

Sicherheitsmassnahmen

Version 2.1, gültig ab 5. Oktober 2026

OutLine Digital Agency (Einzelunternehmer), Via Dalmazia 36, 76125 Trani (BT), Italien — USt-IdNr. IT08978680729

Wie wir Daten schützen: getrennte Arbeitsbereiche, Verschlüsselung, Zugriffskontrolle, Sicherungen — einschliesslich dessen, was wir noch nicht tun.

Rechtsgrundlagen	Verordnung (EU) 2016/679 (DSGVO), Art. 32 (Sicherheit der Verarbeitung) · Verordnung (EU) 2016/679 (DSGVO), Art. 25 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)
------------------	---

1. Eine Datenbank pro Arbeitsbereich

Das ist die wichtigste Massnahme, und nur wenige Cloud-Anwendungen setzen sie um, weil sie mehr kostet: **Jeder Arbeitsbereich hat eine eigene Datenbank**, keine „Kunden“-Spalte in gemeinsam genutzten Tabellen.

Der Unterschied zeigt sich an dem Tag, an dem etwas schiefgeht. Bei gemeinsamen Tabellen zeigt eine Abfrage, der der Kundenfilter fehlt, die Daten aller; hier gibt es eine solche Abfrage nicht, denn die Daten anderer Kunden liegen in einer anderen Datenbank. Dasselbe gilt für Sicherungen, die sich Arbeitsbereich für Arbeitsbereich wiederherstellen lassen, ohne jemand anderen zu berühren.

2. Verschlüsselung

Was	Wie
Datenverkehr zur Website und zur Anwendung	HTTPS mit automatisch erneuerten Zertifikaten. Unverschlüsselter Datenverkehr wird umgeleitet.
Passwörter der Benutzer	Nie in lesbarer Form oder umkehrbar verschlüsselt gespeichert: nur ein mit bcrypt berechneter Hash, mit zufälligem Salt pro Benutzer und Vergleich in konstanter Zeit. Nicht einmal wir können sie lesen oder Ihnen mitteilen.
Sitzungstoken	Die Datenbank speichert nur einen Fingerabdruck des Tokens, nie den im Cookie abgelegten Wert.
Zugangsdaten von API-Konnektoren	Verschlüsselt gespeichert mit AES-256-GCM , mit einem eigenen, von den Daten getrennten Schlüssel. Wer eine Kopie der Datenbank erlangt, erhält nicht Ihre API-Schlüssel.

Das Bedrohungsmodell, ehrlich gesagt

Die Verschlüsselung der Zugangsdaten schützt davor, dass Datenbankabzüge und Sicherungen dorthin gelangen, wo sie nicht hingehören — mit Abstand der wahrscheinlichste Vorfall. Sie schützt nicht vor einer vollständigen Kompromittierung des Servers, bei der der Schlüssel dennoch lesbar ist: Dafür bräuchte es einen externen Schlüsselverwaltungsdienst, den wir heute nicht nutzen. Wir sagen das lieber offen, als Sie etwas anderes annehmen zu lassen.

3. Zugriffskontrolle

- Anmeldung mit persönlicher E-Mail-Adresse und Passwort; Sitzungen laufen ab und können beendet werden.
- Das Sitzungscookie ist **HttpOnly** (für Skripte nicht lesbar), **Secure** (nur über verschlüsselte Verbindungen gesendet) und **SameSite=Lax** (wird nicht mit Anfragen anderer Websites gesendet).
- **Rollen und Berechtigungen:** Inhaber/in, Administrator/in, Mitglied und Gast. Gäste sehen nur die Projekte, zu

denen sie eingeladen wurden.

