DiliTrust

Sicherheit bei DiliTrust

Die Sicherheit Ihrer Daten hat für uns oberste Priorität

Unsere Kunden vertrauen uns ihre strategisch wichtigsten Informationen an – und wir schulden ihnen ein Höchstmaß an Schutz. Der Schutz Ihrer Daten ist entscheidend für den langfristigen Erfolg Ihres Unternehmens. Datenschutzverletzungen, die Nichteinhaltung von Vorschriften wie der DSGVO oder die betrieblichen und finanziellen Auswirkungen von Serviceunterbrechungen können jedem Unternehmen ernsthaften Schaden zufügen.

Die Sicherheit Ihrer Daten ist für Sie – und noch mehr für uns – von entscheidender Bedeutung.

Ob es um die Abwehr externer Angriffe, die Verhinderung interner Schwachstellen, die Vermeidung von Datenlecks oder die Minimierung menschlichen Versagens geht – Sicherheit ist für unsere Kunden von grundlegender Bedeutung und in jeden Aspekt unserer Dienstleistung eingebettet. Unser gesamtes Unternehmen hat sich einem Ziel verschrieben: die Bereitstellung eines Höchstmaßes an Datenschutz.

Eine Kultur, in der Sicherheit an erster Stelle steht

DiliTrust ist nach ISO 27001:2017, ISO 27701:2019 und SOC 2 zertifiziert – international anerkannte Standards, die Best Practices für das Informationssicherheitsmanagement und den Schutz personenbezogener Daten definieren. Diese Zertifizierungen gehen weit über technische und sicherheitstechnische Schutzmaßnahmen hinaus; sie umfassen auch Vertraulichkeit, Data Governance und die Compliance. Alle unsere Mitarbeiter sind so geschult, dass sie diese Standards auf allen Ebenen unserer Tätigkeit einhalten.

Infrastruktur

Server-Standort

Unsere Server erfüllen die höchsten Sicherheitsstandards und befinden sich **ausschließlich in der Region unserer Kunden:** in Europa für EU-Kunden, in Kanada für kanadische Kunden, im Nahen Osten, in Afrika oder Marokko für MEA und in den USA für amerikanische Kunden usw.

Die gehosteten Daten werden niemals an Dritte weitergegeben und unterliegen in keiner Weise extraterritorialen Gesetzen, so dass unsere Kunden jederzeit die volle Kontrolle über ihre sensiblen Informationen behalten.

Physische Sicherheit

Ein ebenso wichtiger Aspekt des Datenschutzes ist die physische Sicherheit. Der Zugang zu den Rechenzentren wird durch Ausweissysteme, Videoüberwachung und Personal vor Ort, das rund um die Uhr zur Verfügung steht, strengstens kontrolliert.

Die Einrichtungen sind mit Rauchmeldesystemen und vollständig redundanter Stromversorgung ausgestattet, einschließlich Notstromgeneratoren mit einer anfänglichen Autonomie von 48 Stunden. Darüber hinaus gibt es doppelte Netzwerkverbindungen, **um die Abhängigkeit** von einem einzigen Internetanbieter **zu vermeiden.**

Die gesamte Infrastruktur ist gegen Überschwemmungen, Feuer und andere Umweltrisiken geschützt, um ein Höchstmaß an Widerstandsfähigkeit und Kontinuität zu gewährleisten.

Hochgradig sicheres Hosting

Um den Datenschutz kontinuierlich zu stärken und die Vertraulichkeit aller Informationen zu gewährleisten, werden alle Systeme und Daten von DiliTrust auf Servern gehostet, die die höchsten internationalen Zertifizierungen für Informationssicherheit besitzen.

Unsere **Hosting-Infrastruktur ist nach ISO/IEC 27001 zertifiziert** – ein weltweit anerkannter Standard, der die Implementierung eines Informationssicherheits-Managementsystems (ISMS) zum Schutz von Daten bestätigt.

ISO 27001 definiert auch eine umfassende Reihe von Kontrollen, die sicherstellen sollen, dass unsere Systeme unseren Kunden stets ein Höchstmaß an Sicherheit bieten.

