DILITRUST

Security at DiliTrust

Your Data Security is our Top Priority

Our clients entrust us with their most strategic information — and we owe them the highest level of protection. Safeguarding your data is essential to the long-term success of your organization. Data breaches, non-compliance with regulations such as the GDPR, or the operational and financial impact of service disruptions can cause serious harm to any business.

Your data security is critical to you — and even more so to us.

Whether it's defending against external attacks, preventing internal vulnerabilities, avoiding data leaks, or minimizing human error, security is fundamental to our clients and embedded in every aspect of our service. Our entire organization is committed to one goal: delivering the highest level of data protection.

A Security-First Culture

DiliTrust is ISO 27001:2017, ISO 27701:2019, and SOC 2 certified — internationally recognized standards that define best practices for information security management and the protection of personal data. These certifications go far beyond technical and security safeguards; they also encompass confidentiality, data governance, and regulatory compliance. All our employees are trained to uphold these standards at every level of our operations.

Infrastructure

Server Location

Our servers meet the highest security standards and are **located exclusively in our client region**: in Europe for UE clients, Canada for Canadian, Canada or Europe for Latin America, in the Middle East, Africa, or Morocco for MEA and in the U.S. for American clients.

Hosted data is never shared with third parties and is in no way subject to extraterritorial laws, ensuring our clients maintain full control over their sensitive information at all times.

Physical Security

An equally critical aspect of data protection is physical security. Access to the data centers is tightly controlled through badge systems, video surveillance, and on-site personnel available 24/7.

The facilities are equipped with smoke detection systems and fully redundant power supplies, including backup generators with an initial autonomy of 48 hours. In addition, dual network connections are in place **to prevent dependency** on a single internet service provider.

All infrastructure is protected against flooding, fire, and other environmental risks to ensure maximum resilience and continuity.

Highly Secure Hosting

To continuously strengthen data protection and ensure the confidentiality of all information, all DiliTrust systems and data are hosted on servers that hold the highest international certifications in information security.

Our **hosting infrastructure is ISO/IEC 27001 certified** — a globally recognized standard that confirms the implementation of an Information Security Management System (ISMS) to safeguard data.

ISO 27001 also defines a comprehensive set of controls designed to ensure our systems consistently deliver the highest level of security to our clients.

24/7 Monitoring and Control

Our systems are monitored around the clock to detect and respond to any attempted attacks or technical incidents in real time. This includes:

- Continuous monitoring of hardware metrics such as RAM usage, CPU load, and storage capacity, as well as application performance;
- Automatic alerts triggered upon detection of suspicious activity;
- Advanced security layers including EDR, firewalls, intrusion detection systems (IDS), anti-flood (DDoS) mechanisms, and brute-force attack protection.

All servers are equipped with redundant disks and network access, along with daily backup systems to ensure data integrity and operational continuity.

Backups

Complete system backups are performed daily and stored at a secondary location that is geographically separate from the primary servers, yet subject to the same security standards and located within the same country — ensuring compliance with the same legal jurisdiction.

Backups are retained on a **rolling seven-day basis and are then permanently deleted**, with no possibility of recovery. For example, Monday's backup automatically overwrites the previous Monday's file.

A fully operational secondary environment is available to restore service in case of a major incident, subject to standard DNS propagation times.

Encryption

“DATA-AT-REST”: AES 256

All confidential data at rest is encrypted using AES (Advanced Encryption Standard, Rijndael) with a 256-bit key — **the highest encryption standard currently available**.

This applies both to data stored on servers and to data stored locally on mobile devices.

« DATA-IN-MOTION »: HTTPS 256 BITS

All data in motion — whether entering or leaving our servers — is **systematically encrypted using TLS** (Transport Layer Security, version 1.2 and above), with 256-bit encryption as the standard. Unencrypted traffic is strictly prohibited.

Only modern, secure browsers are supported, including Edge, Firefox, Chrome, and Safari, as well as DiliTrust’s native mobile applications. Access is denied to outdated or insecure browsers (such as Internet Explorer 8).

Hardware Security Module (HSM)

An HSM is a digital safe — a dedicated cryptographic processor designed to securely manage encryption keys throughout their entire lifecycle.