- API-Schlüssel und Schlüssel für KI-Assistenten (MCP) handeln mit den Berechtigungen der Person, die sie erstellt hat, und können auf Lesezugriff beschränkt werden.
- Der Support-Zugriff nutzt einen **befristeten Benutzer, der nach 15 Minuten abläuft** und so lange Administratorrechte hat; jeder Zugriff wird dem Inhaber und den Administratoren des Arbeitsbereichs in der Admin-Konsole (Datenschutz und Compliance) angezeigt — wann, wie lange, durch wen, warum und welche Dateien heruntergeladen wurden —, der Inhaber wird beim Öffnen per E-Mail benachrichtigt, und der vollständige Datenexport ist währenddessen gesperrt.
- Die Daten eines Arbeitsbereichs sind nur innerhalb dieses Arbeitsbereichs erreichbar: Es gibt keine Ansicht, auch nicht für uns, die die Arbeitsdaten mehrerer Kunden gemeinsam zeigt.

4. Infrastruktur

- Server bei IONOS SE in Deutschland, in der Europäischen Union.
- Die Datenbank ist nicht aus dem Internet erreichbar: Sie lauscht nur auf dem Server selbst.
- Private Seiten (die Anwendung, die Verwaltungskonsole, die Einrichtung, die APIs) sind von der Indexierung durch Suchmaschinen ausgeschlossen.
- Geplante Aufgaben laufen über einen internen Kanal, der durch ein gemeinsames Geheimnis geschützt ist: Ohne dieses Geheimnis weist der Endpunkt jede Anfrage ab, statt offen zu bleiben.
- Ausgehende Aufrufe an Webhooks und API-Konnektoren sind nur über HTTPS und nur an öffentliche IP-Adressen erlaubt, sodass der Dienst nicht genutzt werden kann, um interne Netze zu erreichen.
- Aktualisierungen des Betriebssystems und der Abhängigkeiten werden regelmässig eingespielt; Releases durchlaufen einen geprüften Build, keine manuellen Änderungen auf dem Server.

5. Sicherung und Wiederherstellung

- **Tägliche** Sicherung aller Datenbanken, komprimiert; die Grösse jeder Kopie wird bei der Erstellung geprüft.
- **Rotation: 7 tägliche, 4 wöchentliche und 3 monatliche Kopien.** Ältere Kopien werden automatisch gelöscht.
- Die Kopien liegen auf derselben europäischen Infrastruktur, mit Berechtigungen, die auf den Systembenutzer beschränkt sind, der sie erzeugt.
- Wiederherstellungen erfolgen **pro Arbeitsbereich**: Ein Kunde kann zurückgesetzt werden, ohne die anderen zu berühren.
- Wiederherstellungen erfolgen von Hand. Wir verpflichten uns, das Verfahren mindestens zweimal jährlich an einer Kopie zu testen: Eine Sicherung, die nie wiederhergestellt wurde, ist keine Sicherung.

Was das für Sie bedeutet

Wenn Sie versehentlich etwas Wichtiges löschen, beträgt das nutzbare Zeitfenster für eine tagesgenaue Wiederherstellung in der Regel sieben Tage. Je früher Sie uns schreiben, desto wahrscheinlicher können wir alles wiederherstellen: Schreiben Sie an amministrazione@outlinedigital.it mit dem Namen des Arbeitsbereichs und, falls bekannt, dem Zeitpunkt des Vorfalls.

6. Wie die Software geschrieben ist

- Benutzereingaben werden vor dem Speichern validiert; Datenbankabfragen sind parametrisiert und können von aussen nicht manipuliert werden.
- Schreibende Vorgänge laufen über serverseitige Aktionen mit Rollenprüfung: Sie sind nicht durch manuelles Aufrufen einer Adresse erreichbar.
- Links zu öffentlichen Formularen verwenden **nicht erratbare Codes**, die widerrufen werden können: Das Neuerzeugen eines Codes macht den vorherigen sofort ungültig.
- Geheimnisse stehen nicht im Code, sondern in den Umgebungsvariablen des Servers.
- Vor jedem Release prüfen automatisierte Kontrollen, dass die Funktionen arbeiten und die Konfigurationen

stimmig sind.

7. Wenn etwas passiert

Verletzungen des Schutzes personenbezogener Daten werden dem Kunden **innerhalb von 48 Stunden**, nachdem sie uns bekannt geworden sind, mit den Informationen gemeldet, die zur Beurteilung einer Meldung an die Behörden nötig sind. Das Verfahren ist in Abschnitt 6 des Auftragsverarbeitungsvertrags (<https://work.omegasuiteapp.com/legal/dpa>) geregelt.

