

Data and Access Protection 2026

Overview

Dokka is committed to protecting the confidentiality, integrity and security of our customers. We use a variety of industry-standard security technologies and procedures to help protect your Information from unauthorized access, use, or disclosure.

As part of our focus for customer data protection and security awareness, we implemented development and operational processes in place to make sure we protect the most valuable asset we have - customer data.

Data Privacy

✓ **Cookie Policy**

A published cookie policy explains what data is collected through the product and site, and how it is used, supporting transparency with customers and end users.

✓ **Data Breach Notification**

A formal process is in place to notify affected parties promptly if a data breach occurs, so they can take immediate protective action.

✓ **Employee Security & Privacy Training**

Staff complete security and privacy awareness training so that sensitive data is handled consistently and breach risk is reduced.

Data Security

✓ **Access Monitoring**

Network, application, and system logs are streamed into a Security Information and Event Management (SIEM) platform and monitored continuously (24/7/365) by the security team.

✓ **Data Deletion**

Data is stored with defined deletion procedures; storage media decommissioning follows an industry-standard method (e.g. NIST 800-88).

✓ **Encryption at Rest**

Data at rest is encrypted using AES-256, with encryption keys held and rotated in a managed key-management service.

✓ **Encryption in Transit**

Data moving across open networks is encrypted using TLS 1.3, with TLS 1.2 as the minimum accepted version.

✓ **Geographic Location of Data**

Dokka's infrastructure and data is hosted in Azure EU, Netherlands.

Application Security

✓ **Application Penetration Testing**

An independent third party performs application penetration testing on an annual basis, combining manual and automated techniques.

✓ **Code Analysis**

All code is statically analyzed and peer-reviewed before it reaches production.

✓ **Secure Development Training**

Developers complete dedicated secure-coding training sessions as needed.

✓ **Software Development Lifecycle**

Development follows an OWASP-aligned secure SDLC, with continuous vulnerability monitoring and automated scanning of third-party libraries for known issues.

✓ **Vulnerability & Patch Management**

Vulnerabilities are centralized, classified by impact to confidentiality, integrity, and availability, and remediated within severity-based timeframes set by internal policy.

✓ **Web Application Firewall**

A WAF filters, monitors, and blocks application-layer traffic to defend against known attack patterns.

Access Control

✓ **Least Privilege**

Access is granted by role through a central identity provider, following least-privilege principles to minimize unauthorized access.

✓ **Logging**

Intrusion-detection, edge traffic, and authentication/authorization logs feed the SIEM, supporting faster threat detection and incident response.

✓ **Password Security**

A formal password policy enforces minimum length and complexity requirements to reduce the risk of unauthorized access.

Infrastructure

✓ **Cloud Hosting**

Core systems are hosted on Microsoft Azure, with certain backup data optionally held with a secondary provider.

✓ **Anti-DDoS**

A leading CDN provides DDoS and brute-force protection, with rate limiting configured at both the edge and application layers.

✓ **Data Center Security**

Hosting facilities apply physical and environmental security controls consistent with a highly resilient infrastructure.

✓ **Environment Segregation**

Production, staging and development environments are physically segregated , with customer data logically segregated at the application level using unique identifiers.

Endpoint Security

✓ **Anti-Malware / EDR**

Company workstations run a centrally managed Endpoint Detection and Response (EDR) solution, monitored 24/7/365 by the security team.

✓ **Disk Encryption**

All workstations are encrypted (e.g. FileVault/BitLocker).

✓ **Host Intrusion Detection**

Host-based intrusion detection/prevention runs on employee workstations, with daily signature updates.

Network Security

✓ DDoS Protection

CDN-based mitigation protects against distributed denial-of-service attacks, preserving availability and performance.

✓ SIEM

A Security Information and Event Management solution continuously monitors network events for real-time threat detection and compliance.

Incident Response

✓ Designated Response Personnel

A documented incident response plan covers detection, escalation, internal and external communication, mitigation, and post-mortem analysis. A cross-functional response team (security, engineering, legal, and other teams as needed) leads the process, engaging a third-party incident response firm when required.

✓ Incident Reporting

Affected customers are notified without undue delay, in line with contractual data-processing terms, and are informed of the nature of the incident, its known impact, and remediation steps taken.

Business Continuity & Disaster Recovery

✓ Business Continuity Plan

A business continuity plan aligned with ISO 27001 addresses disruption affecting physical office locations.

✓ Data Backup

Backups are performed daily, encrypted, and cloud based. Backup and restoration procedures are tested at least annually.

✓ Disaster Recovery

A documented Disaster Recovery Plan restores core service functionality from a dedicated DR site. DR testing (walk-through, mock disaster, or component testing) is conducted at least once a year.

✓ Recovery Objectives

Recovery Time Objective (RTO): 24 hours. Recovery Point Objective (RPO): 24 hours.

Risk Management

✓ Risk Assessments

An ongoing risk management process identifies vulnerabilities and emerging threats. A formal risk assessment is conducted annually as part of ISO 27001 certification.

✓ Supply Chain Risk Management

Sub-processors are held to defined security and privacy standards, covered by data processing agreements, and assessed at least annually through privacy, legal, and security reviews.

Corporate Security

✓ Email Protection

Corporate email is protected against malware and phishing, with DMARC enforced.

✓ Employee Training

Staff receive ongoing training to stay current on security and compliance best practices.

✓ Personnel Termination / Transfer

HR procedures define clear steps for employee termination and role changes, keeping access consistent and reducing legal and security risk.

Security Training

✓ Employee Privacy Training

New hires complete mandatory security and privacy training during onboarding and at least annually thereafter, including tutorials and monitored exercises. Quarterly awareness campaigns reinforce the program.

✓ Phishing Training

Company-wide awareness training covers phishing and social engineering.

✓ Role-Based Training

Dedicated sessions are held as necessary for specific roles — for example, secure coding training for developers.

Change Management

✓ Change Management Program

Documented change management procedures apply to all infrastructure changes, including peer review, evaluation of security implications, and an audit trail supported by

infrastructure-as-code. Changes are communicated to relevant technical staff through an internal knowledge base.

Compliance

- ✓ DOKKA is ISO 27001 Certified
- ✓ SOC 2 TYPE 2 Compliant (Report available on request)
- ✓ GDPR and Israeli Privacy Law Compliant

