Legal Sector Guide

Client Confidentiality & Data Protection

Stannp operates as a Data Processor under UK GDPR and Data Protection Act 2018 with ICO registration ZA134992. All client data and legal communications are classified as confidential and protected with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys. Data is hosted exclusively in Ireland (EEA) on Microsoft Azure with no transfers outside the EEA.

Security Architecture & Access Control

Multi-factor authentication is mandatory for all internal systems with 2-hour session timeouts. Access follows role-based access control with least privilege and need-to-know principles, ensuring unique user authentication with no shared accounts. The platform operates 24/7 SIEM monitoring with 12-month audit log retention and clock synchronisation. Critical services maintain 99%+ uptime SLA with RTO 30 minutes and RPO 6 hours for databases.

Compliance & Security Testing

ISO 27001, Cyber Essentials, and PCI-DSS certifications provide regulatory compliance assurance. Comprehensive security programme includes:

- Monthly vulnerability scans using Qualys and Security Scorecard
- Annual penetration testing and security assessments
- OWASP Top 10 application security testing
- Automated GitHub vulnerability scanning for source code
- CVSS-based patching: Critical 7 days, Important 14 days, Moderate 30 days

Data Retention & Secure Disposal

Critical data backups occur every 15 minutes with daily full backups retained for 30 days. All backups are encrypted and geographically separated within the EEA. Standard retention is 3 years (customisable) with 2-month processing retention, supporting GDPR erasure rights. Secure disposal procedures include physical destruction of hard drives before equipment disposal, complying with WEEE legislation and UK GDPR requirements.

Incident Response & Business Continuity Testing

Data breaches are reported to the ICO within 72 hours as required by UK GDPR. Incident management framework classifies incidents by severity (Critical, Major, Minor) with structured response processes including detection, containment, investigation, eradication, recovery, and post-incident review. Comprehensive Business Continuity Plan covers all facilities with regular testing through recovery scenarios and tabletop simulations.

Physical Security & Training

Facilities maintain 24/7 alarm monitoring and CCTV surveillance with controlled access and visitor accompaniment. Clean desk policy and locked cabinets protect confidential documents. Network equipment is housed in protected cabinets with restricted access. All staff receive annual security awareness training covering UK GDPR, data handling, phishing, social engineering, and incident reporting. Technical personnel receive specialised training on secure coding practices and OWASP Top 10 guidelines.