Regionalisation & Data Residency Guide

Overview

Stannp maintains a robust regionalised infrastructure designed to ensure data sovereignty, regulatory compliance, and optimal service delivery for our UK and European customers. Our regional architecture provides both security and performance benefits through strategic data placement and network segregation.

Data Storage Location

EEA-Based Infrastructure For all UK customers, data is stored exclusively on cloud-based servers located in Ireland, within the European Economic Area (EEA). This ensures full compliance with UK GDPR and EU data protection regulations.

No Data Transfers Outside EEA We do not transfer UK customer data outside the EEA. All processing, storage, and backup operations for UK customer data remain within EEA boundaries, maintaining complete data sovereignty and regulatory compliance.

Microsoft Azure Hosting Our infrastructure is hosted on Microsoft Azure's Ireland data centres, benefiting from enterprise-grade physical security, environmental controls, and infrastructure management whilst maintaining EEA data residency.

Regional Network Architecture

Multiple Virtual Networks Our infrastructure utilises multiple virtual networks for regionalised areas, ensuring that data remains within appropriate geographic boundaries whilst maintaining network isolation and security.

Regional Separation Capabilities We maintain regional separation capabilities as part of our multi-tenancy architecture. This ensures that customer data can be segregated by geographic region whilst maintaining the security and efficiency benefits of our shared infrastructure.

Network-Based Tenant Separation Each customer account maintains complete data isolation through unique account IDs and network-based tenant separation. Regional architecture ensures your data remains in the designated geographic location throughout its lifecycle.

Backup & Disaster Recovery

Geographically Separated Backups All backup data is stored in separate availability zones within the Republic of Ireland. This zonal separation ensures that zone-level incidents or failures do not affect both primary and backup data simultaneously.

Regional Redundancy All redundant systems remain within EEA boundaries for UK customer data, maintaining both availability and compliance.

Backup Frequency Critical data is backed up every 15 minutes with weekly secondary backups. All backups are encrypted and stored in alternative EEA server regions, ensuring both security and geographic resilience.

Environment Segregation

Separate Development Environments We maintain separate virtual networks for development data and staging environments. Development and testing activities are conducted in isolated environments that maintain the same regional boundaries as production systems.

Production Environment Protection Production customer data remains in designated regional infrastructure, completely segregated from development and staging environments through network-based separation controls.

Compliance & Data Sovereignty

UK GDPR Compliance Our EEA-based infrastructure ensures full compliance with UK GDPR requirements, including data residency, transfer restrictions, and territorial scope provisions.

Data Controller Requirements By maintaining data within the EEA, we support our clients (as data controllers) in meeting their regulatory obligations regarding international data transfers and data subject rights.

No Sub-Processors Outside EEA We do not use sub-processors to handle personal data, and all data processing is performed directly by Stannp within EEA infrastructure. This eliminates concerns about international data transfers to third-party processors.

Service Delivery & Performance

Regional Optimisation Our multi-region infrastructure provides optimal performance for UK and European customers through reduced latency, improved response times, and efficient content delivery whilst maintaining data residency requirements.

High Availability We maintain a 99%+ uptime SLA through zonally redundant systems within the EEA. This geographic distribution provides resilience without compromising data sovereignty.

Scalability Within Region Our infrastructure scales to handle campaigns of any size whilst maintaining all data within EEA boundaries. From individual mailings to enterprise-level volumes, regional infrastructure supports consistent service quality.

Data Security Within Region

Encryption Throughout All data remains encrypted both at rest and in transit as it moves between EEA server regions for backup, redundancy, or load balancing purposes. Encryption maintains security whilst data remains within regional boundaries.

Access Controls Access to regionally stored data follows strict role-based access control principles. All access is logged, monitored, and restricted to authorised personnel, regardless of which EEA region the data is stored in.

Monitoring & Compliance

Data Residency Controls Our infrastructure is configured to maintain data residency within the EEA, with policies in place to ensure compliance with regional data storage requirements.

Audit Trail Comprehensive audit logs track all data movements within our regional infrastructure, ensuring full visibility and accountability for where data is stored and how it is processed.

Transparency & Control

Data Location Visibility We maintain transparency about data storage locations. UK customers can be assured that their data resides exclusively within EEA infrastructure in accordance with our data protection commitments.

Customer Control Customers retain full control over their data through our platform, including the ability to update, delete, or restrict data processing in compliance with UK GDPR requirements, all whilst data remains within EEA boundaries.

Commitment to Regional Compliance

Our regionalised infrastructure ensures that UK customer data remains within the EEA throughout its entire lifecycle, from initial upload through processing, backup, and eventual deletion. This commitment to data residency supports regulatory compliance whilst maintaining the security, availability, and performance standards our customers expect.