Privacy Policy

The data SmartEx needs and how you can control it.

Updated: 1 November 2026

> Meeting audio stays on the device.
>
> Text is sent to the server for cleanup and a summary.
>
> We do not sell data for advertising.

This policy describes the processing of personal data in the SmartEx iOS and Android apps and the smart-expo.ru web service. SmartEx helps companies and exhibition visitors exchange contacts, materials and messages, and helps booth staff keep a record of their meetings.

Contents

1. Who is responsible for your data
2. Data we process
3. Why we need this data
4. Meeting audio and text
5. Who can see information within SmartEx
6. Technical service providers
7. Statistics, permissions and local settings
8. Legal bases and transfers outside Russia
9. How long data is kept
10. Account deletion and your rights
11. Protecting data
12. Children and policy changes

01 Who is responsible for your data

Individual Entrepreneur Alla Vladimirovna Lokot (Локоть Алла Владимировна). Tax ID (INN): 780443351167. Registration number (OGRNIP): 323784700389194. Address: 4 Vedeneeva Street, Saint Petersburg, 195427, Russia.

For personal data enquiries, contact data@smart-expo.ru. For product support, contact support@smart-expo.ru. privacy@smart-expo.ru also accepts personal data enquiries.

This policy takes effect on the revision date shown above. It explains how data is processed and does not itself replace a separate consent where the law requires one.

02 Data we process

- Account and profile: email address, password hash, email verification, first and last name, job title, phone number and photo, depending on what you provide. Passwords are not stored in plain text.

- Company and exhibitions: company name, tax ID, description, city, website, contacts, logo, categories, employees and roles, invitations, exhibition participation, booth access and staff assignments.
- Contacts: the parties and time of an exchange, the exhibition, QR-code information, shared materials, personal notes and favourites. Visitor details may be provided through a web form after scanning a QR code.
- Messages and materials: chat messages, attachments, catalogues, presentations, images, links and other files you choose to upload or share.
- Meetings: the original transcript, cleaned transcript, summary, participants, meeting time and duration. Audio is processed separately on the device, as explained below.
- Technical information: IP address, device and operating system details, app version, installation and session identifiers, push tokens, usage events, error information and crash reports.
- Requests: support messages, complaints, account deletion requests and the information needed to handle them.

03 Why we need this data

- To register users, provide sign-in, protect accounts and manage company teams.
- To display profiles, find companies, exchange contacts, run chats and share selected materials.
- To give employees access to booths at particular exhibitions and prepare meeting materials.
- To deliver service emails and notifications, provide support and handle complaints.
- To diagnose errors, prevent abuse and meet obligations imposed by law.

04 Meeting audio and text

Recording starts when a user chooses to record and grants microphone permission. Speech recognition runs on the device. The meeting audio track is not uploaded to SmartEx servers or sent to the language model provider.

The recording may remain on the device so that the user can listen to it again, for example if the summary is inaccurate. The user controls this local copy and can delete it using the app. If processing is incomplete, the file is also needed to retry speech recognition.

SmartEx does not use the voice to establish a person’s identity, create a user voice profile or train the speech recognition model on their recordings. Audio is used to obtain a text transcript of the conversation.

The text transcript is sent to the SmartEx server and the REG.Cloud language model service for cleanup and summarization. The text may contain names, contact details and other information spoken during the meeting. The original transcript and processing results are stored on the server as meeting materials.

The shared summary is available to both sides of the meeting. The original and cleaned transcripts are available only to the recording side, within its employees’ access rights. Audio is not automatically shared with other participants.

If the person who recorded the meeting shares local audio with others, they are responsible for obtaining the necessary permissions and choosing the transfer method. This is a separate user action, not an automatic transfer by the service.

Before recording, inform everyone present and obtain consent where required. Microphone permission does not replace participants' consent. See https://smart-expo.ru/en/recording.

05 Who can see information within SmartEx

Published company profiles, contacts and materials are visible according to their purpose and access settings. Do not publish someone else's personal information without an appropriate basis.

Company-to-company chats are shared by the companies' employees. New employees can access the company's history, including earlier messages. Contact notes and status are visible within your own company and are not shown to the other side. Each employee controls their own favourites and notification mute settings.

Materials shared through a contact exchange or chat become available to recipients. A meeting summary is shared between the meeting's sides; the original and cleaned transcripts remain restricted to the recording side.

Authorized staff of the operator may process data as necessary to provide support, handle complaints, maintain security and respond to user requests.

