Information Security and Data Protection

Customer Notice

(version 4.1)

Information Security and Data Protection Customer Notice

4.1 last updated August 24, 2022

This notice is to provide a summary of LoopUp's information security measures and to help you with your own General Data Protection Regulation (GDPR) / Data Protection Act 2018 compliance program (in the event either applies to you).

This notice sets out details of the type of personal data we may process on your behalf and how we process such personal data when we provide our services to you. It also outlines our commitment to you in relation to how we handle information (including personal data). LoopUp is strongly committed to protecting the personal data of your employees, users and such other individuals using our services as well as upholding their rights to privacy.

Personal data collected

We collect a reasonably small amount of personal data and do not actively collect any 'sensitive personal data' or special categories of data from individuals. Such personal data principally is limited to:

- name, email, phone number (desk and mobile) and office location of users of the services (including, where applicable, SIP addresses and caller IDs);
- contact details of account administrators;
- call detail records (such as call duration and time) as may be required for the provision and billing of our service; and
- call recordings (if so requested by the user).

Full details of all the personal data which we collect and the purposes for which we collect such personal data is set out in our Privacy Policy.

How such personal data is processed

We shall process personal data only for the provision of our services in accordance with our agreed Terms of Service or for such other 'legitimate interests' of ours (such as for the recovery of debts or for protection against fraudulent use or damage to our services). A summary of how we process personal data for each of the different services provided by LoopUp is provided below with full details set out in our Privacy Policy.

Voice services: We will only process personal data as requested by you or as required by regulators or us in order to provide the services to you. This broadly involves the transmission of call data in order to provide our services to you. Such transmission takes place over our Tier 1 carrier interconnections. LoopUp uses Tier 1 regionally best-in-class carriers to perform this function to ensure highly resilient and highly secure transmission.

Remote meetings: One of the great features of using LoopUp remote meetings is that you know who is on your call, a feature that assists you in protecting personal data and maintaining confidentiality. This is used on the vast majority of calls due its simplicity and protects meeting security in a very real, pragmatic way. Users are able to see in real-time who's joining their call, who's speaking and have additional controls over their meeting. If a user does not wish to share their name, phone number or LinkedIn profile when joining a call, the decision is with them at all times. With our service, it is the individual who is in control of their own personal data. Any transmission of personal data is made across the Tier-1 carrier interconnections as mentioned above. All other personal data is process as required by regulators or us in order to provide the services to you.

Operator assisted event calls: Again, you and your users are in control of all personal data provided to LoopUp and LoopUp will only collect information from guests on your calls as prescribed by you and our Privacy Policy.

Technical and organizational security measures

LoopUp is ISO 27001 certified meaning that we adhere to industry recognised standards and processes for the protection of data (including personal data). We encrypt data both in transit and at rest and such data is held in highly secure and resilient Tier 3 datacentres.

The following measures are implemented:

- **Audio bridge data** - data on our audio bridges contains names and numbers, which is considered to be personal data. These bridges are in highly secure datacentres with secure connectivity that it not publicly assessable. Data can only be accessed by authorized personal using specific, secure APIs.

- **Database data** – call detail records and user data are stored in databases that are encrypted at rest, which includes backups. Databases are in highly secure datacentres with secure connectivity that is not publicly accessible. Data can only be accessed by authorized personal using specific, secure APIs.

- **Recordings** - video recordings stored in secure cloud-based facilities and are encrypted at rest and in transit. Audio recordings are stored in highly secure datacentres with secure connectivity that is not publicly accessible. Data can only be accessed by authorized personal using specific, secure APIs. Users can access their data and recordings using personal login credentials via either portals or client plug-ins. Both data and recordings are encrypted in transit via TLS.

Access to data within LoopUp is limited only to those persons who need to access such personal data to provide you our services. All employees are trained appropriately on information security and data protection compliance obligations (training on induction with annual refresher courses) and suitable confidentiality obligations are contained in our contracts of employment.

Transfers and storage of data

We shall only share data with third parties when we are legally permitted to do so.

In all such instances we put contractual arrangements and security mechanisms in place to protect the personal data and where any transfers are to third parties located outside of the European Economic Area, we will ensure that adequate safeguards are in place (such as Standard Contractual Clauses and such supplementary measures as recommended by the EDPB (European Data Protection Board)). More details are set out below.

Datacentres

We provide our meeting and collaboration services from regional datacentres located in the United States (Chicago and Miami), Europe (London), Asia (Hong Kong), Australia (Sydney) and South Africa (Johannesburg) .

Each datacentre is collocated with industry-leading hosting partners and positioned strategically to be at the centre of multiple Tier 1 telephony and data service providers enabling us to deliver highly available, high quality, cost effective services. Within each datacentre, LoopUp's infrastructure is designed to maximise availability and service performance.

Carriers

Calls are delivered to and from LoopUp datacentres via resilient connections to multiple Tier 1 carriers using both circuit-switched telephony (PSTN) and packet-switched telephony (VoIP) over managed Quality-of-Service networks. Carriers are selected primarily based on quality, which is continually monitored.

We work with Tier 1 carriers that have extensive global or regional networks that keeps calls 'on-net' as close as possible to local providers.

Other transfers

We currently may transfer personal data to the following: other members of the LoopUp Group (for the provisions of our services to you); Salesforce products (for managing our CRM), Microsoft (for storage of limited amounts of data and communication or use of Microsoft software); SendGrid (for the delivery of secure email communications); Mixpanel (for customer support platform) and such other third party organizations that may help provide, run and manage our internal IT systems or provide additional support (such as credit agencies, professional advisers or where we agree to provide additional services (such as translation or transcription of operator assisted event calls)). In addition, when you are paying by credit card your data shall be processed by Braintree on our behalf. Such processing is in accordance with Payment Card Industry Data Security Standard (PCI DSS). Please let us know if you would like further details on our sub-processors for each specific service line and the safeguards we have in place with each of them.

International transfers

Where any transfers are to third parties located outside of the European Economic Area (including transfers from the European Economic Area to the UK following 'Brexit'), we will ensure that adequate safeguards are in place. These safeguards include:

- entry into Standard Contractual Clauses (or such other suitable contractual protection) with the third party;
- implementation of supplementary measures as recommended by the EDPB (European Data Protection Board) including:
    - assessing the regulatory landscape and legal system of the recipient country;
    - assessing technical and organisational measures in place with the recipient;
    - assessing whether additional contractual measures are required;
    - continuously reviewing such measures and seeking to improve safeguards wherever practical; and
- implementation of such other measures as recommended by regulators from time to time.

Deletion of data

We will hold data only for as long as we are required to do so either to perform the services to you or for regulatory reasons. Any personal data that forms part of the call detail records are retained for 6-9 months (depending on the deletion / purge cycle). Call recordings (for remote meetings) are available to download for 60 days by each call leader and are only retained on our system for 180 days.

Our commitment to you

We are committed to both your and our own compliance to data protection regulations. As such you can find our commitment to you here.

Our policy is to be as transparent as possible about how and why we process personal data. However, should you have any questions please contact us at either privacy@loopup.com or by writing to us at **Legal and Compliance, The Tea Building, 56 Shoreditch High Street, London E1 6JJ**.