



## Honch Data Limited: Information Security & Risk Management

Last reviewed: 14.10.2026

### Introduction

Honch Data Limited provides specialised B2B subscription services, offering clients information on global CMOs, finance, and HR decision-makers. Data is primarily collected from publicly available sources, such as LinkedIn public pages and Companies House, and includes verified email addresses. Honch follows a "minimal client data" approach: it holds only the client data needed to deliver the service, such as account details and the lists and settings clients choose to add, and it never seeks out sensitive client data. Clients stay in control of how data leaves the platform, whether by export, CRM integration or API.

### Compliance & Governance

- Fully compliant with UK & EU GDPR regulations, actively respecting individual rights (Articles 15-22).
- Appointed Data Protection Officer (DPO): Millie Brown, contactable at [dpo@honch.co](mailto:dpo@honch.co), supported by Anthony Cooper for additional oversight.
- Established and regularly reviewed policies include:
  - GDPR Legitimate Interest Assessment
  - Data Privacy Policy outlining responsible personal data handling.
  - Disaster Recovery Plan for business continuity.
  - Third-Party Management Policy ensuring supplier compliance with security standards.
- Utilises hosting providers with recognised security certifications: Fasthosts (UK-based ISO 27001 certified data centres) and Microsoft Azure (Level 1 CSA STAR Certified).

### Security Controls in Practice

- **Access Management:** Implementation of Multi-Factor Authentication (MFA) across internal accounts, robust password policies requiring complexity and regular updates (every 90 days), and strict internal Role-Based Access Controls (RBAC) applying the least privilege principle.
- **Data Protection:** Industry-standard AES-256 encryption for data at rest, TLS encryption for data in transit, and ensuring data residency within UK-based facilities.
- **Application Security:** Secure software development practices guided by "Security-by-Design" principles, regular third-party penetration testing (at least

annually), and vulnerability scanning through Veracode. Continuous adherence to OWASP Top 10 security standards.

- **Network & Cloud Security:** Robust protection via Azure DDoS mitigation, Azure Web Application Firewall (WAF) to guard against common threats, intrusion detection with real-time 24/7 monitoring, and integrated threat detection via Azure Defender.
- **Endpoint Security:** Comprehensive internal security including antivirus software with real-time scanning and quarterly updates, full-disk encryption on all endpoints, strict MFA enforcement, prohibition of external portable devices, and immediate termination of system access upon staff departure.
- **Logging & Monitoring:** Secure storage of event logs for a minimum of 12 months and login/export records for 6 months. Continuous system monitoring to identify vulnerabilities and suspicious activities swiftly.

### **Risk & Vulnerability Management**

- Regular quarterly technical risk assessments to proactively identify vulnerabilities.
- Frequent penetration testing (at least annually or after major changes), coupled with rapid remediation processes aiming to resolve high-priority vulnerabilities within 48 hours.
- Continuous operational monitoring for security threats and immediate reaction capabilities.

### **Incident Response & Business Continuity**

- Clearly defined incident management procedures, including immediate escalation to senior management and a targeted 1-hour initial response to security incidents.
- Commitment to notify clients of any data breach affecting their interests within 48 hours.
- Annual testing and review of Business Continuity and Disaster Recovery plans with a realistic 48-hour Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

### **Third-Party Management**

- Formal and structured third-party management policy, including annual risk assessments of critical suppliers.
- Suppliers must comply with Honch's security and privacy standards as outlined in relevant policies and procedures.

### **Conclusion**

Honch Data Limited operates a secure and responsible approach to information security and risk management. By maintaining a "minimal client data" approach, utilising certified secure hosting infrastructure, implementing comprehensive security

controls, and adopting a proactive stance towards risk and incident management, Honch ensures client confidence and compliance with industry standards.