Technische und organisatorische Maßnahmen

Version 1.3 · gültig ab 09.11.2026 · Prüfsumme 1eff19a39621

Anlage zum Vertrag zur Auftragsverarbeitung. Beschreibt die Maßnahmen des Auftragnehmers nach Art. 32 DSGVO für MeisterLEICHT. Aufgeführt ist nur, was umgesetzt ist. Maßnahmen, die geplant, aber noch nicht umgesetzt sind, stehen gesondert im letzten Abschnitt.

1. Betrieb und Aufbau

Der Server ist ein Arbeitsplatzrechner des Auftragnehmers mit Docker Desktop in dessen Räumen (Standort: Räume des Anbieters in Deutschland (eigener Rechner, kein Rechenzentrum)). Ein Hosting-Dienstleister ist nicht beteiligt. MeisterLEICHT läuft dort in eigenen Containern mit eigener Datenbank, eigenen Datenträgern (Volumes) und eigenen Netzen. Auf demselben Rechner laufen auch die Entwicklungsumgebung und ein weiteres Produkt des Auftragnehmers, jeweils in getrennten Containern mit eigenen Datenbanken.

- Datenbank (PostgreSQL) und die eigene Spracherkennung laufen in einem internen Container-Netz ohne von außen erreichbaren Port.
- Der Zugriff aus dem Internet erfolgt ausschließlich über einen vom Server ausgehend aufgebauten Tunnel von Cloudflare. Für eingehende Verbindungen aus dem Internet ist am Server kein Port geöffnet.
- Die Spracherkennung läuft je nach Vertrag des Betriebs über Workers AI von Cloudflare oder auf diesem Server; fällt Cloudflare aus, übernimmt dieser Server. Zu Cloudflare gehen die Aufnahmen verschlüsselt (TLS); nach den kommerziellen Bedingungen von Cloudflare (Self-Serve Subscription Agreement) und seinen Angaben zu Workers AI werden sie dort nicht über die Anfrage hinaus gespeichert und nicht zum Training verwendet. Einen weiteren externen Sprachdienst gibt es nicht. Gespeichert werden Aufnahmen nur, wenn der Betrieb „Audio speichern“ eingeschaltet hat – dann auf diesem Server.

2. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

2.1 Zutrittskontrolle

Standort des Servers: Räume des Anbieters in Deutschland (eigener Rechner, kein Rechenzentrum). Zutrittsschutz: Der Server-Rechner steht in privaten, nicht öffentlich zugänglichen Räumen des Inhabers; Dritte haben keinen unbegleiteten Zutritt..

2.2 Zugangskontrolle

- Anmeldung nur mit persönlichem Benutzerkonto (E-Mail-Adresse und Passwort mit mindestens 10 Zeichen). Passwörter werden nur als Hash gespeichert.
- Zweiter Faktor (zeitbasierte Einmalcodes, TOTP) für alle Nutzer einrichtbar; für Inhaber und Administratoren kann er verpflichtend geschaltet werden.
- Begrenzung der Zahl von Anmeldeversuchen und Anfragen je Zeitraum (Ratenbegrenzung).
- Sitzungen sind nach 30 Tagen ohne Nutzung ungültig; Abmelden beendet die Sitzung sofort.
- Datenbank und interne Dienste sind aus dem Internet nicht erreichbar.
- Administratorzugriff auf den Server-Rechner, Anmeldung und Bildschirmsperre: Administratorzugriff hat ausschließlich der Inhaber persönlich, über sein eigenes, passwortgeschütztes Benutzerkonto..
- Testsysteme sind zusätzlich durch einen Zugangscode geschützt.

2.3 Zugriffskontrolle

- Rollen- und Rechtekonzept mit sieben Rollen (Inhaber, Administrator, Büro, Disposition, Buchhaltung, Mitarbeiter im Außendienst, Nur Ansicht). Rechte werden bei jeder Anfrage auf dem Server geprüft, nicht nur in der Oberfläche.
- Mitarbeitende im Außendienst sehen nur eigene Aufträge und Arbeitsscheine. Stundenkostensätze sind nur mit dem Recht zur Bearbeitung von Mitarbeiterdaten sichtbar. Finanzielle Freigaben erfordern ein gesondertes Recht.
- Dateien werden nur nach Rechteprüfung ausgeliefert. Das Herunterladen von Dateien und Belegen wird protokolliert.
- Zugangsdaten zu Postfächern und Schnittstellen (Passwörter, Zugriffstoken, Schlüssel) werden mit AES-256-GCM verschlüsselt gespeichert.

