



# Technische und organisatorische Maßnahmen

Kurzfassung für Schulleitung und Datenschutzbeauftragte. Die Spalte „Nachlesen“ verweist auf die Abschnitte der Datenschutzerklärung unter [kopernikus-lernapp.de/datenschutz.html](https://kopernikus-lernapp.de/datenschutz.html).

**Rahmen:** Datenbank, Anmeldung, Dateien und Serverfunktionen laufen bei einem Hosting-Dienstleister in einem Rechenzentrum in Frankfurt am Main (EU). Website und App-Dateien werden über ein weltweites CDN ausgeliefert. Für Daten von Schüler:innen ist die Schule verantwortlich; Kopernikus verarbeitet sie als Auftragsverarbeiter (Art. 28 DSGVO).

| Bereich                          | Maßnahme                                                                                                                                                                                                                                                                                                                     | Nachlesen         |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Verschlüsselung                  | Alle Verbindungen per TLS (https). Gemerkte WebUntis-Passwörter verschlüsselt (AES-GCM); das Apple-Token für die Trennung der Apple-ID beim Löschen verschlüsselt auf dem Server.                                                                                                                                            | Abschn. 5, 14, 23 |
| Zugang                           | Lehrkräfte: E-Mail und Passwort bzw. Anmeldelink oder Google-, Microsoft-, Apple-Konto. Schüler:innen: Klassencode, Vorname und ggf. eigenes Passwort – ohne E-Mail-Adresse. Eltern und Ausbildungsbetriebe: Code und Passwort.                                                                                              | Abschn. 5         |
| Passwörter und Fehlversuche      | Passwörter von Schüler:innen, Eltern und Betrieben nur als gesalzene Hashwerte (bcrypt). Nach 10 Fehlversuchen in 15 Minuten sperrt die Schüler-Anmeldung 15 Minuten; auch Eltern- und Betriebs-Zugang sperren nach wiederholten Fehlversuchen. Klassen lassen sich für neue Anmeldungen schließen.                          | Abschn. 5, 23     |
| Zugriff (Rechte)                 | Rechteprüfung in der Datenbank (Row Level Security) je Person und Rolle: Schüler:innen sehen nur eigene Daten, Lehrkräfte nur ihre Klassen. In der Gruppenarbeit sieht eine Gruppe nur ihre eigenen Placemat-Felder; fremde Antworten im Peer-Feedback gibt der Server nur ohne Namen heraus.                                | Abschn. 6, 23     |
| Einwilligung technisch gesichert | Inhalte des Eltern-Zugangs gibt die Datenbank nur bei gültiger Einwilligung zur aktuellen Fassung heraus; Bewertungen für Ausbildungsbetriebe nur nach Freigabe der Klassenleitung.                                                                                                                                          | Abschn. 5, 23     |
| Besondere Kategorien             | Felder nach Art. 9 DSGVO sind freiwillig, nur für Klassenleitung und Schulleitung sichtbar und gehen nie an KI-Dienste.                                                                                                                                                                                                      | Abschn. 8         |
| Integrität                       | Noten, Bewertungen und das Protokoll von Klassenarbeiten setzt nur die Lehrkraft – geprüft in der Datenbank. Entwürfe eines Tadelns gibt nur die anlegende Lehrkraft frei.                                                                                                                                                   | Abschn. 23        |
| Protokollierung                  | Wichtige Änderungen in Klassen werden protokolliert; der Beitritt weiterer Lehrkräfte zu einer Klasse wird protokolliert und gemeldet. KI-Nutzung wird mit Funktion, Modell und Umfang protokolliert, ohne Inhalt der Anfrage.                                                                                               | Abschn. 9, 17, 23 |
| KI und Datenminimierung          | KI nur nach Zustimmung; keine Kontodaten an KI-Anbieter; Vorkorrektur ohne Namen; Lernstandsanalyse und KI-Check mit Pseudonymen (S1, S2, ...); Namen aus Klassen- und Kurslisten ersetzt die App vor dem Senden, soweit sie sie erkennt. KI-Hilfen für Schüler:innen je Klasse abschaltbar – auch der Server lehnt dann ab. | Abschn. 9, 21     |

| Bereich                      | Maßnahme                                                                                                                                                                                                                                                                                   | Nachlesen          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Schlüssel und Dienste</b> | Schlüssel für KI-, Mail- und Push-Dienste liegen nur auf dem Server, nie im Programmcode der App. Kontingente für KI-Anfragen und Tagesgrenzen für den Mail-Versand schützen vor Missbrauch.                                                                                               | Abschn. 11, 13, 23 |
| <b>Geräte</b>                | Beim Abmelden entfernt die App Sitzung, zwischengespeicherte Antworten der Datenbank und Entwürfe von Schüler:innen vom Gerät. Während einer LEK oder Klassenarbeit sperrt die Android-App Bildschirmfotos.                                                                                | Abschn. 18, 19     |
| <b>Verfügbarkeit</b>         | Sicherungskopien der Datenbank beim Hoster, die nach dessen Fristen überschrieben werden. Kurze Offline-Nutzung durch zwischengespeicherte Antworten (höchstens 5 Minuten).                                                                                                                | Abschn. 18, 22     |
| <b>Löschung</b>              | Lehrkräfte löschen Schüler:innen, Klassen und ihr Konto selbst; Dateien folgen automatisch, in der Regel innerhalb eines Tages. Feste Fristen in der Datenbank, z. B. Gruppeneinteilungen 30 Tage, Fehlerprotokolle 90 Tage, Zähler der KI-Anfragen 62 Tage, Nutzungsereignisse 13 Monate. | Abschn. 22, 25     |
| <b>Organisation</b>          | Daten der Schule sieht Kopernikus nicht routinemäßig ein, auch nicht über ein Administratorkonto – nur auf Weisung der Schule. Unterauftragsverarbeiter sind vertraglich gebunden (siehe AVV-Muster, Anlage 2).                                                                            | Abschn. 2, 20      |
| <b>Überprüfung</b>           | Automatisierte Prüfungen vor Veröffentlichungen, darunter Prüfungen der Rechte-Regeln der Datenbank.                                                                                                                                                                                       | –                  |

Kopernikus Lernapp · Lukas Jarius · Gerhart-Hauptmann-Straße 25, 15834 Rangsdorf · [lukas.jarius@kopernikus-lernapp.de](mailto:lukas.jarius@kopernikus-lernapp.de) · Unterlagen für Schulen: [kopernikus-lernapp.de/fuer-schulen.html](https://kopernikus-lernapp.de/fuer-schulen.html)