Wenn Sie eine Schwachstelle finden, schreiben Sie an **amministrazione@outlinedigital.it**. Wir verpflichten uns, innerhalb von 5 Geschäftstagen zu antworten und nicht gegen Personen vorzugehen, die in gutem Glauben melden, ohne auf fremde Daten zuzugreifen, ohne den Dienst zu beeinträchtigen und ohne das Problem vor seiner Behebung offenzulegen.

8. Was wir (noch) nicht tun

Eine Liste von Massnahmen ohne ihre Grenzen ist Werbung. Folgendes gibt es heute **nicht**, damit Sie es vorher wissen und nicht erst hinterher:

- **Zwei-Faktor-Authentifizierung:** nicht verfügbar. Verwenden Sie ein langes Passwort, das Sie nirgendwo sonst nutzen, und einen Passwort-Manager.
- **Verschlüsselung der gesamten Datenbank im Ruhezustand:** nicht aktiviert. Passwörter und Zugangsdaten verbundener Dienste sind geschützt; die übrigen Daten schützen Zugriffskontrolle und Systemisolation, nicht Verschlüsselung.
- **Zertifizierungen** (ISO/IEC 27001, SOC 2): keine. Wir beanspruchen keine Standards, für die wir nicht geprüft wurden.
- **Beschränkung nach IP-Adressen und ein für den Kunden einsehbares Anmeldeprotokoll pro Benutzer:** nicht verfügbar.
- **Sicherung von Dateien und Kopien an einem anderen Ort:** nicht vorhanden. Die Sicherungen umfassen die Datenbanken; sie liegen auf demselben Server, sind durch Dateirechte geschützt und nicht verschlüsselt, und an einem anderen Standort wird keine Kopie aufbewahrt. Die von Ihnen hochgeladenen Dateien — Anhänge, Dokumente — liegen auf dem Server und sind nicht Teil der Sicherungen: Bewahren Sie von Dateien, deren Verlust Sie sich nicht leisten können, eine eigene Kopie auf.
- **Getrennte Datenbank-Zugangsdaten je Arbeitsbereich:** nicht vorhanden. Jeder Arbeitsbereich hat seine eigene Datenbank, die Anwendung greift aber mit demselben Datenbankkonto auf alle zu.
- **Verschlüsselung der Kanal-Adressen:** nicht vorhanden. Die Adressen und Signaturgeheimnisse der Kanäle, die Sie für Benachrichtigungen verbinden (Slack, Microsoft Teams, Discord, Google Chat, Telegram, Webhooks), werden ohne zusätzliche Verschlüsselung in der Datenbank des Arbeitsbereichs gespeichert.

Sobald eine dieser Massnahmen umgesetzt ist, wandert sie in die obigen Abschnitte, und die Version dieses Dokuments wird erhöht.

9. Ihr Beitrag

Mindestens die Hälfte der Sicherheit einer Arbeitssoftware entscheidet sich ausserhalb der Software:

- verwenden Sie starke Passwörter und nicht dieselben wie bei anderen Diensten;
- legen Sie für jede Person einen eigenen Benutzer an: Gemeinsam genutzte Konten machen es unmöglich zu wissen, wer was getan hat;
- vergeben Sie nur die nötigsten Berechtigungen und **entfernen Sie Personen sofort**, wenn sie ausscheiden;
- erzeugen Sie öffentliche Links neu, wenn Sie vermuten, dass sie weitergegeben wurden, und widerrufen Sie API-Schlüssel, die Sie nicht mehr verwenden;
- halten Sie die Geräte, mit denen Sie sich anmelden, aktuell;
- exportieren Sie regelmässig die Daten, deren Verlust Sie sich nicht leisten könnten.

Der aktuelle vollständige Text ist jederzeit unter <https://work.omegasuiteapp.com/legal/security?lang=de> abrufbar. Bei Fragen: amministrazione@outlinedigital.it.