladen (Zwei-Klick-Lösung); die Umschreibung erfolgt serverseitig, sodass ohne Aktivierung keine Verbindung zum Anbieter aufgebaut wird.
- Weitere Sicherheitskopfzeilen (u. a. Unterbindung von Objekteinbettung, Beschränkung der Formularziele und der Basisadresse).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

3.1 Hosting-Infrastruktur

- Betrieb aller personenbezogenen Daten ausschließlich in Deutschland: Anwendungs- und Infrastruktur-Hosting sowie Object Storage in der Hetzner-Region Falkenstein (FSN1); die Managed-Datenbank (MySQL) wird über Elestio in derselben Region (Falkenstein) betrieben; die Vektordatenbank läuft auf derselben Infrastruktur; die verschlüsselten Datensicherungen werden bei IONOS in Berlin gespeichert (siehe Abschnitt 3.2).
- Die Auslieferung von Medien- und statischen Inhalten aus dem Object Storage erfolgt über das Content Delivery Network von bunny.net (BunnyWay d.o.o., Slowenien). Die eingesetzte Zone ist auf europäische Edge-Server beschränkt; das CDN cached und liefert diese Inhalte ausschließlich über EU-/EWR-Edge-Server aus und verarbeitet dabei technische Verbindungsdaten (insb. IP-Adressen) der abrufenden Nutzer weisungsgebunden auf Grundlage eines Auftragsverarbeitungsvertrags.
- **Infrastrukturelle Redundanz:** Die Plattform nutzt die Hochverfügbarkeits-Infrastruktur der Provider Hetzner und Elestio. Dies umfasst redundante Stromversorgung, Netzwerkanbindung und Storage-Systeme auf Rechenzentrumsebene.
- **Rapid Recovery:** Die Verfügbarkeit wird durch eine "Rapid Recovery"-Strategie sichergestellt. Durch den Einsatz von Image-basierten Wiederherstellungsverfahren und automatisierten Prozessen können die Dienste im Falle eines Hardware-Ausfalls in der Regel innerhalb von 6 Stunden auf neuer Infrastruktur wiederhergestellt werden.

3.2 Backup-Konfiguration

- Gesichert werden sämtliche Datenbestände, die personenbezogene Daten enthalten können: Datenbank, Object Storage (Medien und Uploads), Vektordatenbank sowie die Betriebskonfiguration.
- Die Datenbank wird alle 6 Stunden gesichert, die übrigen Bestände täglich; die Vektordatenbank wöchentlich.
- Alle Sicherungen werden **vor der Übertragung clientseitig verschlüsselt** (AES-256). Der Speicheranbieter hat zu keinem Zeitpunkt Zugriff auf Klartextdaten.
- Die Sicherungen werden bei einem **zweiten, vom Hosting unabhängigen Anbieter in Deutschland** gespeichert (IONOS Object Storage, Region Berlin) und liegen damit räumlich getrennt vom Produktivstandort Falkenstein.
- Automatische Rotation und Überschreibung nach 14 Tagen gemäß AVV. Für die wöchentlich gesicherte Vektordatenbank werden die beiden jeweils jüngsten Generationen vorgehalten; ältere werden überschrieben.
- Die Sicherungen sind zusätzlich durch eine Objektsperre (WORM) über 14 Tage gegen Löschung und Veränderung geschützt. Die auf dem Anwendungsserver hinterlegten Zugangsdaten können diese Sperre nicht aufheben; ein kompromittierter Server kann bestehende Sicherungen daher nicht vernichten.
- Erfolg, Vollständigkeit und Aktualität jedes Sicherungslaufs werden automatisiert überwacht. Fehlgeschlagene sowie ausbleibende Läufe lösen unverzüglich eine Benachrichtigung aus.
- Zusätzlich bestehen systemseitige Managed-Database-Backups durch Elestio; deren Aufbewahrungsdauer richtet sich nach dem gebuchten Support-Level (derzeit 7 Tage), ihre Aufbewahrung und Löschung ausschließlich nach den Richtlinien bzw. der DPA von Elestio.