24/7 Überwachung und Kontrolle

Unsere Systeme werden rund um die Uhr überwacht, um alle Angriffsversuche oder technischen Vorfälle in Echtzeit zu erkennen und darauf zu reagieren. Dies beinhaltet:

- Kontinuierliche Überwachung von Hardware-Metriken wie RAM-Nutzung, CPU-Last und Speicherkapazität sowie der Anwendungsleistung;
- Automatische Warnmeldungen, die bei der Erkennung verdächtiger Aktivitäten ausgelöst werden;
- Hochentwickelte Sicherheitsschichten, einschließlich EDR, Firewalls, Intrusion Detection Systems (IDS), Anti-Flood (DDoS)-Mechanismen und Schutz vor Brute-Force-Angriffen.

Alle Server sind mit redundanten Festplatten und Netzzugängen ausgestattet und verfügen über tägliche Sicherungssysteme, um die Datenintegrität und die Betriebskontinuität zu gewährleisten.

Backups

Vollständige Systemsicherungen werden täglich durchgeführt und an einem sekundären Standort gespeichert, der geografisch von den primären Servern getrennt ist, jedoch denselben Sicherheitsstandards unterliegt und sich im selben Land befindet, wodurch die Einhaltung derselben Rechtsprechung gewährleistet ist.

Die Backups werden **sieben Tage lang aufbewahrt und dann endgültig gelöscht**, ohne dass eine Wiederherstellung möglich ist. Zum Beispiel überschreibt die Sicherung vom Montag automatisch die Datei vom vorherigen Montag.

Eine voll funktionsfähige sekundäre Umgebung steht zur Wiederherstellung des Dienstes im Falle eines größeren Vorfalls zur Verfügung, vorbehaltlich der üblichen DNS-Verbreitungszeiten.

Verschlüsselung

“DATA-AT-REST”: AES 256

Alle vertraulichen Daten im Ruhezustand werden mit AES (Advanced Encryption Standard, Rijndael) mit einem 256-Bit-Schlüssel verschlüsselt – **dem höchsten derzeit verfügbaren Verschlüsselungsstandard.**

Dies gilt sowohl für die auf Servern gespeicherten Daten als auch für die lokal auf mobilen Geräten gespeicherten Daten.

DATA-IN-MOTION »: HTTPS 256 BITS

Alle Daten, die unsere Server erreichen oder verlassen, werden systematisch mit TLS (Transport Layer Security, Version 1.2 und höher) verschlüsselt, wobei eine 256-Bit-Verschlüsselung Standard ist. **Unverschlüsselter Datenverkehr ist strengstens untersagt.**

Es werden nur moderne, sichere Browser unterstützt, darunter Edge, Firefox, Chrome und Safari, sowie die nativen mobilen Anwendungen von DiliTrust. Veralteten oder unsicheren Browsern (wie Internet Explorer 8) wird der Zugang verweigert.

Hardware Security Module (HSM)

Ein HSM ist ein digitaler Tresor - ein spezieller kryptografischer Prozessor, der für die sichere Verwaltung von Verschlüsselungsschlüsseln während ihres gesamten Lebenszyklus konzipiert ist.

Das HSM dient als vertrauenswürdige Grundlage für unsere kryptografische Infrastruktur. Es erzeugt, speichert und verwaltet Verschlüsselungsschlüssel sicher in einer **manipulationssicheren Serverumgebung.**

Mit dieser Technologie sind wir in der Lage, das höchste derzeit verfügbare Niveau an Verschlüsselung und Datenschutz zu bieten, so dass unsere Kunden von branchenführenden Sicherheitsstandards profitieren.

Bring your Own Key (BYOK)

Wir bieten unseren Kunden die Möglichkeit, ihr eigenes Hardware-Sicherheitsmodul (HSM) zu hosten, **das dem PKCS#11-Standard entspricht,** um ihre Verschlüsselungsschlüssel zu schützen.

