Charities & Not-for-Profit Organization Guide

Donor Data Protection & Fundraising Compliance

Charitable organizations hold a unique position of trust with their supporters, donors, and beneficiaries. Stannp operates under applicable US privacy regulations including state data protection laws, providing the security infrastructure necessary to maintain this essential trust relationship.

All donor, supporter, and beneficiary data receives confidential classification with 256-bit AES encryption at rest and TLS 1.2/1.3 in transit, achieving an A+ SSL rating from Qualys. Our infrastructure specifically addresses the unique obligations charities face including compliance with the applicable nonprofit compliance requirements, and the sensitive nature of vulnerable beneficiary data.

Platform Security and Access Control

The platform enables charitable organizations to manage their own user accounts and access controls, supporting role-based access control tailored to charity operations. Organizations can configure access appropriate for fundraising teams, volunteer coordinators, service delivery staff, and trustees, ensuring supporter data is accessible only to authorized personnel with legitimate need.

Multi-factor authentication is available for enhanced security, providing additional protection for accounts accessing sensitive donor and beneficiary information. The platform operates continuous monitoring with 99%+ uptime SLA, ensuring fundraising and service delivery systems remain accessible when needed most.

Regulatory Compliance & Security Standards

We maintain ISO 27001 and PCI-DSS certifications demonstrating our commitment to recognized security standards. These certifications provide assurance to charity trustees and donors that supporter data receives appropriate protection.

Monthly vulnerability scans and security assessments identify and address potential security weaknesses. Critical vulnerabilities receive remediation within 7 days, with important vulnerabilities addressed within 14 days, ensuring supporter data remains protected against emerging threats.

Application security testing performed against OWASP Top 10 standards protects against common web application vulnerabilities. Automated GitHub vulnerability scanning monitors source code continuously, identifying security issues before they reach production systems.

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 Protection & Recovery

Critical data receives backup every 15 minutes with daily full backups retained for 30 days. All backup data is encrypted and stored in zonally separated locations, ensuring recovery capability.

Organizations manage their own data retention policies within the platform. The system supports appropriate data retention periods in compliance with applicable privacy regulations. Secure disposal procedures include physical destruction of hard drives before equipment disposal, ensuring complete data sanitization.

Incident Response

Data breaches are reported to relevant authorities within 72 hours as required by applicable US privacy regulations. Our incident management framework classifies incidents by severity level—Critical, Major, or Minor—with structured response processes including detection, classification, containment, investigation, eradication, recovery, and post-incident review.

Charities receive timely notification of any incidents affecting their supporter data, enabling them to meet their own notification obligations to affected supporters. Staff receive annual security awareness training covering phishing, social engineering, and incident reporting procedures specific to the charity sector's unique risk profile.

Data Security & Personnel Vetting

All IT equipment is tracked throughout its lifecycle with hard drives physically removed and destroyed before disposal. This ensures supporter data including legacy pledges and vulnerable beneficiary details cannot be recovered from disposed equipment.

All new employees are subject to background checks before commencing employment, ensuring appropriate vetting for personnel who may access sensitive data.