3.3 Notfall- und Wiederherstellungsmanagement

- Ein internes Verfahren zur Wiederherstellung der Plattform aus Backups ist definiert und dokumentiert.
- Die Integrität des gesamten Sicherungsbestands wird wöchentlich automatisiert und vollständig geprüft.
- Die Wiederherstellbarkeit wird regelmäßig praktisch erprobt und protokolliert: Wiederherstellung einzelner Dateien monatlich; vollständige Wiederherstellung der Datenbank in eine isolierte Instanz mit anschließendem Abgleich gegen den Produktivbestand vierteljährlich (zuletzt durchgeführt am 10.08.2026). Ergänzend ist ein vollständiger Wiederanlauftest auf neuer Infrastruktur im Jahresturnus vorgesehen.
- Die Protokolle dieser Erprobungen werden dem Auftraggeber im Rahmen einer Dokumentenprüfung auf Anfrage vorgelegt.
- Der Wiederanlauf umfasst Betriebskonfiguration, Datenbank, Object Storage und Vektordatenbank sowie den Neustart der Systeme über die Hetzner-Cloud-Konsole bzw. das Elestio-Dashboard. Die Reihenfolge ist so festgelegt, dass die Plattform bereits vor Abschluss der

Medienwiederherstellung nutzbar ist.
- Das Verfahren wird bei Bedarf aktualisiert.

4. Belastbarkeit und Protokollierung

4.1 Sicherheitsrelevante Ereignisse

Die Plattform protokolliert sicherheitsrelevante Ereignisse strukturiert und auswertbar. Erfasst werden insbesondere: * **Anmeldungen**, erfolgreiche wie fehlgeschlagene, jeweils mit Zeitpunkt, IP-Adresse und – soweit das Konto bekannt ist – Kontobezug. Ist die eingegebene Kennung keinem Konto zugeordnet, wird an ihrer Stelle ausschließlich ein kryptografischer Streuwert gespeichert, sodass wiederholte Versuche auf dieselbe Kennung erkennbar sind, ohne die Kennung selbst zu speichern. Ergänzend führt jedes Konto Zeitpunkt und IP-Adresse der letzten Anmeldung sowie die Zahl der Anmeldungen. * **unerwartete Serverfehler (5xx)**, sowohl im vorgelagerten Webserver – dieser erfasst auch die Fälle, in denen die Anwendung selbst nicht mehr antwortet – als auch in der Anwendung mit technischem Kontext. Einbezogen sind ebenso Fehler der Hintergrundverarbeitung und der Schnittstelle für KI-Assistenten. * **verweigerte Zugriffe** auf Ressourcen, für die dem angemeldeten Nutzer die Berechtigung fehlt. * **gescheiterte Autorisierungsvorgänge** der Schnittstelle für KI-Assistenten, mit dem standardisierten Fehlercode und der öffentlichen Kennung der anfragenden Anwendung. * das **Zugriffsprotokoll des vorgelagerten Webservers** mit Statuszeilen, aus dem sich Fehlerhäufungen und ungewöhnlich hohe Zugriffsmuster nachvollziehen lassen, die auf automatisierte oder missbräuchliche Nutzung hindeuten können. * **anwendungsseitige Fehlerprotokolle.** * **Meldungen der Content-Security-Policy** über blockierte bzw. gemeldete Verstöße.

Nicht protokolliert werden Passwörter – auch nicht in gekürzter oder abgeleiteter Form –, Zugangs- oder Autorisierungsschlüssel, Anfrageinhalte und Inhalte von KI-Eingaben.

Auswertung und Reaktion: Für Anmeldefehlversuche, Serverfehler, verweigerte Zugriffe und gescheiterte Autorisierungsvorgänge sind Schwellenwerte je Zeitfenster hinterlegt. Wird eine Schwelle überschritten, löst dies unverzüglich eine Benachrichtigung an den Auftragnehmer aus; die Auslösung wird ihrerseits protokolliert. Ergänzend wird täglich automatisiert ausgewertet und berichtet, sofern Befunde vorliegen. Darüber hinaus erfolgt eine anlassbezogene Auswertung durch befugte Personen.

Eine automatische Sperrung von Konten oder Netzadressen nach fehlgeschlagenen Anmeldeversuchen ist derzeit **nicht** eingerichtet; die Reaktion auf eine Benachrichtigung erfolgt manuell. Unberührt bleibt die Benachrichtigung bei Fehlschlagen oder Ausbleiben der Sicherungsläufe (Abschnitt 3.2).

