Information Security Policy

Effective Date: Last Updated as of July 23, 2020

Directly has implemented administrative, technical, and physical security measures designed to protect the confidentiality and integrity of data, including confidential information and personal data as referred to in the Master Subscription Agreement ("Agreement"). These measures may be modified from time to time, provided that any such modification will not materially decrease the overall security of the Marketplace Platform during the term of the Agreement.

Physical Access control (to data processing systems). Measures designed to prevent unauthorized persons from obtaining physical access to the data processing systems with which personal data are processed.

- The data center buildings are controlled by Directly's hosting providers, which are ISO 27001 certified and provide SOC 2, Type 2 attestation reports.

Access control (to use of data processing systems and methods). Measures designed to prevent data processing systems and methods from being used by unauthorized persons.

- We require 2 Factor Authentication for access to our data systems.
- Accounts are locked for repeated invalid attempts to log on, and audit trails are logged and monitored for inappropriate and unauthorized activity.
- Role-based authentication is used where possible with auditing processes and activities to manage appropriateness of access. Privileged accounts utilize two-factor authentication with enterprise-level management where required.
- Data systems are encrypted at rest using AES-256 and in transit using HTTPS.
- Strict Firewall rules are established only allowing required access to and from the production environment.
- Internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data.
- Data systems are designed to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.
- These mechanisms are designed to grant only approved access rights to site hosts, logs, data, and configuration information. The granting or modification of access rights must also be in accordance with Directly's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented.

Access control (to data). Measures designed to ensure that persons who are authorized to use a data processing method only have access to that personal data to which their access authorization applies and that this data cannot be read, copied, modified or removed during processing without authorization.

- User accounts are unique and assigned to appropriate groups by administrative personnel for control.
- Roles limit access to objects through an authorization process with appropriate audit trails.
- Audit logs are monitored for activity and access appropriateness.
- System policies and procedures protect data during processing for appropriate access by authorized personnel.
- All changes to access are logged and reviewed during periodic audits. Abnormal changes create alerts to appropriate personnel.
- Data is deleted according to policy and wiped when no longer required.

Disclosure controls. Measures designed to prevent data from being read, copied, modified, or removed during electronic transmission, data transport, or storage on data carriers without authorization.

- Industry-standard practices are employed to protect data in transit. Private Networks, Virtual Private Networks, and Secure Socket Layer technologies are used to prevent unauthorized access
- Logging of system access is monitored and reviewed for appropriateness

Input controls. Measures to allow Directly to retroactively check and verify whether, when and by whom data has been entered into, modified or removed from the data processing system.

- Access and activity logs are monitored for unauthorized or inappropriate activity as well as to provide change history

Control of instructions. Measures designed to restrict the processing of personal data in accordance with the instructions of the Client.

- Corporate compliance and security policies highlight that client data is accessed only with a business need and is not disclosed

Availability control. Measures designed to protect data from accidental destruction or loss.

- Systems are backed up daily to enable recovery of data on a schedule determined by policy
- High availability or recovery technologies are employed to maintain system operation, availability, and redundancy
- Production environments are replicated in geographically separated data centers with remote storage of backups and recovery systems
- Our infrastructure includes malicious activity detection technology
- Our Disaster Recovery Plans are documented, reviewed and tested on a regular basis

Separation controls. Measures to separately process data that is stored for separate purposes.

- Tiered development, testing, stage, and production environment to separate function and operation
- Access controls are employed to segregate the environments

Personnel.

- Personnel are required to conduct business in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Directly conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
- Personnel must execute a confidentiality agreement and must acknowledge receipt of, and comply with, Directly's confidentiality and privacy policies. Personnel must complete security training.

Subprocessor Security.

- Prior to onboarding subprocessors, Directly evaluates the security and privacy protections of subprocessors to ensure subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Directly requires all subprocessors to enter into appropriate security, confidentiality, and privacy contract terms.

Data Trustees.

- Directly's data trustees, the Director of Security, the VP of Engineering, and the VP of Platform, have primary responsibility for reviewing and updating Directly's information security policies, and for provisioning and revoking authorization for data access.