Privacy Rooted in Engineering

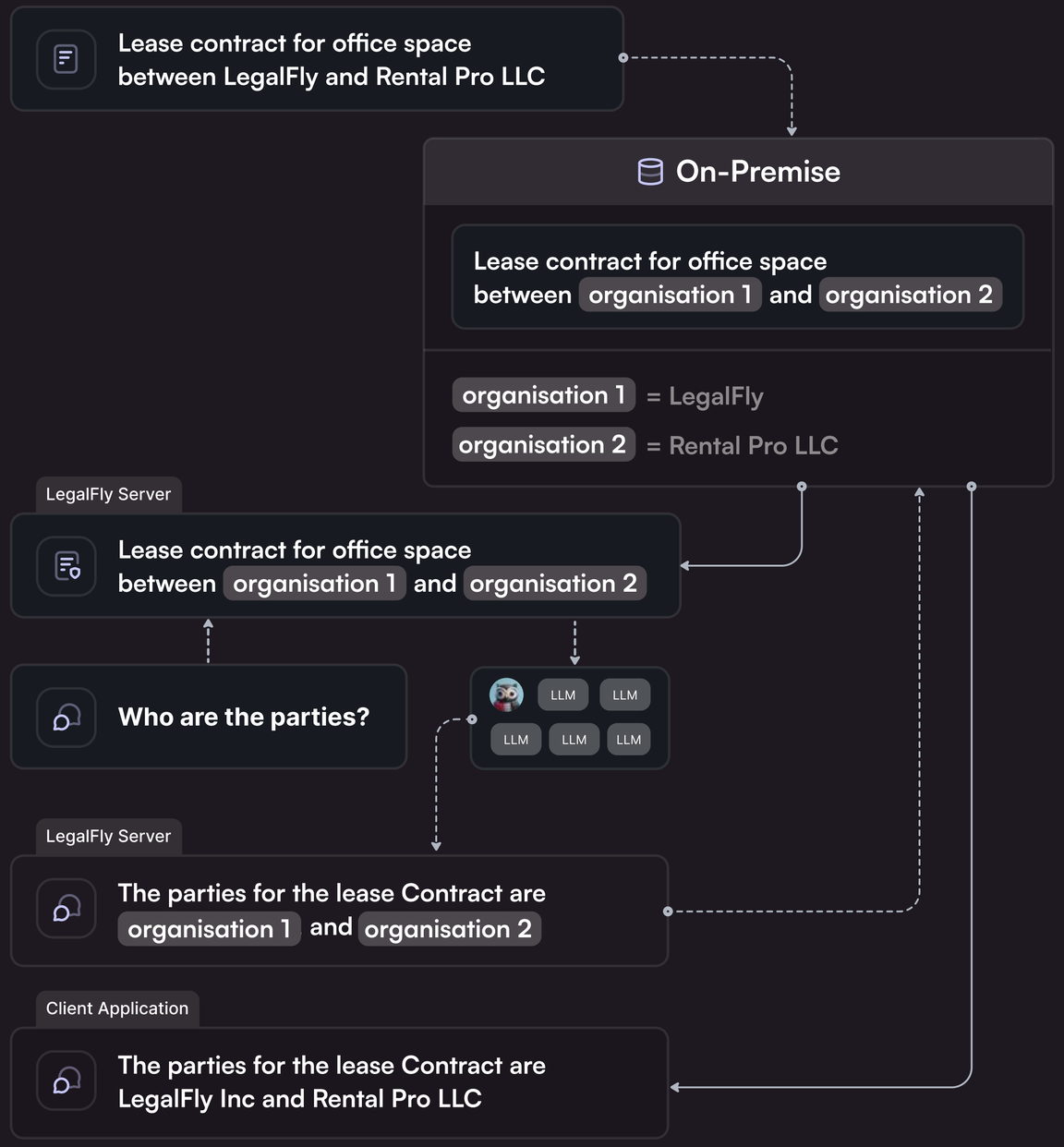
PII never hits the LegalFly server

Before ever hitting the LegalFly servers, **all user-generated input is sent to a Dedicated On-Premise Environment**.
The environment has **three functionalities**:

- Running LegalFly's **anonymisation AI model**
- Storing the **anonymised entities**
- **Access Control** for the Client Application

Direct Client To On Premise Connectivity

All Personal Identifiable Information (PII) is processed and stored on-premise. The LegalFly Server and public models only have access to anonymised data. The Client Application requests the original entities when visualisation is required.



Security Compliance

Understanding the industry's cautious approach to data sharing with LLMs, LegalFly has designed a security infrastructure that stands unmatched.

Our solution is tailored for the protection of confidential legal data and benefits from the unparalleled security expertise of some of the **leading cybersecurity experts in Europe and the United States**.

