Data Transfer and Security

Secure Data Transfer Methods

At Stannp, we understand that secure data transfer is critical to protecting your sensitive information. We have implemented multiple layers of security to ensure your data remains protected throughout the transfer and processing lifecycle.

How Data is Transferred to Stannp

File Upload Security Customer data is provided via Excel/CSV files through our secure platform. All file uploads are processed through secure channels with validation checks for file types and sizes. Uploaded data is scanned for security threats and encrypted immediately upon receipt.

API Integration Our API-first platform implements comprehensive security measures including authentication tokens, rate limiting, encrypted connections via HTTPS/TLS, and detailed access logging. All API calls are monitored for suspicious activity and require valid authentication credentials.

Data in Transit Protection

Encryption Standards All data transmitted to and from Stannp is protected using TLS 1.2/TLS 1.3 protocols. Our connections are rated A+ by Qualys SSL Labs, ensuring the highest level of encryption security during data transfer.

Secure Channels Only We enforce encrypted connections for all data transfers. No unencrypted transfer methods are permitted, ensuring your data remains protected from interception during transmission.

Data Processing

Types of Data We Process We process full names and postal addresses for mail delivery, along with optional personalisation fields such as titles, customer IDs, and dynamic content. We follow data minimisation principles, processing only the minimum data necessary for mail delivery services.

Segregated Environments Customer data files are isolated and processed in segregated environments. Each customer maintains unique account IDs with data isolation through multi-tenancy architecture and network-based tenant separation.

Data Storage Location

EEA-Based Storage All data is stored on cloud-based servers located in Ireland (within the EEA). We do not transfer data outside the EEA, ensuring compliance with UK GDPR requirements.

No Sub-Processors We do not use sub-processors to handle personal data. All data processing is performed directly by Stannp, maintaining complete control over your data security.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ

01271 320 863
www.stannp.com

Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992

Data Encryption at Rest

All stored data is protected using 256-bit AES encryption. Cryptographic keys are securely managed and stored in Azure Key Vault, ensuring that your data remains protected even when stored on our servers.

Data Retention and Deletion

Retention Policy Data is retained for 3 years as standard, though retention periods can be customised based on client requirements. Customer data used for processing is removed after processing when no longer required, with a standard retention period of 2 months for reprocessing needs.

Secure Deletion All data is securely deleted at the end of the retention period. Our platform allows authorised users to update and delete data as needed, with self-service deletion options in compliance with GDPR requirements.

Access Controls

Authorised Access Only We enforce role-based access control (RBAC) with least privilege principles, ensuring data is accessible only to authorised personnel who require it for specific job functions. All access is logged and monitored.

Authentication Security Multi-factor authentication (MFA) is implemented on all systems, with unique user accounts requiring complex passwords. Regular access reviews and automatic de-provisioning ensure that only current, authorised employees can access systems.

Monitoring and Compliance

Continuous Monitoring All data transfers and access are monitored through our SIEM system, providing real-time alerts for any anomalies or suspicious activity. Comprehensive audit logs are maintained for all system access and data processing activities.

Regular Security Assessments We conduct monthly vulnerability scans and annual penetration testing to ensure our data transfer mechanisms remain secure and resilient against emerging threats.

Your Data Control

Customers retain full control of their data through our platform. You can update, delete, or restrict data processing as needed, ensuring compliance with data subject rights under UK GDPR.

Stannp
Unit 12, Taw Trade Park
Braunton Road, Barnstaple, EX31 1JZ
01271 320 863
www.stannp.com
Stannp Ltd
Company Reg: 09086822
ICO Data Protection Reference: ZA134992