Technical and Organizational Measures for Data Protection

Bolt Insight Limited implements a comprehensive set of technical and organizational measures (TOMs) to protect personal data in compliance with EU and UK GDPR. The TOMs encompass a set or adequate information security controls, strict data privacy practices, internal organizational policies, and ongoing monitoring to ensure continuous compliance.

1. **Information Security**

Bolt Insight employs strict logical access controls to prevent unauthorized access to data. Access to systems and data is managed through role-based access control (RBAC), granting employees only the minimum permissions needed for their role.

User privileges are reviewed at least annually to maintain a least-privilege model, and access provisioning/deprovisioning follows formal procedures for consistency. Strong authentication mechanisms are in place: production systems require unique credentials and multi-factor authentication (MFA) for remote access, ensuring only authorized staff with MFA can reach sensitive environments.

Password policies enforce complexity and are applied uniformly across in-scope systems in line with company standards. When staff leaves the company, their access rights are revoked within 24 business hours to mitigate any security risk from departing personnel.

Network and infrastructure security is rigorously maintained. Bolt Insight's cloud environment is segmented and protected by firewall rules to isolate data and services, preventing unauthorized network access to customer data. An automated intrusion detection system provides continuous monitoring of the network for any suspicious or malicious activities.

The production infrastructure is hosted in leading cloud data centers (such as Amazon Web Services), where physical and environmental security controls (e.g. guarded facilities, biometric access, fire suppression) are handled by the cloud provider. Bolt Insight leverages these state-of-the-art data center protections and further reviews its cloud providers' security attestations (like SOC reports) on at least an annual basis to ensure ongoing trust.

Encryption is utilized extensively to safeguard data. All sensitive customer data is encrypted at rest (in databases, storage, and backups) and in transit (across networks) using strong cryptographic protocols. Data stored in Bolt Insight's AWS cloud databases and backup

repositories is encrypted, with encryption keys tightly controlled and accessible only to authorized personnel. All web traffic and data exchanges occur over encrypted connections (HTTPS/TLS), ensuring personal data cannot be intercepted during transmission. Even portable media and company devices are encrypted through a mobile device management (MDM) program, so that any data on laptops or removable drives remains secure.

Bolt Insight maintains a secure software development lifecycle (SDLC) and rigorous patch management practices. The company has documented SDLC policies and change management procedures to ensure that any changes to systems or software are carefully reviewed, tested, and approved before deployment. Development and testing are performed in segregated environments (separate from production) to avoid any impact on live personal data.

Code quality and security are built into the process: Bolt Insight uses automated scanning tools to examine source code for common vulnerabilities and to check for known security issues in open-source libraries. Identified issues are addressed according to an internal service-level agreement, ensuring timely remediation of vulnerabilities. Moreover, the infrastructure is kept up-to-date through routine patching – servers and applications are regularly patched as part of maintenance or in response to new threats, which helps harden systems against emerging security risks.

2. **Data Privacy**

Bolt Insight's data privacy measures ensure that personal data is handled lawfully, fairly, and transparently, with respect for privacy by design principles. The company classifies data based on sensitivity and applies protective controls accordingly. In particular, any customer-provided data or research participant information that includes personal data is classified as "Confidential" and treated with the highest level of protection. Public or internal non-sensitive information is segregated from confidential personal data, which helps prevent inadvertent exposure. Where possible, Bolt Insight uses anonymization or pseudonymization techniques to protect individuals' privacy.

By default, the platform and projects are designed to limit personal data collection to only what is necessary for the stated purpose, reflecting GDPR's principle of data minimization and privacy by default.

Adequate policies govern the handling of any personal information throughout its lifecycle. Bolt Insight has implemented internal data handling and privacy policies that align with EU and UK data protection regulations and client contractual requirements. All employees and

contractors are made aware of these policies and are obligated to follow them, as a condition of their employment or engagement.

These policies cover how to properly collect, use, store, and disclose personal data, and they are reviewed at least annually to incorporate any changes in law or best practices. This regular review ensures that Bolt Insight's privacy practices remain up-to-date and effective.. Bolt Insight follows "privacy by design" by considering data protection requirements from the early stages of new projects or features. Senior management stays informed of regulatory changes and adjusts business processes or software features as needed to maintain compliance.

Bolt Insight also addresses data retention and deletion in line with GDPR principles. Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws and contracts. The company has formal data retention and disposal procedures to ensure data is not kept indefinitely. When data is no longer needed, these procedures mandate secure disposal or deletion of the data, whether by erasing electronic records or securely destroying physical media.

In the event of a security incident or personal data breach, Bolt Insight has a well-defined incident response plan that includes privacy-specific protocols. The company's incident response procedures outline how to identify, contain, and resolve security incidents, and they explicitly address the handling of data breaches involving personal information. There are clear steps for internal reporting and escalation so that incidents are acted upon without delay. Critically, Bolt Insight's plan includes notification processes to inform clients and, if required, regulatory authorities of a breach within the timeframe mandated by GDPR.