Alle Kundendaten werden mit ihrem eigenen Schlüssel verschlüsselt, der sicher im eigenen HSM und nicht in der Infrastruktur des Anbieters gespeichert und verwaltet wird.

Dieses Modell gewährleistet, dass die Kunden die volle Kontrolle über ihre Verschlüsselungsschlüssel behalten und stärkt die Datensouveränität und die Einhaltung interner Sicherheitsrichtlinien.

Authentication

Secure Passwords

Jeder Benutzer wird durch einen eindeutigen Benutzernamen und ein Passwort identifiziert. Die Benutzer müssen ihre eigenen sicheren Passwörter erstellen – keine Passwörter werden jemals per E-Mail verschickt oder jemandem angezeigt. Die Passwörter werden in einem Hash-Format unter Verwendung einer Einwegverschlüsselung (Injektionsverschlüsselung) gespeichert.

Die Passwortanforderungen umfassen:

- Mindestens 10 Zeichen
- Mindestens drei verschiedene Zeichentypen (Kleinbuchstaben, Großbuchstaben, Ziffern oder Sonderzeichen)

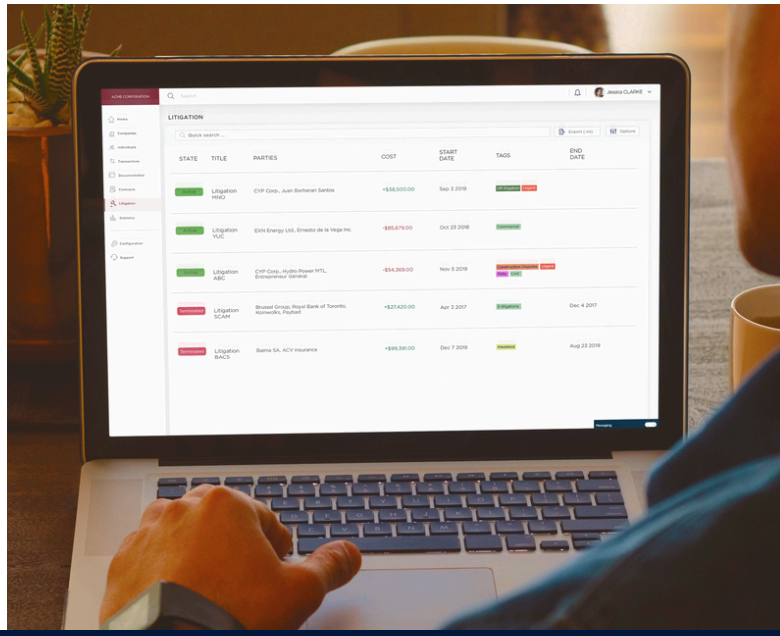
Die Erstellung und Wiederherstellung von Passwörtern erfolgt über einen sicheren, einmalig verwendbaren Link, der per E-Mail versandt wird. Dieser Link verfällt nach 24 Stunden oder nach der ersten Nutzung.

Jede Anfrage an die Server wird authentifiziert, um die Identität des Benutzers und seine Berechtigung zur Durchführung der angeforderten Aktion zu überprüfen. **Die Anfrage wird nur ausgeführt, wenn alle Überprüfungen erfolgreich abgeschlossen wurden.**

Zwei-Faktor-Authentifizierung (TFA)

Die Zwei-Faktor-Authentifizierung (TFA) bietet eine zusätzliche Sicherheitsebene für den Benutzerzugang zur Anwendung. Nach der Eingabe des Benutzernamens und des Passworts erhält der Benutzer einen einmaligen Code per SMS, der eingegeben werden muss, um den Anmeldevorgang abzuschließen.

Jeder Code ist einmalig und nur für einen einzigen Anmeldeversuch gültig, so dass der Zugang sowohl sicher als auch nachvollziehbar ist.



Künstliche Intelligenz

100% proprietäre KI

Bei DiliTrust basiert unser Ansatz für künstliche Intelligenz auf Ethik, Verantwortung und Transparenz. **Alle unsere KI-Technologien werden intern entwickelt und vollständig kontrolliert,** so dass wir die vollständige Kontrolle über ihr Design, ihr Training und ihren Betrieb haben - ohne Beteiligung oder Datenaustausch mit Dritten.

