INTENTHQ

PRIVACY AND SECURITY IN PRACTICE

PRIVACY AND SECURITY IN PRACTICE

At Intent HQ (IHQ), we take the security and privacy of your data and your customers' data very seriously. Privacy and Security is at the core of everything we do. This document details our current privacy and security practices we implement at Intent HQ.

Certification

- **Certified SOC 2 (Type II) compliant** assuring you that our systems and processes are robust from the perspective of security, availability, processing integrity, confidentiality and privacy of your data
- **We are ISO27001 certified** and undergo regular compliance audits to provide ongoing assurances that our information security and system controls remain effective as our business evolves
- **We are fully GDPR & CCPA legislation compliant** as required as a processor of your Personal Data
- This includes all legal, physical and technical controls in pursuit of best practice information risk management

Client user management

- Client user access to Intent HQ products is administered using **role-based data access controls**. These controls assign permissions determining what data each user can access, and what actions can be taken
- Single Sign-On, **Two-Factor Authentication** is available where supported
- Authorisation using the principle of least privilege

Platform and product

- The IHQ Platform utilises multi-layer access control, secure information event monitoring and audit logging
- We manage staff access using **Role Based Access Control** (RBAC) with time-restricted access to infrastructure
- Our products **automatically maintain data lineage at every stage**. For every data element, visualisation, filter or export, our product maintains meta-data describing the feed and field names of every piece of data that went into creating it. Knowing precisely how data moves around the Intent HQ Platform, you can enforce any privacy regulation efficiently
- Intent HQ **Privacy Controls** enable Privacy and Legal teams to enforce compliance with corporate or legislative policy regarding how different types of Personal Data can be used
- **Complete transparency and auditability of IHQ data processing activity**. Any data processing session requiring staff to access your Personal Data data is logged, recorded and easily audited
- The IHQ Platform is hosted in the AWS Cloud, one of the most secure clouds in the world, holding such compliance certifications as ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2
- AWS Operating System and Container hardening is applied to enhance our secure Platform environment further
- Our security by design approach applies rigorous code tests and vulnerability scans before code is ready for production
- We conduct regular 3rd party accredited penetration tests to secure against Platform vulnerabilities
- We are able to offer **single-tenancy architecture on the cloud for each client** creating separate database and instances at the most fundamental level

Data

- We are fanatical about your ability to provide your customers with the highest level of data privacy and security. We take a fundamentally different approach to how we enable you to use Personal Data in a privacy-safe manner:
    - **We do not store raw customer action data**. Instead, our Action Processor transforms personal action data in to privacy-safe Customer Context Vectors which retain meaning in a numeric form usable by data science models
    - **Each customer profile is stored as a single de-identified and encrypted 'micro database'**
    - We retain customer privacy preferences against each customer profile creating a single source of truth, and privacy control against each customers data

- **Data is encrypted in transit and at rest** and volumes with sensitive customer data are encrypted with support for Customer Master Keys (CMK) owned by IHQ with custom key rotation schedule. We utilise TLS protocol version 1.2/1.3 and use certificates based on SHA-256 hashing algorithms. All volumes are encrypted at rest using 256-bit Advanced Encryption Standard (AES).
- All data we ingest is de-identified so your **customers' data remains anonymous** within the IHQ Platform but **can always be re-identified by you**
- Customer data is only retained in complete compliance with either your information security requirements, the local jurisdiction of the law in the geography you operate, or Intent HQ's Security and Privacy Policy (whichever is the more robust)
- Extensive use of allow-lists and block-lists in the process of ingesting data ensures **data is ingested by design, not default**

Physical environment & culture

- Intent HQ has **dedicated security and privacy teams** that implement and manage our security and privacy programs
- Strict **supplier Information Security (InfoSec) regulations.** All new suppliers are vetted against these standards
- All staff adhere to network access by VPN when working away from the office
- Continuous review, on-going communication and compulsory regular company InfoSec training, reminders and internal InfoSec campaigns
- **Controlled access** - All IHQ offices have controlled access at office level. London also benefits from secure access control at building level and CCTV in operation
- A member of IHQ staff accompanies guests at all times beyond office access control
- All laptops & workstations are centrally managed and hardened with full disk-encryption, automated updates, endpoint protection, application-based firewalls and persistence monitoring tools
- Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards

Business continuity

- We conduct periodic risk assessments and regular internal and external InfoSec audits
- Documented Business Continuity and Disaster Recovery plan
- Periodic tests of Business Continuity scenarios

Complementary user entity controls

Intent HQ's services are designed with the assumption that certain controls will be implemented by user entities. Clients should establish their own internal controls or procedures to complement those of Intent HQ's.

The following complimentary user entity controls should be implemented by clients to provide additional assurance that the Trust Services Criteria described within this document are met.

- Stripping or pseudo-anonymizing personally identifiable information from the data feeds sent to Intent HQ.
- Notifying Intent HQ about any data to be removed.
- Adhering to their own password policies.
- Establishing and notifying Intent HQ about the retention policies they wish Intent HQ to apply to client's customer data.
- Determining which personnel should have access to Intent HQ Insights Platform.

INTENT HQ

If you want to discover more about why better privacy controls lead to better results, we'd love to help.

Contact us today at **tellmemore@intenthq.com** or visit us at **intenthq.com**