3. Organizational Measures

Bolt Insight fosters a strong organizational culture of security and privacy, backed by internal governance and documented policies. The company has established a comprehensive set of information security and data protection policies that are approved by management and communicated to all employees. These policies (covering areas such as access control, acceptable use, data handling, and incident response) are kept current and are reviewed at least annually for relevance and effectiveness. Through this policy framework, Bolt Insight sets clear expectations and guidelines for protecting personal data and maintaining compliance with GDPR. Crucially, Bolt Insight Limited has appointed a dedicated Data Protection Officer (DPO) in accordance with GDPR Articles 37–39.

The DPO is responsible for overseeing the company's data protection strategy and ensuring that Bolt Insight meets its obligations under EU and UK GDPR

Roles and responsibilities related to security and privacy are clearly defined within the organization. Bolt Insight's management has formally assigned responsibility for the design, implementation, and monitoring of security controls to specific roles, ensuring that accountability is built into job descriptions.

A senior member of management (including the DPO and Chief Technology Officer) provides oversight of data protection activities, and there is top-down support for security initiatives..

Bolt Insight also implements thorough personnel security practices as part of its organizational measures. All prospective employees undergo background checks as permitted by law, to verify their integrity and reduce insider risk. During onboarding, every employee is required to sign a confidentiality and non-disclosure agreement, contractually binding them to protect company and customer information.

Employees must also review and acknowledge Bolt Insight's key policies (including the Code of Conduct and information security policies) when they join. To ensure ongoing vigilance, Bolt Insight provides regular security awareness training to all staff. New hires receive security and privacy training within their first month of employment, and all employees must complete refresher training at least annually thereafter. This training educates personnel on data protection principles, phishing risks, safe data handling, and their individual responsibilities under GDPR. By reinforcing training on a yearly basis, Bolt Insight helps its team stay current with evolving best practices and reminds them of the critical role they play in safeguarding personal data.

Bolt Insight's risk management and third-party oversight processes further strengthen its organizational controls. The company maintains a documented risk management program that continually evaluates security and privacy risks to the organization.

Management conducts risk assessments at least annually, examining the potential threats to personal data and compliance in light of changes in technology, business operations, and regulations. This annual risk assessment includes consideration of scenarios like cyber threats or fraud, as well as any new legal requirements, ensuring that Bolt Insight proactively identifies and addresses vulnerabilities before they can be exploited. The results of these risk assessments are reviewed by leadership and drive updates to controls or procedures as needed. In addition to internal risks, Bolt Insight carefully manages risks arising from its vendors and service providers.



The company has a vendor management program that imposes security and privacy due diligence on third parties who handle Bolt Insight's data or systems. Key components of this program include maintaining an inventory of critical suppliers, defining security and data protection requirements that vendors must meet, and conducting at least annual reviews of those critical vendors. Before engaging a new sub-processor or service provider, Bolt Insight assesses the vendor's security measures and obtains contractual commitments (such as Data Processing Agreements) to ensure GDPR-compliant handling of personal data. By actively monitoring vendor compliance and insisting on strong data protection clauses in contracts, Bolt Insight extends its security and privacy standards throughout its supply chain.

4. **Monitoring and Evaluation**

Bolt Insight continuously monitors the effectiveness of the above measures and evaluates its security posture on an ongoing basis. Technical controls are subject to regular testing and auditing. Bolt Insight performs routine vulnerability scanning of its networks and systems to identify any weaknesses or misconfigurations.

These scans are run at least quarterly on externally facing systems and more frequently on code repositories, as part of the development cycle. In addition, the company engages in periodic penetration testing of the production environment. Independent security experts probe Bolt Insight's applications and cloud infrastructure to find potential vulnerabilities, so that the company can remediate them before they are exploited. When vulnerabilities or security findings do arise, Bolt Insight has processes to promptly address them – patches or configuration changes are applied to mitigate risks within defined timeframes.

Bolt Insight uses various tools and services to achieve continuous security monitoring. The company's cloud monitoring services (such as AWS CloudWatch/CloudTrail and GuardDuty) track infrastructure and application logs in real time, alerting the security team to any anomalies or unauthorized access attempts. An intrusion detection system generates alerts for potential attacks from outside the system's boundaries, allowing the team to respond swiftly. Internally, Bolt Insight's DevOps and security personnel keep dashboards of key security metrics and regularly review system events to ensure everything remains within normal operational parameters.

Bolt Insight also conducts periodic internal reviews and assessments of its controls to verify that policies are being followed and that controls operate effectively. Management performs control self-assessments and internal audits against security policies, and any exceptions

or improvement areas are documented. These internal evaluations, along with the annual risk assessment, help Bolt Insight to identify gaps and strengthen its control environment proactively. The company`s security controls are audited annually in the SOC 2 Type 2 report, and it maintains certifications/attestations as needed to satisfy client and regulatory expectations.

More information about the technical and organizational measures can be found by accessing our Trust Center.