06 Technical service providers

We do not sell personal data for advertising. The following providers support the service:

- REG.Cloud / REG.RU: SmartEx server infrastructure, database, files and backups. The main server infrastructure is located in Russia.
- REG.Cloud language model service (ai.reg.cloud): processing meeting text for cleanup and summaries. It does not receive the meeting audio recording.
- REG.RU email service: email verification, invitations, account recovery and replies to enquiries. It processes recipient addresses and email content.
- Google Firebase Cloud Messaging and Apple Push Notification service: delivery of notifications, using installation identifiers, delivery tokens and notification data.
- Google Analytics for Firebase and Firebase Crashlytics: usage events and diagnostics while statistics collection is enabled. They process technical identifiers, device information, events and crash reports.

07 Statistics, permissions and local settings

You can turn off statistics and crash report collection in your profile settings. Collection is enabled by default in current versions. SmartEx does not add your name, email, phone number, chat text or meeting transcript to its own analytics events. Firebase technical identifiers are not fully anonymous data.

The camera is used for QR scanning and selected image actions; the microphone is used for meeting recording; notifications are used for messages and service events. Photos and files are accessed when you select materials. You can manage permissions in your device settings.

SmartEx does not request your phone's address book or precise GPS location. Technical services may infer an approximate region from the IP address. Advertising identifiers are not used for cross-app tracking.

The device stores sign-in information, settings, a queue of unfinished actions, the downloaded speech model and cached files. The web service uses local storage for sign-in and language and theme preferences. These data support the operation of the service.

08 Legal bases and transfers outside Russia

We process data to perform the user agreement and company contracts, meet legal obligations, protect rights and service security where permitted by law, and on the basis of consent where required. Publication of this policy does not mean automatic consent to every form of processing.

Google and Apple operate international infrastructure. Notifications and Firebase may involve processing the relevant technical data outside Russia. This does not involve sending meeting audio to these providers. Firebase describes its data and processing locations at https://firebase.google.com/support/privacy.

Sharing data with service providers and transferring it across borders require the applicable legal bases and safeguards. Contact the operator to ask about the recipients and legal bases for processing your data.

09 How long data is kept

- Profile and sign-in data are used while the account is active. Following a verified request, the account and personal data subject to deletion are deleted or anonymized, generally within 30 calendar days, unless the law requires a different period.
- Messages, company materials and meeting texts are retained for collaboration while participants need them and until an authorized user deletes them or a justified request is fulfilled. Deleting a personal account does not automatically delete the entire company history.
- Local meeting audio remains on the device until deleted by the user or through the app. The operator does not hold a server copy of this audio track.
- Push tokens that have not been refreshed for more than 120 days are removed during the next cleanup. Server logs rotate as new entries accumulate: application logs have a size limit, and web server logs keep 14 archives. They therefore have no single retention period in calendar days. Firebase diagnostic events follow that service's retention rules and project settings and are used to investigate crashes and app operation.
- Automatic daily backups of the database and server files are kept for 7 days and removed during the next rotation. They are used to restore the service, not as active accounts. If data is restored from a backup, previously completed deletion requests must be applied again.
- Contract, payment, request and incident records may be retained to the extent and for the periods required by law or needed to protect rights. On request, we will explain what is retained and why.

10 Account deletion and your rights

You may request information about processing, correction, restriction or deletion, and withdraw consent where processing relies on it. Write to data@smart-expo.ru. Do not send your password. We may ask you to confirm ownership of the account.

Open Settings → Security → Account deletion in the app and confirm your request. If an older Android version opens a web page instead, update the app or follow the instructions on that page. You can also make a request without installing the app: https://smart-expo.ru/en/delete-account.

If you own a company workspace with other employees, tell us whether to retain the workspace and who should take over its management. This helps separate your personal information from the whole team's data.

Withdrawal of consent does not affect the lawfulness of earlier processing. Necessary processing may continue on another lawful basis. You may contact Roskomnadzor or a court to protect your rights, as well as exercise rights available under other applicable law.

Deleting an account does not automatically remove copies other participants have already saved outside SmartEx or local audio on your device. The deletion page explains the request process.

11 Protecting data

Data is transferred over HTTPS. Passwords are stored as hashes. Access to accounts, materials and administrative functions is controlled by permissions. We use backups, technical logs and measures against unauthorized access.

Ordinary chats and server-side materials are not an end-to-end encrypted vault. Do not share information requiring special protection without the appropriate legal basis and arrangements.

12 Children and policy changes

SmartEx is intended for professional use and is not directed at children. If the operator discovers unlawful processing of a minor's data, it takes steps to stop that processing.

The current Russian policy is available at https://smart-expo.ru/privacy and the English version at https://smart-expo.ru/en/privacy. The document is updated when features, providers or processing practices change. Material changes are communicated through an available channel where required by law.

Service operator

Individual Entrepreneur Alla Vladimirovna Lokot (Локоть Алла Владимировна)

Tax ID (INN): 780443351167 · Registration number (OGRNIP): 323784700389194
4 Vedeneeva Street, Saint Petersburg, 195427, Russia
data@smart-expo.ru

Permanent link: https://smart-expo.ru/en/privacy