Data Breach Response & Notification Guide

Overview

Stannp maintains a comprehensive Data Breach Response Plan to ensure prompt, appropriate, and transparent handling of any data security incidents. Our structured approach prioritises containment, risk assessment, and communication, ensuring the security and integrity of customer data whilst meeting all regulatory obligations under UK GDPR.

Our Commitment

We are responsible for the security, integrity, and confidentiality of all data we hold. Any suspected breach is managed through our formal response plan, ensuring swift action to protect customer data and minimise potential impact.

Structured Response Process

Our response follows five key steps: immediate identification and assessment, containment and recovery actions, comprehensive risk assessment for affected individuals, notification to relevant parties including the Information Commissioner's Office (ICO) where required, and post-incident evaluation and improvement. This systematic approach ensures consistent, effective handling whilst maintaining transparency.

Immediate Action

Upon discovering a potential breach, we immediately assess the situation, determine what data is involved, identify the root cause and extent, evaluate potential harms to affected individuals, and implement containment measures. We categorise incidents by severity to determine appropriate response actions based on the level of risk.

Risk Assessment & Notification

We conduct thorough risk assessments considering the type and sensitivity of data involved, protective measures in place, how many individuals are affected, and potential harms. Based on this assessment, we determine appropriate notifications to affected individuals, the ICO, clients, and other relevant parties. Notifications include clear descriptions of the breach, actions taken, and protective steps individuals can implement.

ICO Reporting

We notify the Information Commissioner's Office within 72 hours of becoming aware of breaches that pose risks to individuals' rights and freedoms. Where breaches result in high risk, we communicate directly with affected individuals without undue delay, providing clear explanations and protective measures.

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

Continuous Improvement

Following any breach, we conduct comprehensive reviews to identify improvement areas. We maintain incident logs to identify patterns and implement recommendations to prevent similar incidents, strengthen vulnerabilities, enhance training, and improve response effectiveness.

Types of Incidents

Our plan addresses disclosure of data to unauthorised individuals, loss or theft of devices or records, inappropriate access controls, IT security breaches and hacking attempts, unauthorised alterations or deletions, viruses and security attacks, physical security breaches, and misdirected communications containing sensitive information.

Commitment to Transparency

Our Data Breach Response Plan ensures that any security incidents are handled swiftly, professionally, and transparently through immediate containment, thorough risk assessment, appropriate notification, and continuous improvement, maintaining the highest standards of data protection whilst meeting all regulatory obligations.