

Vertrag zur Auftragsverarbeitung

nach Art. 28 DSGVO für Lokyy Managed · Muster

Verantwortlicher (Auftraggeber)

Firma

Anschrift

Ansprechperson Datenschutz

nachfolgend „Kunde“

Auftragsverarbeiter

CodeLabs Hees & Rosenbusch GbR

Marke Lokyy

Hauptstr. 5b, 21394 Westergellersen

info@lokyy.de

nachfolgend „Lokyy“

§ 1 Gegenstand und Dauer

(1) Lokyy betreibt für den Kunden eine eigene Instanz der Software Lokyy auf einem eigenen Server in Deutschland (Lokyy Managed) nach dem zwischen den Parteien geschlossenen Vertrag und den Allgemeinen Geschäftsbedingungen von Lokyy (nachfolgend „Hauptvertrag“). Dabei verarbeitet Lokyy personenbezogene Daten im Auftrag des Kunden. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO.

(2) Die Dauer dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet jedoch nicht vor Abschluss der Löschung nach § 9.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) **Art und Zweck:** Bereitstellung, Betrieb, Wartung, Aktualisierung und Sicherung der Lokyy-Instanz des Kunden sowie Support. Dazu gehören das Speichern, Ordnen, Durchsuchen, Auswerten und Übermitteln von Daten nach den Einstellungen und Anweisungen des Kunden, auch durch KI-Modelle und Agenten.

(2) **Arten personenbezogener Daten:**

- Stammdaten der Nutzer: Name, E-Mail-Adresse, Rolle, Bereich, Einstellungen
- Nutzungs- und Protokolldaten: Anmeldungen, Audit-Log, Agenten-Läufe, Verbrauch
- Inhalte, die der Kunde einbringt oder erzeugt: Chats, Dokumente, Firmenwissen, E-Mails, Nachrichten aus angebundenen Kanälen (zum Beispiel WhatsApp, Microsoft Teams, Web-Chat), Kalendereinträge, Aufgaben und Dateien, einschließlich darin enthaltener Kontakt- und Vertragsdaten Dritter

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) verarbeitet Lokyy nur, soweit der Kunde sie einbringt. Der Kunde prüft, ob dies zulässig ist, und nutzt dafür die Schutzfunktionen von Lokyy, insbesondere die Datenschleuse.

(3) Kategorien betroffener Personen:

- Beschäftigte und sonstige Nutzer des Kunden
- Kunden, Interessenten, Lieferanten und Geschäftspartner des Kunden
- sonstige Personen, deren Daten in den Inhalten des Kunden enthalten sind

(4) **Ort der Verarbeitung:** Die Instanz wird ausschließlich in Rechenzentren in Deutschland betrieben. Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums findet nicht statt, soweit der Kunde nicht selbst Dienste außerhalb dieses Raums anbindet (zum Beispiel über eigene Zugangsschlüssel zu einem Modellanbieter).

§ 3 Weisungen

(1) Lokyy verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Kunden, es sei denn, Lokyy ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt Lokyy dem Kunden diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Die Weisungen ergeben sich aus dem Hauptvertrag, diesem Vertrag und den Einstellungen, die der Kunde in der Verwaltung seiner Instanz vornimmt (zum Beispiel freigegebene Modelle, Datenflüsse, Aufbewahrungsfristen). Weitere Weisungen erteilt der Kunde in Textform.

(3) Ist Lokyy der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert Lokyy den Kunden unverzüglich und darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.

§ 4 Pflichten von Lokyy

(1) Lokyy

- setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,
- trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind,
- unterstützt den Kunden mit geeigneten Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Art. 12 bis 22 DSGVO), insbesondere durch die Export- und Löschfunktionen der Software, und leitet Anfragen Betroffener, die bei Lokyy eingehen, unverzüglich an den Kunden weiter,
- unterstützt den Kunden bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation),
- stellt dem Kunden alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung.