SOC 2 Type 2

ISO 27001 Compliant

GDPR Compliant

Security Whitepaper

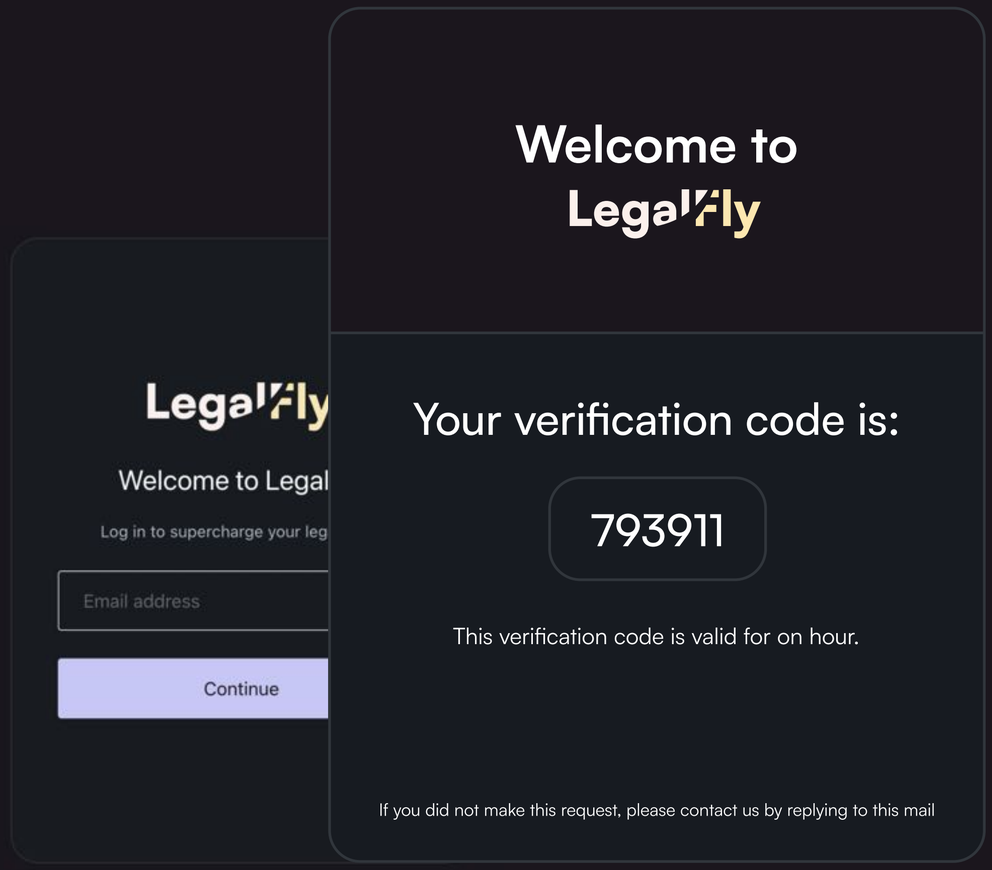
Frictionless authentication & Single Sign On

Passwordless Authentication

- Six-digit code sent via e-mail for instant sign-in
- Short-lived and single-use
- Increases security by eliminating the use of passwords

Enterprise-grade Single Sign-On (SSO)

- Support for SAML 2.0 and OIDC identity providers
- Seamless integration with most customer directories (e.g Azure AD)
- Supports Enterprise-grade security needs with MFA and audit logs



We're Built to Secure your Most Sensitive data

At-Rest Encryption

All stored data, including databases and cloud storage, is securely encrypted at rest utilizing AES-256 encryption. This includes **both disk-level and object-level encryption**.

In-Transport Encryption

LegalFly enforces transport layer encryption of at least TLS 1.2 (**HTTPS**) across all infrastructure, including APIs and microservices.

All internal communications are secured via a **WireGuard VPN**, providing an additional layer of security as a **defense-in-depth measure**.

Secrets Management

Our secrets management approach aligns with the stringent **key management protocols** recommended by frameworks like NIST and adheres to ISO/IEC 27001 standards.

All secrets and encryption keys are stored in dedicated **key management vaults** and are subject to systematic rotation to prevent unauthorized access and enhance security integrity.

World class In-house Security Operations

The LegalFly security team has deployed world class best practices and tools to maintain security on all levels: across our company, within the infrastructure, and in the product and platform itself.

Corporate Security

Our corporate security framework is built on strict **least privilege principles** and robust data protection policies to safeguard sensitive information and ensure **regulatory compliance**. All LegalFly employees undergo annual security training.

Infrastructure Security

Our infrastructure security is structured around a **defense-in-depth** approach, incorporating multiple layers of protection including encryption and VPNs. We implement **network segmentation** to isolate and protect different environments effectively.

Regular risk assessments are carried out to identify and mitigate any potential risks, ensuring the security, availability, and privacy of the Legalfly platform.

Product Security

Each release undergoes rigorous **security testing** by our internal security team before deployment, ensuring that all features meet our standards for security.

Additionally, regular **third-party security audits** are conducted, allowing us to identify and address any vulnerabilities and ensuring our products continue to protect user data effectively.