2.4 Trennungskontrolle

- Jeder Datensatz ist genau einem Betrieb zugeordnet. Der Betrieb wird bei jeder Anfrage aus der Anmeldung abgeleitet und nie aus Eingaben des Browsers oder der KI übernommen.
- Die Trennung der Betriebe erfolgt in der Anwendung: Jede Abfrage filtert nach dem Betrieb. Automatisierte Tests prüfen, dass Zugriffe auf Daten eines anderen Betriebs scheitern.
- Dateien liegen je Betrieb in getrennten Verzeichnissen.
- KI-Gespräche sind zusätzlich je Nutzer getrennt. KI-Werkzeuge erhalten den Betrieb und die Rechte des Nutzers vom Server.
- Demo- und Testdaten liegen in eigenen Betrieben.
- Entwicklung und Produktivbetrieb sind getrennt: eigene Kopie des Programmstands für den Betrieb, eigene Datenbank und eigene Konfiguration mit eigenen Schlüsseln. Entwicklung und Tests nutzen eine eigene Datenbank mit Demo- und Testdaten. Auf die Produktivdatenbank kann nur lokal am Server zugegriffen werden (Wartungszugang, nur bei Bedarf eingeschaltet).

2.5 Pseudonymisierung und Datensparsamkeit

- In Nachweisen von Zustimmungen wird die IP-Adresse nur als Prüfwert gespeichert, der mit einem geheimen Schlüssel gebildet wird (HMAC); die Browser-Kennung wird auf 200 Zeichen gekürzt.
- Die Produktstatistik speichert je Ereignis nur Ereignisname, Zeitpunkt, die Kennung des Betriebs und kleine Angaben wie Tarif oder Gewerk (pseudonym, ohne Namen, E-Mail-Adressen, IP-Adressen oder Inhalte).
- Sprachaufnahmen werden standardmäßig nach der Umwandlung in Text verworfen.
- An den Anbieter des KI-Modells werden keine Kennungen des Betriebs oder einzelner Personen als Metadaten übermittelt.

3. Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)

3.1 Weitergabekontrolle

- Verbindungen zwischen Browser und Cloudflare sind mit TLS verschlüsselt; im Produktivbetrieb verlangt MeisterLEICHT HTTPS (HSTS). Cloudflare leitet den Datenverkehr über den Tunnel an den Server weiter. Da die TLS-Verbindung bei Cloudflare endet, kann Cloudflare den Datenverkehr technisch einsehen (siehe Anlage Unterauftragsverarbeiter).
- Sicherheits-Header und eine Content-Security-Policy begrenzen Angriffe im Browser.
- E-Mails an Dritte versendet MeisterLEICHT nur nach Freigabe bzw. im Rahmen der vom Betrieb eingeschalteten kontrollierten Automatik, und zwar über das vom Betrieb verbundene Postfach. Hat der Betrieb kein Postfach zum Versand verbunden, laufen seine E-Mails samt Anhängen über den E-Mail-Versanddienst des Auftragnehmers (siehe Anlage Unterauftragsverarbeiter).

- Inhalte gehen nur bei eingeschalteten KI-Funktionen an den Anbieter des KI-Modells, über eine verschlüsselte Verbindung.

3.2 Eingabekontrolle

- Fachliche Änderungen, Freigaben und Ausführungen werden mit Zeitpunkt und handelnder Stelle (Person, KI, System) protokolliert.
- Das Protokoll, der Verlauf der Freigaben und die Nachweise von Zustimmungen sind durch Datenbank-Trigger gegen Änderung und Löschung über die Anwendung geschützt; Eingriffe auf Datenbankebene erfolgen nur im dokumentierten Löschverfahren.
- Zu jeder angenommenen Fassung eines Vertragsdokuments wird der Wortlaut gespeichert; eine Fassung kann nach der ersten Zustimmung im Produktivbetrieb nicht mehr unbemerkt geändert werden.
- Jede Freigabe bezieht sich auf eine bestimmte Version mit Prüfsumme (SHA-256) des Inhalts. Ausgeführt wird nur die freigegebene Fassung; eine Änderung erfordert eine neue Freigabe. Jede Ausführung ist gegen doppeltes Auslösen gesichert.
- Gespeicherte Dateien erhalten eine Prüfsumme (SHA-256).
- Von der KI vorbereitete Vorgänge sind in den Daten als solche gekennzeichnet (Herkunft und Modell).

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b und c DSGVO)

- Tägliche Sicherung (03:30 Uhr) der Datenbank und der Dateiablage mit Prüfsummen; aufbewahrt werden die letzten 14 Sicherungsläufe. Die Sicherungen liegen auf dem Server-Rechner. Zusätzliche Sicherungen außerhalb dieser Rotation (z. B. vor einem Umzug) werden nach 30 Tagen gelöscht.
- Eine zusätzliche Kopie auf einen weiteren Datenträger schreibt das Sicherungsverfahren nur verschlüsselt (AES-256, Schlüsselableitung mit PBKDF2); eine unverschlüsselte Kopie lehnt es ab.
- Die Wiederherstellung wird alle vier Wochen mit einer Wiederherstellungsübung in einer getrennten Testdatenbank geprüft; Datum und Ergebnis werden protokolliert.
- Ratenbegrenzungen für Anmeldung, KI-Chat und Spracherkennung sowie ein monatlicher Kostenrahmen für die KI schützen vor Überlastung und Missbrauch.
- Server-Protokolle werden größenbasiert rotiert, je Dienst höchstens 5 × 10 MB.

5. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 Buchst. d DSGVO)

- Zur Software gehören automatisierte Tests, unter anderem für Rechteprüfung, Freigabe-Logik, Trennung der Betriebe und die Versionierung der Rechtstexte. Sie werden bei der Entwicklung von Änderungen ausgeführt. Vor jeder Aktualisierung des Servers prüft das Update-Skript die Rechtstexte auf fehlende Angaben; der Bau des Programms bricht bei Typfehlern ab.
- Wiederherstellungsübungen laufen alle vier Wochen automatisch und werden mit Datum und Ergebnis protokolliert.
- Sicherheitshinweise zu eingesetzten Komponenten werden bei Aktualisierungen berücksichtigt.

6. Maßnahmen für die KI-Funktionen

- Die KI-Funktionen sind beim Anlegen eines Betriebs ausgeschaltet. Das Einschalten wird mit Person, Zeitpunkt und Fassung der Zusatzbedingungen protokolliert.

- Die KI kann nichts freigeben und nichts selbst nach außen ausführen; Vorgänge mit Außenwirkung oder finanziellen Folgen laufen über das Freigabe-Center. Nur wenn der Betrieb die kontrollierte Automatik einschaltet, werden die von ihm freigeschalteten Vorgangsarten innerhalb seiner Betragsgrenzen ohne Einzelfreigabe ausgeführt.
- Mit jeder KI-Anfrage geht nur ein kurzer Betriebskontext mit. Angaben zu Mitarbeitenden ruft die KI nur bei Bedarf über Werkzeuge mit Rechteprüfung ab; Abwesenheitsgründe (z. B. Krankheit) erhält sie nicht, nur „abwesend“.
- Fragt jemand nach einer Bewertung oder einem Vergleich von Mitarbeitenden, stehen der KI in dieser Anfrage keine Werkzeuge mit Arbeitszeiten, Einsätzen oder Abwesenheiten je Person zur Verfügung.
- Ausgehende E-Mails aus KI-Entwürfen tragen eine maschinenlesbare Kennzeichnung im E-Mail-Kopf (X-BetriebNOW-AI-Assisted).
- Inhalte aus E-Mails und Dokumenten werden der KI als Daten gekennzeichnet übergeben, nicht als Anweisungen.
- KI-Werkzeuge prüfen die Rechte des jeweiligen Nutzers auf dem Server.
- An den Anbieter des KI-Modells werden keine Kennungen des Betriebs oder einzelner Personen als Metadaten übermittelt.
- Server-Protokolle der KI-Funktionen enthalten keine Eingaben oder Antworten, nur Fehlermeldungen. Konsolen-Ausgaben werden vor dem Schreiben gefiltert: Abfrageparameter in Adressen und in Datenbankfehlern zitierte Werte werden entfernt, E-Mail-Adressen und IBANs maskiert. Namen in Fehlermeldungen können enthalten bleiben.

7. Organisatorische Maßnahmen und Voreinstellungen

- Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO): KI-Funktionen aus, Speicherung von Sprachaufnahmen aus, keine Analyse- oder Werbe-Cookies.
- Dokumentiertes Lösch- und Aufbewahrungskonzept: Export der Daten eines Betriebs durch den Inhaber, Anonymisieren von Kunden und ausgeschiedenen Beschäftigten, Löschung eines Betriebs auf Antrag nach dokumentiertem Verfahren mit Protokoll.
- Rechnungen, Zahlungen und versendete Belege sind gegen versehentliches Löschen geschützt; statt Löschen gibt es Archivieren bzw. Anonymisieren.
- Zustimmungen zu Vertragsunterlagen werden mit Version und Prüfsumme des angezeigten Textes nachgewiesen; der Wortlaut jeder angenommenen Fassung wird gespeichert.

8. Geplante Maßnahmen

Die folgenden Maßnahmen sind geplant und noch **nicht umgesetzt**. Sie werden erst nach ihrer Umsetzung in die vorstehenden Abschnitte übernommen:

- zusätzliche Trennung der Betriebe in der Datenbank (Row-Level-Security) und datenbankseitige Prüfung, dass Verweise nur auf Datensätze desselben Betriebs zeigen,
- Verschlüsselung der gespeicherten Daten: Datenträgerverschlüsselung des Server-Rechners einschließlich der Docker-Datenträger und der Sicherungen – vor dem ersten Betrieb mit echten Daten,
- verschlüsselte Sicherung an einem zweiten Ort außerhalb des Serverstandorts,
- verbindlicher automatischer Testlauf vor jeder Aktualisierung des Servers,
- Hash-Verkettung oder Zeitstempel für Protokolle und Nachweise,
- Verfahren zum Wechsel des Schlüssels für gespeicherte Zugangsdaten,

- externer Sicherheitstest (Penetrationstest) und gezielte Tests gegen eingeschleuste Anweisungen (Red-Team-Test),
- zusätzliche Zugangskontrolle vor der Anwendung über Cloudflare Access,
- automatische Löschung der Daten nach Vertragsende (bisher dokumentiertes manuelles Verfahren),
- zentrale Überwachung der Protokolle und Erkennung von Angriffen,
- Betrieb in einem Rechenzentrum mit redundanter Strom- und Netzanbindung.