Sympa

Sympa's commitment to

data security

Protecting your data is our top priority. We've put in place strong security measures to ensure your information is safeguarded at every step. From compliance with global standards to recovery protocols, we offer comprehensive protection to keep your data secure.

Our industry-leading certifications

When choosing an HR system, don't rely on promises — choose a solution that backs up its security claims with globally recognised certifications.

- **ISO 27001:2022 Certified:** Demonstrating a long-standing commitment to information security since 2014.
- **ISO 9001:2015 Certified:** Ensuring high standards in quality management across all processes.

Compliance with GDPR and NIS2

We ensure full compliance with **GDPR** regulations, offering transparency and control over your personal data. In alignment with the **NIS2 Directive**, we are in the process of enhancing the security of network and information systems across the EU.

Ensuring your data stays secure and within the EU

We implement a strong encryption policy and mechanism to prevent any unauthorised access to customers' personal data. Whether your data is in transit or at rest, it's encrypted to ensure full protection at every stage.

- Sympa creates, holds, and controls all encryption keys to customers' personal data under the BYOK (Bring Your Own Key) model. **Microsoft does not have access to these keys.**
- Encryption keys for personal data stored in Sympa HR databases are managed by Sympa in FIPS 140-2 certified key vaults. **Microsoft does not have access to these keys.**
- The hosting provider (Microsoft) or governmental authorities cannot access the personal data or the encryption keys, as Sympa control them using BYOK. **"With Key Vault, Microsoft doesn't see or extract your keys."**
- Personal data stored in Microsoft Azure is configured to remain within **Microsoft's EU Data Boundary**, meaning all processing is conducted within the EU/EEA.

Our backup and recovery protocols

We maintain comprehensive protocols to ensure your data is recoverable in the case that there is a disruption:

- **Regular Backups:** Periodic backups ensure that your data is always available and can be fully restored if needed.
- **Disaster Recovery Plan:** Our thorough disaster recovery protocols ensure continuity, even in the event of a system failure.

Why we use Microsoft Azure

We partner with Microsoft Azure for its unmatched security, compliance, and scalability. Azure's EU Data Boundary ensures all data is processed and stored within the EU, fully aligning with GDPR.

Azure provides top-tier protection, including FIPS 140-2 compliant encryption, 24/7 threat monitoring, and AES 256 encryption at rest. With the Bring Your Own Key (BYOK) model, you maintain full control of encryption keys, ensuring your data is always secure.

In short, Azure offers the security, reliability, and global infrastructure that local providers can't match.

How we stay ahead of security threats

We continuously monitor and test our systems to stay ahead of potential threats:

- **Quarterly Security Audits and Penetration Testing:** Every three months, we perform thorough penetration testing and security audits through a **trusted third-party vendor** to simulate real-world attacks and identify potential vulnerabilities. This proactive approach ensures that any weaknesses are addressed before they can be exploited.
- **24/7 Security Operations Center (SOC) -service:** Our cybersecurity experts and cloud providers monitor our systems around the clock, identifying and responding to threats in real time.
- **Advanced Network Security:** We use a web application firewall (WAF) and other advanced protocols to prevent unauthorised access.

How we build secure software

Security is a key component of our robust and secure software development lifecycle (SDLC), ensuring our platform is resilient against any potential threats:

- **Security and Data Protection Training:** Our Engineering gets periodical data protection and security trainings
- **Environment Chain:** Development, testing and staging environments are separated from Production environment.
- **Peer Code Reviews:** Proper code reviews for all the code entered to the version control system.
- **Static Code Analysis:** Integrated automated code scanners for every commit to detect problems or security issues in the code commits.
- **Integrated Vulnerability Scanning:** Automated checks are performed throughout the SDLC to detect and address vulnerabilities in the code or used libraries. On top of this, as part of our software development process, we periodically use the **OWASP ZAP (Zed Attack Proxy)** tool to identify and address security vulnerabilities, ensuring our application remains a secure and trusted platform for your information.
- **Robust CI/CD:** Robust Continuous Integration (CI) and Continuous Deployment (CD) tooling to deploy one-touch to any environment.
- **Continuous Improvement:** We regularly enhance our security practices, adopting new technologies and techniques to maintain the highest levels of protection.

Who can access your data?

Access to your data is strictly controlled, ensuring that only authorised personnel can view or modify information:

- **Role-Based Access Control (RBAC):** You can define who has access to specific data based on their role, providing tight control over sensitive information.
- **Least Privilege Principle:** Access is granted only to those who require it for their job functions, minimising the risk of unauthorised access.
- **Multi-Factor Authentication (MFA) and Single Sign-On (SSO):** Enhanced security options like MFA and SSO ensure only verified users can access your system.