Stannp.com
The Direct Mail Platform

Retail & E-Commerce Guide

Data Protection & PCI-DSS Compliance

Stannp operates as a Data Processor under UK GDPR and Data Protection Act 2018 with ICO registration ZA134992. All customer and payment data is 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. ISO 27001, Cyber Essentials, and PCI-DSS certifications ensure retail sector compliance. Data is hosted exclusively in Ireland (EEA) on Microsoft Azure with no transfers outside the EEA.

High Availability & Scalability

The platform delivers 99%+ uptime SLA with 24/7 SIEM monitoring and 12-month audit log retention. Critical services maintain RTO 30 minutes and RPO 6 hours for databases, supporting high-volume processing requirements. 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.

Security Testing & Monitoring

Comprehensive security programme includes:

- Monthly vulnerability scans using Qualys and Security Scorecard
- Monthly PCI-DSS compliance scans
- 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 Management & Recovery

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.

Incident Response & business Continuity

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: detection, classification, containment, investigation, eradication, recovery, and post-incident review. Business Continuity Plan includes periodic recovery scenario testing and staff training exercises.

Physical Security & Staff Training

Facilities maintain 24/7 alarm monitoring and CCTV surveillance with controlled access and visitor registration. Clean desk policy and locked cabinets protect confidential materials. All equipment is tracked throughout its lifecycle with secure disposal procedures. Staff receive annual security awareness training covering UK GDPR, PCI-DSS requirements, phishing, social engineering, and incident reporting. Technical personnel receive specialised training on secure coding practices and OWASP Top 10 guidelines.