(2) Lokyy meldet dem Kunden Verletzungen des Schutzes personenbezogener Daten unverzüglich, in der Regel innerhalb von 24 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie vorliegen.

(3) Ansprechpartner für Datenschutz bei Lokyy ist Oliver Hees, erreichbar unter info@lokyy.de. Ein Datenschutzbeauftragter ist nicht bestellt, da die gesetzlichen Voraussetzungen dafür nicht vorliegen. Ändert sich dies, teilt Lokyy dem Kunden die Kontaktdaten mit.

(4) Lokyy nutzt die Daten des Kunden nicht für eigene Zwecke und nicht zum Training von KI-Modellen.

§ 5 Pflichten des Kunden

(1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Zulässigkeit der Daten, die er in Lokyy einbringt, und für die Auswahl der Modelle und Datenflüsse, die er freigibt.

(2) Der Kunde informiert Lokyy unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 6 Unterauftragnehmer

(1) Der Kunde erteilt Lokyy die allgemeine Genehmigung, Unterauftragnehmer einzusetzen. Bei Vertragsschluss sind die in Anlage 2 genannten Unterauftragnehmer genehmigt.

(2) Lokyy informiert den Kunden mindestens 4 Wochen vorher in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragnehmers. Der Kunde kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, kann der Kunde den Hauptvertrag zum Zeitpunkt der Änderung außerordentlich kündigen.

(3) Lokyy verpflichtet jeden Unterauftragnehmer vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen, und überprüft deren Einhaltung in angemessenem Umfang.

(4) Nicht als Unterauftragsverhältnis gelten Dienste, die der Kunde selbst beauftragt und in seiner Instanz anbindet, etwa eigene Zugangsschlüssel zu Modellanbietern, eigene Postfächer oder Messenger-Konten.

§ 7 Nachweise und Kontrollen

(1) Lokyy weist die Einhaltung seiner Pflichten durch diese Unterlagen, die Beschreibung der technischen und organisatorischen Maßnahmen, die Zertifikate der Rechenzentren und auf Anfrage durch weitere geeignete Nachweise nach.

(2) Darüber hinaus kann der Kunde Prüfungen, einschließlich Inspektionen, selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen. Prüfungen sind mindestens 14 Tage vorher anzukündigen, finden während der üblichen Geschäftszeiten statt und dürfen den Betrieb von Lokyy nicht unverhältnismäßig stören. Inspektionen im Rechenzentrum richten sich nach den Regeln des Rechenzentrumsbetreibers.

§ 8 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags.

§ 9 Löschung und Rückgabe nach Vertragsende

(1) Nach Ende des Hauptvertrags bleibt die Instanz 30 Tage lang lesend erreichbar, damit der Kunde seine Daten exportieren kann. Lokyy unterstützt den Export der gesamten Instanz in offenen Formaten.

(2) Nach Ablauf dieser Frist löscht Lokyy alle personenbezogenen Daten des Kunden einschließlich aller Sicherungen und bestätigt die Löschung in Textform, sofern keine Pflicht zur Speicherung nach

Unionsrecht oder dem Recht eines Mitgliedstaats besteht.

§ 10 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit es um den Schutz personenbezogener Daten geht.

(2) Änderungen dieses Vertrags bedürfen der Textform. Der Vertrag kann elektronisch geschlossen werden.

(3) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum

Ort, Datum

Kunde (Name, Funktion, Unterschrift)

Lokyy, CodeLabs Hees & Rosenbusch GbR

Anlage 1: Technische und organisatorische Maßnahmen

Diese Übersicht beschreibt die technischen und organisatorischen Maßnahmen (TOM), mit denen die CodeLabs Hees & Rosenbusch GbR (Marke Lokyy, nachfolgend „Lokyy“) personenbezogene Daten bei Lokyy Managed schützt. Lokyy Managed bedeutet: Jeder Kunde erhält eine eigene Instanz auf einem eigenen Server in Deutschland, die nicht mit anderen Kunden geteilt wird. Maßnahmen im Rechenzentrum erbringt der Unterauftragnehmer Hetzner Online GmbH im Rahmen seines nach ISO/IEC 27001:2022 zertifizierten Managementsystems.