Jede KI-gestützte Funktion wird von Menschen überwacht, um sicherzustellen, dass die Ergebnisse zuverlässig sind, mit den Geschäftsanforderungen übereinstimmen und den höchsten Leistungs- und Sicherheitsstandards entsprechen.

Wir sind fest entschlossen, transparente und erklärbare Ergebnisse zu liefern. Unsere Praktiken stehen in **vollem Einklang mit dem Europäischen AI ACT**, das Fairness, Verantwortlichkeit und Nichtdiskriminierung in den Vordergrund stellt.

KI-Interoperabilität

Unsere Technologie ist offen und flexibel gestaltet und ermöglicht eine nahtlose Integration mit kundeneigenen großen Sprachmodellen (LLMs).

Durch **sichere API-Konnektivität** und modulare KI-Frameworks ermöglichen wir es Unternehmen, ihre eigenen KI-Modelle zu nutzen und gleichzeitig von der robusten und sicheren Infrastruktur von DiliTrust zu profitieren.

End-to-End Verschlüsselung

Bei DiliTrust hat die Datensicherheit höchste Priorität. Wir implementieren eine End-to-End-Verschlüsselung mit AES-256 für Daten im Ruhezustand und TLS 1.2+ für alle Daten bei der Übertragung, um ein hohes Maß an Vertraulichkeit und Integrität in jeder Phase zu gewährleisten – ob bei der Vertragsanalyse, der Dokumentenzusammenfassung oder anderen fortschrittlichen Verarbeitungsprozessen.

Es werden niemals Kundendaten zum Trainieren globaler Modelle verwendet, und die gesamte KI-Verarbeitung bleibt streng auf das sichere DiliTrust-Ökosystem beschränkt.

Unsere Systeme folgen einem „Security-first"-Ansatz, der vollständig mit der DSGVO und neuen internationalen Standards konform ist. Das Ergebnis: ethische, vertrauenswürdige und vollständig kontrollierte KI.

Datenschutz

Wir verpflichten uns, Ihre Daten zu schützen und gleichzeitig die Einhaltung der geltenden Vorschriften zu gewährleisten - und damit Vertrauen, Verantwortlichkeit und ethische Verantwortung zu fördern.

- **Reduzierung von Verzerrungen:** Unsere KI-Modelle werden strengen Tests und einer kontinuierlichen Überwachung unterzogen, um potenzielle Verzerrungen zu erkennen und zu korrigieren und so faire und nicht diskriminierende Ergebnisse zu gewährleisten.
- **Transparenz:** Wir bemühen uns, unsere Prozesse verständlich zu machen, indem wir eine klare Dokumentation und ausführliche Erklärungen dazu liefern, wie unsere Systeme funktionieren und wie Entscheidungen getroffen werden**.**
- **Menschliche Kontrolle:** Bei DiliTrust soll KI das menschliche Urteilsvermögen unterstützen – nicht ersetzen. Alle kritischen Entscheidungen werden standardmäßig von Menschen überprüft.

Commitments

ISO 27001 & ISO 27701 zertifiziert

Die gesamte DiliTrust-Suite ist ISO-zertifiziert – der führende internationale Standard für Informationssicherheits-Management-Systeme (ISMS). Diese Zertifizierung gewährleistet, dass strenge Prozesse zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit aller Daten vorhanden sind.

Unsere ISO 27701-Zertifizierung stärkt dieses Engagement noch, indem sie diese Standards auf die Verwaltung personenbezogener Daten ausweitet und damit internationale Vorschriften wie die GDPR erfüllt.

Diese Zertifizierungen bestätigen, dass unsere Infrastruktur, Verfahren und Kontrollen die höchsten Standards für Informationssicherheit und den Schutz personenbezogener Daten erfüllen.

SOC 2 type II Compliant

DiliTrust erfüllt auch den SOC 2 Type II Standard - ein strenges, vom AICPA entwickeltes Audit-Framework, das die Effektivität der Datenschutzmaßnahmen eines Service Providers im Laufe der Zeit bewertet.