4.2 Logging

Die Plattform erfasst Protokolle, die für den technischen Betrieb und die Untersuchung von Störungen erforderlich sind. Dies umfasst: * technische Fehlerprotokolle * Zugriffsinformationen, einschließlich IP-Adressen, soweit zur Diagnose erforderlich * sicherheitsrelevante Ereignisse gemäß Abschnitt 4.1

Zugriff auf die Protokolle ist auf befugte Personen beschränkt. Das Sicherheitsprotokoll wird mandantenübergreifend geführt und ist ausschließlich für den Auftragnehmer einsehbar; ein Selbstzugriff des Auftraggebers besteht nicht. Auskunft zu Ereignissen, die den Auftraggeber betreffen, erfolgt anlassbezogen.

Löschfristen. Die Fristen sind je Ablage technisch erzwungen und werden in keinem Fall allein über die Dateigröße gesteuert: * **Zugriffsprotokolle: maximal 30 Tage.** Im Webserver ist eine Zeitgrenze konfiguriert; zusätzlich entfernt ein täglicher automatisierter Lauf ältere Archive. * **Ereignisprotokolle: maximal 90 Tage.** Ein täglicher automatisierter Löschlauf entfernt ältere Datensätze aus der Datenbank. * **Fehlerprotokolle auf Dateiebene: maximal 90 Tage.** Durchgesetzt über eine zeitbasierte Rotation. * Längere Speicherung erfolgt ausschließlich zur Untersuchung konkreter technischer oder sicherheitsrelevanter Vorfälle. * Restbestände in verschlüsselten Datensicherungen erlöschen mit deren Aufbewahrungsfrist (Abschnitt 3.2).

Für den Nachweis der Einhaltung steht ein Statusbefehl bereit, der Bestandsalter und Fristeinhaltung je Ablage ausgibt. Die Ergebnisse werden in wiederkehrenden Abständen als Prüfprotokoll abgelegt; das erste Protokoll stammt vom Tag der Inbetriebnahme (11.08.2026). Die Prüfprotokolle werden dem

Auftraggeber im Rahmen einer Dokumentenprüfung auf Anfrage vorgelegt.

4.3 Umgang mit IP-Adressen

- IP-Adressen werden zu technischen Zwecken gespeichert, insbesondere zur Störungsanalyse und zur Erkennung potenziell missbräuchlicher Nutzung.
- IP-Adressen werden bei sicherheitsrelevanten Ereignissen vollständig gespeichert, da eine Kürzung die Unterscheidung einzelner Zugriffsquellen – und damit den Zweck der Erkennung missbräuchlicher Nutzung – ausschließen würde. Die Begrenzung erfolgt über die Speicherdauer (Abschnitt 4.2), nicht über die Genauigkeit.
- Eine Weitergabe an externe KI-Dienste erfolgt nicht.

4.4 Belastbarkeit

Die Belastbarkeit der Plattform ergibt sich aus: * der Nutzung der Rechenzentrumsinfrastruktur von Hetzner in Falkenstein (FSN1) sowie der Managed-Datenbank von Elestio in derselben Region * dem Backup- und Wiederherstellungsverfahren gemäß Abschnitt 3 * der Speicherung der Sicherungen bei einem zweiten, vom Hosting unabhängigen Anbieter an einem anderen Standort, sodass ein Ausfall des Produktivstandorts oder des Hosting-Anbieters die Sicherungen nicht miterfasst * Eine Multi-Server- oder Cluster-Redundanz ist nicht Bestandteil des aktuellen Betriebsmodells.

