Sourcenext's Commitment to GDPR Compliance

Updated : December 21, 2021

The mission that we, Sourcenext (the creators of POCKETALK) uphold, is to deliver happiness to people throughout the world by breaking down language barriers, and we understand that privacy and security is a key factor in delivering this promise. That is why we are committed to protecting and securing our customers' data to the highest levels, which includes abiding by the data privacy obligations set forth by the General Data Protection Regulation (the "GDPR").

Sourcenext acknowledges that our customers need to be ensured that its translation device POCKETALK (and any services related to) implements technical, organizational and contractual measures in a manner that aligns with the GDPR's compliance obligations, and this document has been prepared with a purpose of providing customers with this information.

The following are key facts that reflect Sourcenext's commitment to data protection practices on POCKETALK.

[Technical Measures to Ensure Privacy and Security on POCKETALK]

- **Privacy by design**: the data flow on POCKETALK is designed to not allow any translation / transcription data to be tracked back to device. Data sent to third party servers (translation / transcription engines) are anonymized, so no information about the actual users of the device are sent to any third party engines.
- **Data Retention**: To reinforce privacy on the device, POCKETALK provides a feature to automatically delete logs stored on the device in a specified interval. In addition, any translation log stored anonymously on the Sourcenext servers are deleted periodically as per the HIPAA (Health Insurance Portability and Accountability Act) regulations.
- **Encryption of data in transit and at rest**: All communication between the device and servers are encrypted using https protocol to ensure security for data in transit. In addition, data at rest is also encrypted for added security.
- **Security Assessments by Testing Institutes**: POCKETALK has been rigorously tested against the ETSI (European Telecommunications Standards Institute) standards, and is expected to pass all the baseline requirements for the "EN 303 645: Cybersecurity for Consumer IoT Products". You can find more information about the ETSI here.
- **Monitoring and Updating Security Measures**: A process for regularly testing, assessing, and evaluating the effectiveness of technical measures are carried out periodically to ensure that security is not compromised by any outdated technologies.

[Contractual and Organizational Measures]

- **Transparency and Subject Rights**: We are fully transparent on the data that we collect and are committed to using personal data only as stated in our [Privacy Statement](). Our policy has been drafted respecting the key principles of GDPR – which are defined as data collection that is "lawful, fair and transparent", "limited for its purpose", "adequate and necessary", "accurate", "not retained longer than needed" and "integrity and confidentiality (security)".

- Under our Privacy Statement, the following rights are guaranteed to customers:
  - Right to Access Copies of Personal Data
  - Right to Correction
  - Right to be Forgotten
  - Right to Withdraw Consent
  - Right to Data Portability
  - Right to Restrict Data Processing
  - Right to Make Objections
  - Rights related to automated decision-making including profiling

  For any requests or inquiries regarding personal data, customers can contact us at [contact-privacyen@sourcenext.com]()

- **Contracts with Sub-processors**: We request sub-processors and entities involved in processing data on our behalf to sign Data Processing Agreements. We also ensure that the latest [Standard Contractual Clauses]() (the SCC's) are also signed with data processors to ensure that international data transfers are governed properly.

- **Policy and Procedures**: We actively review our policies and carry out GDPR-focused gap assessments on any new features or services we implement from a developmental stage, to make sure that we are proactively applying the "data protection by design" principle.

- **Training and Awareness**: Sourcenext understands that providing the proper education and training to all staffs and employees (regardless of whether they handle personal data or not) is a key factor in upholding GDPR compliance on an organizational level. We carry out mandatory Information Security trainings to all staffs on an annual basis.

- **Incident Response:** We have an internal Incidence Response Team which oversees our procedures to identify, investigate, rectify and make necessary reports to authorities as per GDPR requirements.

Sourcenext understands that continuous review and employee awareness are key to ongoing compliance with the GDPR and are committed on continuing to review personal data processing, as well as adjusting and adapting our documentation as required. If you have any questions about our GDPR compliance, please contact us at [contact-privacyen@sourcenext.com]()