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

1.1 Zutrittskontrolle

- Server stehen ausschließlich in Rechenzentren der Hetzner Online GmbH in Nürnberg und Falkenstein (Deutschland), zertifiziert nach ISO/IEC 27001:2022.
- Zutritt zu den Rechenzentren nur für berechtigtes Personal des Betreibers, mit elektronischem Zutrittskontrollsystem, Videoüberwachung und Sicherheitsdienst gemäß dem zertifizierten Managementsystem des Betreibers.
- Beschäftigte von Lokyy haben keinen physischen Zutritt zu den Servern.

1.2 Zugangskontrolle (Systeme)

- Administrativer Zugang zu den Servern nur für namentlich benannte Personen von Lokyy.
- Anmeldung am Server nur mit kryptografischen Schlüsseln, keine Passwort-Anmeldung.
- Alle Verbindungen zur Instanz sind mit TLS verschlüsselt.
- Anmeldung der Nutzer in Lokyy mit Passwort oder über den Identity Provider des Kunden (Keycloak, OIDC). Zwei-Faktor-Anmeldung (TOTP) verfügbar und pro Rolle als Pflicht einstellbar.
- Abmelden im Identity Provider beendet auch die Sitzung in Lokyy.

1.3 Zugriffskontrolle (Daten)

- Rollen- und Rechtekonzept in Lokyy. Rechte werden an vier Stellen durchgesetzt: Oberfläche, Schnittstelle (API), Werkzeuge der Agenten und Datenbank.
- Zeilensicherheit in der Datenbank (Row Level Security): Jede Abfrage sieht nur die Zeilen, die der angemeldeten Person erlaubt sind.
- Zugangsdaten und API-Schlüssel werden verschlüsselt in der Datenbank gespeichert und nie im Klartext protokolliert.
- Fernwartung durch Lokyy innerhalb der Anwendung nur nach Freigabe durch einen Administrator des Kunden; jeder Zugriff wird im Audit-Log protokolliert.

1.4 Trennungskontrolle

- Eigener Server und eigene Datenbank pro Kunde. Keine gemeinsame Datenhaltung mehrerer Kunden.
- Test- und Demosysteme sind von Kundeninstanzen getrennt und enthalten keine Kundendaten.

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

- Datenschleuse: Personenbezogene Angaben (zum Beispiel Namen, IBAN, Telefonnummern) werden vor der Übermittlung an Cloud-KI-Modelle durch Platzhalter ersetzt und erst in der Antwort wieder eingesetzt.
- Modus „Pflicht“: Es werden nur lokale Modelle genutzt, kein Klartext verlässt den Server.

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

2.1 Weitergabekontrolle

- Übertragung nur verschlüsselt (TLS).
- Jeder Datenfluss nach außen (zum Beispiel zu Cloud-Modellen, Postfächern, Messengern) ist in der Verwaltung einzeln sichtbar und abschaltbar; die Übersicht ist für das Verzeichnis von Verarbeitungstätigkeiten exportierbar.
- Sicherungen werden vor dem Speichern verschlüsselt (AES-256-GCM).

2.2 Eingabekontrolle

- Audit-Log für Admin-Aktionen, Rechteänderungen, Freigaben und Tool-Aufrufe der Agenten, Aufbewahrung ab Werk 365 Tage.
- Agenten-Läufe werden mit Schritten, Werkzeugen und Modell nachvollziehbar protokolliert.
- Anweisungen von Agenten und Skills sind versioniert.
- Aktionen mit Wirkung nach außen (zum Beispiel Mail senden) benötigen eine Freigabe durch einen Menschen.