The HSM serves as a trusted foundation for our cryptographic infrastructure, securely generating, storing, and handling encryption keys **within a tamper-resistant server environment.**

This technology enables us to deliver the highest levels of encryption and data protection currently available, ensuring our clients benefit from industry-leading security standards.

Bring your Own Key (BYOK)

We offer our clients the option to host their own Hardware Security Module (HSM), **compliant with the PKCS#11** standard, to safeguard their encryption keys.

All client data is encrypted using their own key — securely stored and managed within their own HSM rather than within the provider’s infrastructure.

This model ensures that clients retain full control over their encryption keys and reinforces data sovereignty and compliance with internal security policies.

Authentication

Secure Passwords

Each user is identified by a unique username and password. Users are required to create their own secure passwords — no passwords are ever sent by email or displayed at any time to anyone. Passwords are stored in a hashed format using one-way (injective) encryption.

Password requirements include:

- A minimum of 10 characters
- At least three different character types (lowercase, uppercase, digits, or special characters)

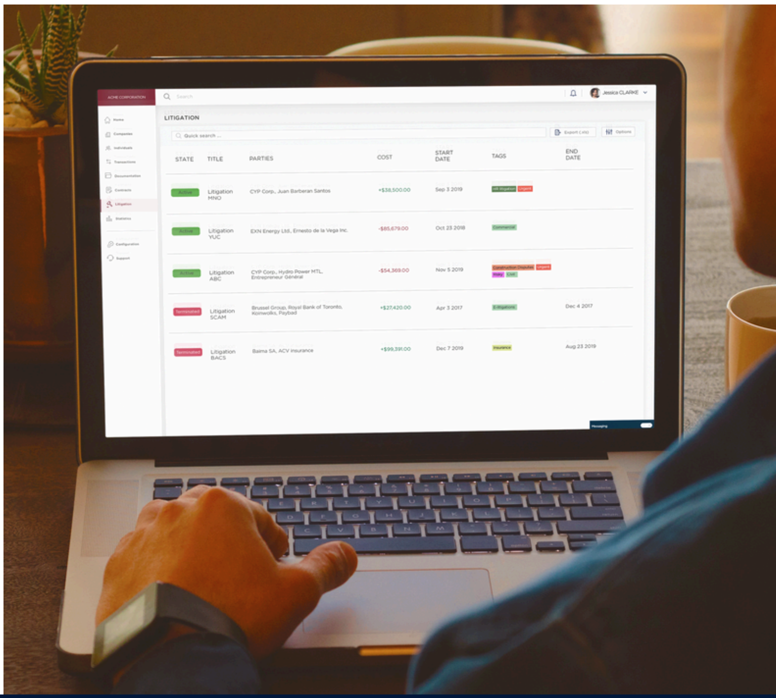
Password creation and recovery is handled through a secure, single-use access link sent by email. This link expires after 24 hours or after first use.

Every request to the servers is authenticated to verify the user’s identity and their authorization to perform the requested action. The request is executed **only if all verification checks are successfully validated.**

Two Factor Authentication (TFA)

Two-Factor Authentication (TFA) provides an additional layer of security for user access to the application. After entering their username and password, **the user receives a one-time code via SMS**, which must be entered to complete the login process.

Each code is unique and valid for a single login attempt, ensuring that access is both secure and traceable.



Artificial Intelligence

100% Proprietary AI

At DiliTrust, our approach to artificial intelligence is grounded in ethics, responsibility, and transparency. All our AI technologies are **developed and fully controlled in-house**, giving us complete oversight of their design, training, and operation — with no involvement or data sharing with third parties.

Every AI-powered feature includes human oversight to ensure outcomes are reliable, aligned with business needs, and meet the highest standards of performance and security.

We are firmly committed to delivering transparent and explainable results. Our practices fully **comply with the European AI Act**, prioritizing fairness, accountability, and non-discrimination.

AI Interoperability

Our technology is designed to be open and flexible, enabling seamless integration with clients' proprietary large language models (LLMs).

Through **secure API** connectivity and modular AI frameworks, we empower organizations to leverage their own AI models while benefiting from DiliTrust's robust and secure infrastructure.