5. Datenschutz durch Technikgestaltung (Art. 25 DSGVO)

Der Auftragnehmer setzt die Grundsätze von Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen um. Dies umfasst insbesondere: * **Datensparsamkeit:** Die Plattform ist so konzipiert, dass für die Nutzung von KI-Funktionen nur die inhaltlich notwendigen Daten übermittelt werden. Metadaten wie User-IDs und Klarnamen werden vor der Übermittlung an KI-Dienste entfernt. Übermittelt werden ausschließlich die für die jeweilige Funktion erforderlichen Inhalte (z. B. Freitextantworten, Dokumenteninhalte). * **Isolierte Verarbeitung:** KI-Funktionen nutzen separate Instanzen oder API-Zugänge, bei denen vertraglich ausgeschlossen ist, dass Eingabedaten zum Training der Modelle Dritter verwendet werden. * **EU-Routing, wo möglich:** Die Inferenz der eingesetzten Anthropic-Modelle ist technisch auf EU-Regionen festgelegt. * **Pseudonyme Identität bei eingebetteter Nutzung:** Erfolgt der Zugriff über eine in Fremdsysteme eingebettete Komponente ohne persönliche Anmeldung, wird aus der Kennung des einbettenden Systems und der dortigen Nutzerkennung ein kryptografischer Streuwert gebildet. Gespeichert wird ausschließlich dieser Wert, nicht die zugrunde liegende Kennung. * **Modellfreigabe je Mandant:** Für den Dialog mit Lernenden lässt sich mandantenbezogen festlegen, welche Sprachmodelle verwendet werden dürfen. Die Freigabe wird zur Laufzeit bei jeder Anfrage geprüft; ein nicht freigegebenes Modell wird durch ein freigegebenes ersetzt, statt die Anfrage abzubrechen. Nicht erfasst sind Texteinbettungen, Sprachausgabe und die Autorenwerkzeuge der Kurserstellung. * **Automatisierte Löschung laufender Bestände:** Unabhängig von der Löschung nach Vertragsende (AVV Ziffer 12) werden Lernstände aus eingebetteter Nutzung ohne Anmeldung 270 Tage nach der letzten Aktivität der jeweiligen Lernidentität gelöscht, Verläufe der Dialogbausteine 270 Tage nach dem Zeitpunkt der einzelnen Nachricht. Die Läufe erfolgen täglich automatisiert. * **Datensparsame Voreinstellung bei Fremdinhalten:** Videos und Karten externer Anbieter werden ohne Zutun des Nutzers nicht geladen (Abschnitt 2.4).

6. Auftragskontrolle

Der Auftragnehmer stellt sicher, dass Unterauftragsverarbeiter nur unter Beachtung der gesetzlichen Anforderungen und der vertraglichen Vorgaben eingesetzt werden. Dies umfasst insbesondere: * Abschluss geeigneter Vertragsgrundlagen (z. B. Standardvertragsklauseln bei Anbietern in Drittländern) * Prüfung der vom Unterauftragsverarbeiter bereitgestellten Datenschutz- und Sicherheitsmaßnahmen anhand öffentlich verfügbarer Dokumentationen und Sicherheitsnachweise * Information des Auftraggebers über neue Unterauftragsverarbeiter gemäß den vertraglichen Regelungen * Dokumentierte Erfassung der eingesetzten Unterauftragsverarbeiter, ihrer Aufgabenbereiche und der jeweils geltenden Vertragsgrundlagen * Keine Beauftragung weiterer Unterauftragsverarbeiter ohne vorherige Prüfung ihrer datenschutzrechtlichen Eignung

7. Trennung von Daten

Die Plattform verwendet eine mandantenfähige Architektur. Jeder Nutzer ist eindeutig einem Mandanten zugeordnet; sämtliche weiteren Datensätze sind über diese Nutzerbeziehung mittelbar dem jeweiligen Mandanten zuordenbar. Personenbezogene Daten sowie personenbezogene Lerndaten werden mandantenbezogen verarbeitet und sind für andere Mandanten nicht einsehbar. Innerhalb der gemeinsamen Datenbank erfolgt eine logische Trennung der Daten durch Mandantenkennungen und Rollenmodelle. Für Medien- und Anhangsdateien im Objektspeicher wird die Trennung dadurch gewahrt, dass eine Abrufadresse nur nach Prüfung der Berechtigung ausgegeben wird (Abschnitt 1.3). Mandantenübergreifende Auswertungen können durchgeführt werden, sofern sie ausschließlich auf aggregierten oder anonymisierten Daten basieren und keine Rückschlüsse auf einzelne Personen ermöglichen.

8. Aktualisierung der TOM

Der Auftragnehmer kann diese Maßnahmen anpassen, wenn sich technische oder organisatorische Anforderungen ändern. Anpassungen sind zulässig, sofern: * das Schutzniveau nicht reduziert wird, * der Zweck der Maßnahmen erhalten bleibt, * die Änderungen dokumentiert werden.

Ende von Anhang 1