GDPR Compliance Guide for Klozer.io

1. Introduction

Klozer.io is committed to protecting personal data and respecting privacy rights. This GDPR Compliance Guide explains how we collect, use, store, share, and protect personal data when you use our website, platform, and related services.

The General Data Protection Regulation applies to the processing of personal data of individuals in the European Union and gives individuals a set of rights over their personal data. The GDPR also sets expectations for controllers and processors, including how requests from individuals must be handled, how processors are engaged, how breaches are reported, and how transfers outside the EEA are managed.

2. About Klozer.io

Klozer.io provides cloud based call centre software and related communication tools. Depending on the context, Klozer.io may act as a controller or a processor. A controller determines the purposes and means of processing personal data, while a processor processes personal data on behalf of a controller.

When we process personal data for our own business purposes, such as account administration, billing, security, or website analytics, Klozer.io acts as a controller. When our customers use the platform to process contact lists, call logs, recordings, or related communication data, Klozer.io typically acts as a processor and the customer remains the controller.

3. Scope of This Guide

This guide applies to personal data processed through:

1. Our website and contact forms.
2. Customer accounts and subscriptions.
3. Platform usage, support interactions, and billing.
4. Call centre operations carried out by customers using Klozer.io.

The GDPR applies where personal data is processed in connection with offering goods or services to people in the Union, or monitoring their behaviour within the Union.

4. Personal Data We May Process

Depending on how you interact with Klozer.io, we may process the following categories of personal data.

Identity data, such as name, company name, and job title.
Contact data, such as email address, phone number, and business contact details.
Account data, such as login credentials, user roles, and subscription details.
Technical data, such as IP address, browser type, device identifiers, and operating system.
Usage data, such as feature activity, login history, session data, and platform interactions.
Communication data, such as call logs, call recordings, transcripts, and support messages.
Billing data, such as invoice details, payment records, and transaction history.

5. Why We Process Personal Data

We may process personal data for the following purposes.

To create and manage user accounts.
To provide and maintain our services.
To process payments and manage billing.
To provide customer support.
To secure the platform and prevent misuse.
To improve product performance and user experience.

To comply with legal obligations.
To send service related notices and important account communications.
To enable customers to use the platform for lawful communications and call centre operations.

6. Legal Bases for Processing
Under the GDPR, processing must have a lawful basis. Common bases include consent, contract performance, legal obligation, and legitimate interests. The GDPR also recognises that legitimate interests may be relied on where the controller's interests are not overridden by the rights and freedoms of the individual.
Klozer.io may process personal data on one or more of the following bases.
Consent, where you have clearly agreed to specific processing.
Contract performance, where processing is necessary to deliver the services you requested.
Legal obligation, where processing is required by law.
Legitimate interests, where processing is necessary for security, service improvement, fraud prevention, or business operations and those interests do not override your rights.

7. Data Protection Principles We Follow
We aim to process personal data in line with the GDPR principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.
We also apply data protection by design and by default. The European Commission explains that organisations should build data protection into the early stages of product design and use the most privacy friendly default settings where possible.

8. How We Share Personal Data
We may share personal data with trusted third party service providers that help us operate our business and deliver our services, such as hosting, payment processing, analytics, customer support, and communications infrastructure.
Where we use processors, we do so with appropriate contractual arrangements and only with processors that provide sufficient guarantees to implement suitable technical and organisational measures. The EDPB has also stated that controllers should have processor and sub processor details readily available so they can meet their Article 28 obligations.

9. International Data Transfers
Where personal data is transferred outside the European Economic Area, we use appropriate safeguards permitted under the GDPR. The European Commission has issued modernised Standard Contractual Clauses for transfers from controllers or processors in the EU or EEA to controllers or processors outside the EU or EEA.

10. Data Retention
We keep personal data only for as long as necessary for the purposes for which it was collected, or for as long as required by law, contract, or legitimate business need.
Retention periods may vary depending on the type of data, the service being used, customer settings, legal obligations, and security requirements. When data is no longer needed, we aim to delete, anonymise, or securely archive it.

11. Security Measures
We use technical and organisational measures designed to protect personal data against unauthorised access, loss, misuse, alteration, or disclosure. These measures may include access controls, authentication, encryption, audit logging, secure hosting, monitoring, and internal policies.

The GDPR requires security of processing to be appropriate to the risk, and the Commission and EDPB both emphasise security and design choices that protect personal data from the start.

12. Personal Data Breaches
If a personal data breach occurs, we will assess the incident and take appropriate action. Under the GDPR, where notification is required, the controller must notify the supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In some cases, affected individuals must also be informed.

13. Your GDPR Rights
The GDPR gives individuals a set of rights over their personal data. These include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object, and rights related to automated decision making and profiling.
Depending on the legal basis and the context of processing, you may also have the right to withdraw consent at any time. The controller must respond to requests and facilitate the exercise of these rights, and processors must assist the controller in doing so.
To exercise your rights, contact us using the details at the end of this guide. We may need to verify your identity before responding.

14. Cookies and Similar Technologies
Our website may use cookies and similar technologies to support essential functionality, measure performance, analyse usage, and improve the user experience.
Where required, we will provide a cookie banner or consent mechanism that lets you manage your preferences. You can also control cookies through your browser settings.

15. Customer Responsibilities
When customers use Klozer.io to upload, store, or process personal data, they are responsible for ensuring they have a lawful basis for doing so and for meeting their own privacy and telemarketing obligations.
Customers should make sure that they:
Obtain valid consent where required.
Provide appropriate notices to individuals.
Use the platform in a lawful and fair manner.
Set retention and recording settings responsibly.
Follow local rules that apply to calls, marketing, and communications.
Klozer.io provides tools and safeguards, but customers remain responsible for their own use of the platform and the data they choose to process.

16. Children’s Data
Our services are intended for business use and are not directed to children. We do not knowingly collect personal data from children for use of our services.

17. Data Processing Agreement
Where Klozer.io acts as a processor, we may provide a Data Processing Agreement that defines the rights and obligations of the controller and processor, including security measures, sub processing terms, and transfer safeguards. The GDPR requires controllers to use processors that provide sufficient guarantees and to define processor obligations in a contract or other legal act.

18. Supervisory Authority

If you are located in the European Economic Area, you have the right to lodge a complaint with your local data protection authority if you believe your personal data has been processed unlawfully.

19. Updates to This Guide
We may update this guide from time to time to reflect changes in our services, legal obligations, or data protection practices. When we do, we will update the revision date at the top of this page.

20. Contact Us
If you have questions, requests, or concerns about this GDPR Compliance Guide or our handling of personal data, please contact us at:
Email: privacy@klozer.io
Website: klozer.io