End-to-End Encryption

At DiliTrust, data security is a top priority. We implement end-to-end encryption using AES-256 for data at rest and TLS 1.2+ for all data in transit, ensuring a high level of confidentiality and integrity at every stage — whether it's contract analysis, document summarization, or other advanced processing.

No client data is ever used to train global models, and all AI processing remains strictly confined within the secure DiliTrust ecosystem.

Our systems follow a "security-first" approach, fully compliant with the GDPR and emerging international standards. The result: ethical, trustworthy, and fully controlled AI.

Data Protection

We are committed to safeguarding your data while ensuring full compliance with applicable regulations — fostering trust, accountability, and ethical responsibility.

- **Bias Reduction**: Our AI models undergo rigorous testing and continuous monitoring to detect and correct potential biases, ensuring fair and non-discriminatory outcomes.
- **Transparency**: We strive to make our processes understandable, providing clear documentation and detailed explanations of how our systems function and how decisions are made.
- **Human Oversight**: At DiliTrust, AI is designed to support — not replace — human judgment. All critical decisions are subject to human validation by default.

Commitments

ISO 27001 & ISO 27701 Certified

The entire DiliTrust suite is ISO certified — the leading international standard for Information Security Management Systems (ISMS). This certification ensures that rigorous processes are in place to protect the confidentiality, integrity, and availability of all data.

Our ISO 27701 certification further strengthens this commitment by extending these standards to the management of personal data, in full alignment with international regulations such as the GDPR.

These certifications confirm that our infrastructure, procedures, and controls meet the highest standards for information security and personal data protection.

SOC 2 type II Compliant

DiliTrust is also compliant with the SOC 2 Type II standard — a rigorous audit framework developed by the AICPA that assesses the effectiveness of a **service provider's data protection measures over time**.

This compliance reflects our ongoing commitment to operational transparency, system reliability, and strong internal controls — particularly in the areas of security, availability, and confidentiality.

The SOC 2 audit provides our clients and partners with assurance that our services are not only secure by design, but also subject to continuous monitoring and improvement in response to emerging risks.

CERTIFIED
ISO 27001

CERTIFIED
ISO 27701

COMPLIANT
AICPA SOC 2

GDPR

Compliance with the Highest Standards

Our artificial intelligence operates within a strict ethical framework, ensuring fairness, transparency, and respect for user rights.

- **GDPR Compliance**: Our systems and processes are designed to meet the most stringent European data protection standards, ensuring that personal data is processed lawfully, fairly, and without any sharing with third parties.
- **Privacy by Design**: Every stage of AI development and deployment incorporates strong privacy safeguards, minimizing risks and ensuring full compliance with all applicable regulations.

Audits

To ensure the highest level of security, we implement three layers of redundant controls: internal audits, weekly automated audits, and at least one annual external audit conducted by independent experts.

If a security vulnerability is identified, it is addressed and resolved without delay. Best practices and audit recommendations are applied systematically to strengthen our infrastructure and processes.

Internal Audits

DiliTrust enforces **strict internal security procedures**, integrated into every stage of development and deployment:

- **Security by Design:** Development teams are trained in intrusion techniques and secure coding practices to proactively prevent vulnerabilities.
- **Code Reviews and Pre-Release Testing**: All new features undergo internal code reviews and security testing before being released to production.
- **Internal Security Testing**: A range of audit tools — primarily from the Kali Linux distribution — are used to conduct regular internal security assessments.

Automated Audits

Our systems are secured by an external provider. The service undergoes **intensive weekly security scans** at the server level (firewall configuration, ports, up-to-date software versions, SSL configuration, etc.) as well as at the application level (XSS, SQL injection, session hijacking, etc.).

External Audits by Independent Experts

At least once a year, we conduct a comprehensive security audit performed by an independent third-party firm specializing in cybersecurity. These audits include manual (non-automated) penetration testing carried out by experienced professionals.

A detailed security report is produced following each assessment. Any identified vulnerabilities are addressed promptly, and all recommended improvements are implemented as quickly as possible.

"Security is our DNA"

Nadim Baklouti
CEO, DiliTrust

For more information on DiliTrust, please visit **www.dilitrust.com**

DiliTrust - Tour OPUS 12 - 77 Esplanade du Général de Gaulle
92081 Paris La Défense Cedex
hello@dilitrust.com