Privacy Policy

on the processing of personal data on the “Connecta” platform

1. General provisions

1.1. This Privacy Policy (the “Policy”) describes what data is processed, and why, by the person named in “Contact information” (the “Operator”) in providing the “Connecta” software platform (the “Platform”).

1.2. The Policy is an integral part of the Public Offer and applies to everyone who uses the Platform: customer companies, their employees and website visitors.

1.3. The Platform is used by many companies. For data that a customer company enters into the Platform about its own customers and employees, the company determines the purposes and means of processing and the Operator acts on its instructions. For the customer company’s own data and for visitors of our website, the Operator determines the purposes of processing itself.

1.4. By starting to use the Platform, the user confirms that they have read the Policy. If you do not agree with it, stop using the Platform.

2. What data we process

2.1. Account and company data: company name, email address, login, employee’s full name, position and role, profile settings (language, theme).

2.2. Employees’ work data entered by the company: shift schedule, vacations and absences, customer ratings, bonuses, penalties and balance, action log.

2.3. Data of the company’s customers received through communication channels: name, Telegram ID and username, contact details the customer provides, the text of requests and conversations, attachments.

2.4. Technical data: IP address, browser and device information, the log of requests to the Platform, browser push subscriptions, strictly necessary cookies.

2.5. Data you give us when contacting support.

3. Purposes of processing

3.1. Data is processed to:

- provide access to the Platform and its features and identify users;
- operate communication channels, notifications and push messages;
- calculate the plan price and maintain the company balance;
- provide technical support and investigate incidents;
- ensure security and prevent fraud and abuse;
- improve the Platform and develop new features based on anonymized statistics;
- send service messages (email confirmation, balance and security notices) and comply with the law.

3.2. Marketing emails are sent only with separate consent, and you can opt out at any time.

4. Conditions of processing and disclosure

4.1. Processing is carried out using automated means: collection, recording, storage, updating, use, blocking and deletion of data.

4.2. We do not sell personal data. Data may be disclosed only to contractors without whom the service cannot work, and only to the extent necessary:

- hosting and infrastructure providers (servers, file storage);
- email service providers for sending service messages;
- communication channel services connected by the company itself (for example, Telegram);
- public authorities — on a lawful request.

4.3. If data is transferred outside the user's country, we take steps to ensure the recipient provides an adequate level of protection and, where the law requires, obtain the necessary consents.

4.4. Data is processed for as long as the Platform is used and afterwards for the period necessary for the purposes of processing or required by law. The data of a company placed in the trash is deleted permanently once the trash retention period expires.

5. User rights

5.1. You have the right to:

- obtain information about what data of yours is processed;
- request correction, blocking or deletion of data;
- withdraw consent where processing is based on consent;
- lodge a complaint with the competent data protection authority.

5.2. If you are an employee or customer of a company that uses the Platform, contact that company first about your data; at its request we will help fulfil your request.

5.3. Withdrawing consent or deleting data may make it impossible to continue using the Platform, in whole or in part.

6. Data protection

6.1. We apply organizational and technical safeguards, including:

- isolating each company's data in a separate database schema and a separate area of file storage;
- encryption of request bodies between the workspace and the server, with replay protection;
- end-to-end encryption of the team's internal chats;
- storing passwords only as strong hashes (Argon2id) and a configurable password policy;
- encrypting keys and tokens of connected services in the database;
- two-factor authentication, IP address restrictions and limits on sign-in attempts;
- an action log and a request log for incident investigation.

6.2. No system can be absolutely secure, so we cannot guarantee complete security of data transmitted over the Internet. We notify of incidents affecting your data as required by law.

7. Cookies and technical data

7.1. We use strictly necessary cookies and browser storage: to keep your session (a secure cookie not accessible to scripts), remember the interface language and theme, and make push notifications

work.

7.2. If we start using analytics or advertising cookies, we will ask for consent and update this Policy.

7.3. You can restrict cookies in your browser settings, but some Platform features may then work incorrectly.

8. Changes to the Policy

8.1. The Operator may change the Policy. The new version is published on the website with its date; we additionally notify Platform users of material changes.

8.2. Continued use of the Platform after changes take effect means acceptance of the new version.

9. Final provisions

9.1. The Policy is governed by the law of the Operator’s place of registration unless mandatory law requires otherwise.

9.2. For questions about data processing, write to the contacts below.

The Operator's contact details are listed in the "Contact information" section on the document page: https://connectacrm.net/legal/privacy?v=1.0. The SHA-256 checksum of the file itself cannot be written inside the file, so it is published on the verification page: https://connectacrm.net/legal/verify.