Technical and Organisational Measures

Document Version Control

Version	Date	Updated by	Comments
1.1	2 January 2019	Edward Cooper	Rebranding
1.2	19 November 2019	Edward Cooper	Review and update

Legal Notice

GDPR – Technical and Organisational Measures

Purpose

This document sets out the security, technical and organisational measures for protecting personal data against unauthorised access, corruption and loss processed by LoopUp in connection with the services it provides to its customers ("**Services**").

Scope

LoopUp must ensure that the latest standards for security and data protection are met and exceeded for the Services, including the protection of personal and confidential data. These standards include operating an information security management system (ISMS) in accordance with the ISO 27001:2013 standard.

LoopUp commits to on-going, comprehensive investments in hardware and software solutions, current technologies and associated processes, policies and audits to ensure that the protective measures are complied with and continually improved.

This document is a summary of some of the technical and organization measures in place. For full details please see the various information security LoopUP policies.

The Policy

Access Control (Building / Offices / Data Centre)

LoopUp has implemented measures to prevent the unauthorised access to data processing systems where personal data is processed including, where appropriate and without limitation, the following:

- Alarm system
- Automatic access control system
- Photoelectric sensors / movement detectors (for alarm system)
- Key Management (Issuance of keys, etc.)
- Visitor management at reception desks
- Protection of building shafts
- Manual locking system (limited usage for key employees to be used in the event of a failure in the access control systems)
- CCTV at entry points (office and data centres)
- Security locks
- Careful selection of cleaning staff
- A separate, specific and documented access control for data centres and server rooms for authorised persons is implemented. Access by authorised persons is documented by name and card or token number. For the data centres, separate access control systems are implemented.

Access Control (Systems)

LoopUp has implemented measures to prevent the use of data processing systems by unauthorised persons including, without limitation, the following:

- Assignment of user rights
- Assignment of passwords
- Authentication with username / password
- Use of Intrusion-Prevention-Systems
- Use of Hardware Firewalls
- Creation of user profiles
- Additional measures: web-application firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity and forced password changes, use of virus scanners
- Assignment of user profiles to IT systems
- Use of VPN Technology
- Encryption of mobile storage media
- Use of central smartphone administration (for example: remote wiping of smartphone)
- Use of a software firewall (office clients)

Access Control (Data)

LoopUp has implemented measures to ensure that authorised users of a data processing system may only access the data for which they are authorised, and to prevent personal data from being read while the data is in use, in motion, or at rest without authorisation including, without limitation, the following:

- Creation of an authorisation concept
- Number of administrators reduced to "absolute necessary"
- Logging of application access, especially during the entry, modification and deletion of data
- Secure media sanitisation before re-use
- Use of shredders or services (if possible with privacy seal)
- Disk encryption (backup tapes for off-site storage)
- Management of rights by system administrators
- Password policy including password length, password change management
- Secure storage of data carriers
- Logging of secure media destruction
- Compliant destruction of data media (DIN 66399)

Transfer Control

LoopUp has implemented measures to ensure that personal data cannot be read, copied or modified during electronic transmission or during transportation or storage to disk, additionally to control and determine to which bodies that the transfer of personal data provided by data communication equipment is allowed including, without limitation, the following:

- Creation of dedicated lines or VPN tunnels
- Documentation of recipients of data and the time periods for the provision of data including agreed deletion times
- During physical transport, careful selection of transport personnel and vehicles (tape off-site storage)
- Disk encryption (backup tapes for off-site storage)
- Disclosure of data in anonymous or pseudonymous form
- TLS encryption of all communications (Web-Client, APIs, mobile Apps)

Input Control

LoopUp has implemented measures to ensure that it is possible to ensure, subsequently control, and determine if and by whom, personal data has been entered, changed or removed on data processing systems including, without limitation, the following:

- Logging of input, modification and deletion of data
- Traceability of input, modification and deletion of data by individual user names (not user groups)
- Granting of rights for the input, modification or the deletion of data based on an authorisation concept
- Creation of an overview of which applications are permitted to input, modify or delete which data
- Storage of forms, through which data has been acquired during automated processing

Order Control

LoopUp has implemented measures to ensure that personal data which is processed by request of the data owner by a data processor, shall only be processed as instructed including, without limitation, the following:

- Subcontractor selection via history review (in particular regarding data security)
- Written instructions to the subcontractor (for example, by Data Processing Agreement)
- Effective control rights over data processors have been agreed
- Prior examination of the documentation and the security measures taken by the subcontractor
- Obligation of the subcontractors' employees to maintain data confidentiality
- Ensure the secure destruction of data after termination of the contract
- Continual review of subcontractor and their activities

Availability Control

LoopUp has implemented measures to ensure that personal data is protected against accidental destruction or loss including, without limitation, the following:

- Uninterruptible power supplies (UPS)
- Devices for monitoring temperature and humidity in server rooms
- Fire and smoke detection systems
- Alarm when unauthorised entry to server rooms is detected
- Testing of data recovery
- Secure off-site storage of data backups
- In flood areas, server rooms are above the water border
- Air conditioning in server rooms
- Protection power strips in server rooms
- Fire extinguishers in server rooms
- Creation of a backup & recovery concept
- Preparation of an emergency response plan
- Server rooms not located under sanitary installations

Segregated Processing

LoopUp has implemented measures to ensure that data which is collected for different purposes can be processed separately including, without limitation, the following:

- Creation of an authorisation concept
- Provision of records with purpose attributes / data fields
- Approved and documented database rights
- Logical client separation (in software)
- In pseudonymous data: the separation of the mapping file and storage on a separate secured IT system
- Separation of production and test systems