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

- Verschlüsselte Sicherung von Datenbank und Dateien nach Zeitplan und vor jedem Update.
- Probe-Wiederherstellung der Sicherungen.
- Automatisches Zurückrollen bei einem fehlgeschlagenen Update.
- Überwachung der Instanzen auf Erreichbarkeit und Fehler.
- Rechenzentrum mit redundanter Stromversorgung, Klimatisierung, Brandfrüherkennung und redundanter Netzanbindung gemäß dem zertifizierten Managementsystem des Betreibers.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Lieferkette: Alle Softwarepakete sind exakt gepinnt, neue Versionen werden frühestens 14 Tage nach Veröffentlichung übernommen; Lizenz- und Schwachstellenprüfung in jeder Build-Pipeline.
- Auslieferung nur als signierte Images mit Stückliste (SBOM); die Signatur wird vor jedem Update geprüft.
- Sicherheitsupdates werden zeitnah eingespielt.
- Diese Maßnahmen werden mindestens einmal jährlich und bei wesentlichen Änderungen überprüft.

5. Organisatorische Maßnahmen

- Alle Personen mit Zugang zu Kundendaten sind schriftlich auf Vertraulichkeit verpflichtet.
- Unterauftragnehmer werden sorgfältig ausgewählt und vertraglich nach Art. 28 DSGVO gebunden.
- Datenschutzverletzungen werden nach einem festgelegten Ablauf erfasst, bewertet und gemeldet.
- Nach Vertragsende werden Instanz und Sicherungen nach Ablauf der Exportfrist von 30 Tagen gelöscht; die Löschung wird bestätigt.

Anlage 2: Unterauftragnehmer

Stand: 19.10.2026

Unterauftragnehmer	Leistung	Ort der Verarbeitung	Einsatz
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Server und Speicher für die Instanz und ihre Sicherungen	Rechenzentren in Nürnberg und Falkenstein (Deutschland), ISO/IEC 27001:2022 zertifiziert	immer bei Lokyy Managed
TensorX Ltd. (früher Tensorix) Unit 25, Classon House, Dundrum Business Park, Dublin 14, Irland (Company No. 796387)	Betrieb von KI-Modellen mit offenen Gewichten. Eingaben und Antworten werden nicht gespeichert und nicht zum Training genutzt	Rechenzentren in Dublin (Irland) und Helsinki (Finnland)	nur wenn der Kunde dieses Modell-Angebot von Lokyy freischaltet (nicht bei eigenen Schlüsseln des Kunden)
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Betrieb von KI-Modellen über Microsoft Azure (Foundry). Kein Training mit Kundendaten, keine Weitergabe an OpenAI	EU-Datenzone von Microsoft (EU-Staaten, zusätzlich Norwegen und Schweiz) oder eine feste EU-Region; Modelle mit weltweiter Verarbeitung nur nach ausdrücklicher Freischaltung durch den Kunden	nur wenn der Kunde dieses Modell-Angebot von Lokyy freischaltet (nicht bei eigenen Schlüsseln des Kunden)
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L- 1855 Luxemburg	Betrieb von KI-Modellen über AWS Bedrock, unter anderem Claude. Kein Training mit Kundendaten, keine Weitergabe an Modellhersteller	AWS-Regionen in der EU (Frankfurt, Stockholm, Mailand, Spanien, Irland, Paris); Modelle mit weltweiter Verarbeitung nur nach ausdrücklicher Freischaltung durch den Kunden	nur wenn der Kunde dieses Modell-Angebot von Lokyy freischaltet (nicht bei eigenen Schlüsseln des Kunden)
EUrouter B.V. Jacob van Lennepstraat 78H, 1053 HM Amsterdam, Niederlande (KvK 42054357)	Weiterleitung von Anfragen an weitere Cloud-KI-Modelle (Modell-Router, Ausweichweg). Inhalte werden standardmäßig nicht gespeichert und nicht zum Training genutzt	ausschließlich Europäischer Wirtschaftsraum; Modellanbieter laut Liste von EUrouter	nur wenn der Kunde den Ausweichweg über den Modell- Router freischaltet