Diese Konformität spiegelt unser kontinuierliches Engagement für betriebliche Transparenz, Systemzuverlässigkeit und starke interne Kontrollen wider – insbesondere in den Bereichen Sicherheit, Verfügbarkeit und Vertraulichkeit.

Das SOC-2-Audit gibt unseren Kunden und Partnern die Gewissheit, dass unsere Dienstleistungen nicht nur von vornherein sicher sind, sondern auch kontinuierlich überwacht und verbessert werden, um auf neue Risiken zu reagieren.

Compliance mit den höchsten Standards

Unsere künstliche Intelligenz arbeitet innerhalb eines strengen ethischen Rahmens, der Fairness, Transparenz und die Achtung der Nutzerrechte gewährleistet.

- **DSGVO-Einhaltung:** Unsere Systeme und Prozesse sind so konzipiert, dass sie die strengsten europäischen Datenschutzstandards erfüllen und sicherstellen, dass personenbezogene Daten rechtmäßig und fair verarbeitet und nicht an Dritte weitergegeben werden.
- **Datenschutz durch Design:** In jeder Phase der KI-Entwicklung und Bereitstellung werden strenge Datenschutzvorkehrungen getroffen, um Risiken zu minimieren und die vollständige Einhaltung aller geltenden Vorschriften zu gewährleisten.

Audits

Um ein Höchstmaß an Sicherheit zu gewährleisten, setzen wir drei Ebenen redundanter Kontrollen ein: interne Audits, wöchentliche automatisierte Audits und mindestens ein jährliches externes Audit, das von unabhängigen Experten durchgeführt wird.

Wenn eine Sicherheitslücke festgestellt wird, wird sie unverzüglich angegangen und behoben. Bewährte Verfahren und Audit-Empfehlungen werden systematisch angewandt, um unsere Infrastruktur und Prozesse zu stärken.

Interne Audits

DiliTrust setzt **strenge interne Sicherheitsverfahren** durch, die in jede Phase der Entwicklung und Bereitstellung integriert sind:

- **Sicherheit durch Design:** Die Entwicklungsteams werden in Intrusionstechniken und sicheren Kodierungspraktiken geschult, um Schwachstellen proaktiv zu verhindern.
- **Code-Reviews und Pre-Release-Tests:** Alle neuen Funktionen werden vor der Freigabe für die Produktion internen Code-Reviews und Sicherheitstests unterzogen.
- **Interne Sicherheitstests:** Eine Reihe von Audit-Tools - hauptsächlich aus der Kali-Linux-Distribution - werden für regelmäßige interne Sicherheitstests eingesetzt.

Automatisierte Audits

Unsere Systeme werden von einem externen Anbieter gesichert.
Der Dienst wird **wöchentlich intensiven Sicherheitsscans unterzogen**, sowohl auf Serverebene (Firewall-Konfiguration, Ports, aktuelle Softwareversionen, SSL-Konfiguration usw.) als auch auf Anwendungsebene (XSS, SQL-Injection, Session-Hijacking usw.).

Externe Audits durch unabhängige Experten

Mindestens einmal im Jahr führen wir ein umfassendes Sicherheitsaudit durch. Dieses wird von einem unabhängigen Unternehmen durchgeführt, das auf Cybersicherheit spezialisiert ist. Diese Audits umfassen manuelle (nicht automatisierte) Penetrationstests, die von erfahrenen Fachleuten durchgeführt werden.

Nach jeder Prüfung wird ein detaillierter Sicherheitsbericht erstellt. Alle festgestellten Schwachstellen werden umgehend behoben und alle empfohlenen Verbesserungen werden so schnell wie möglich umgesetzt.

"Sicherheit ist unsere DNA"

Nadim Baklouti
CEO, DiliTrust

Für weitere Informationen über DiliTrust besuchen Sie bitte **www.dilitrust.com**

DiliTrust GmbH
Claudius-Keller-Straße 3b
81669 München
hello@dilitrust.com

DILITRUST