Privacy Policy Loopsie

What is this document?

Loopsie is a service created and controlled by KRNL S.r.l., a company incorporated under italian law: all Your data will be processed and stored within the European Economic Area. This means that, following art. 3 of European Reg. n. 679/2016 ("**General Data Protection Regulation**" or "**GDPR**"), Your personal data will be processed also in accordance with european data protection law.
Also note that if You are a citizen of the State of California, Section 11 will apply; if You are a citizen of the State of Illinois, then will apply Section 12.
Pursuant to art. 13 GDPR and in compliance with the principles contained therein, KRNL S.r.l. intends to inform each User (the "**User**", "**You**", "**Your**") about the processing of personal data collected through the Loopsie App (hereinafter the "**App**").

1. Who processes Your data?

Who is the data controller?
The data controller is the natural or legal person who determines the purposes and means of the data processing. It is, in fact, who collects and manages Your data and assumes the relevant responsibility provided by the law.

The data controller is KRNL S.r.l. ("**KRNL**" or the "**Controller**"), P.IVA: IT10287770969, registered office in Piazzale Libia 1, 20135, Milano (IT).

2. What data do we process?

- **Contact details** including: first name, last name, email address, phone number, ("**Contact Data**");
- **Navigation data**, such as: IP address, addresses in URI (Uniform Resource Identifier) notation of the requested resources, the time of the request, the method used in submitting the request to the server, the country set in the device settings, the size of the file obtained in response, the numerical code indicating the status of the response given by the server (successful, error, etc.), information about the user's interactions with the App and unique identifiers (i.e. IDFA or AAID) and other parameters related to the user's operating system and computing environment (**"Internet and Network Activity Information**").
- **Images** You upload to the App. In order to generate AI avatars the App needs access to the photo library and camera, but this requires specific permission through a request that will appear on Your phone. Note that the App does not use the Images provided by the users for identification or authorization purposes.

3. Assumptions and purposes for the data processing

What is the legal basis of the process?
The legal basis is the condition by which the company has the right to lawfully process personal data. For further information, please read art. 6 of the EU Regulation (UE) 2016/679 ("**GDPR**") at this link.

On what legal basis do we base the process?
There may be different legal basis that justify the process.

Consent: the process is carried out since the User expressed its consent.

Performance of a contract: the process is necessary to enter into or perform a contract.

Law obligation: the process is required by a specific provision of law.

Legitimate interest: the process is necessary to satisfy a legitimate interest. For each process grounded on such legal basis, we have carefully verified that Your rights and interest do not prevail our interest.

A) Creation and management of a personal User profile.

Legal basis: **Execution of contractual measures [Art. 6, 1, lett. b) GDPR]**

Storage period: Until the account is deleted, but no later than 24 months from the date of last contact.

B) Use of the Service

Legal basis: **Execution of contractual measures [Art. 6, 1, lett. b) GDPR]**

Storage period: Images are stored for no longer than 30 days after the upload.

C) Analyze Your usage information in order to improve our Services;

Legal basis: **Legitimate interest [Art. 6.1 f) GDPR]**

Storage period: The data used to improve our Services are immediately aggregated and anonymized.

D) Sending commercial communications via e-mail, concerning products and services similar to those purchased.

Legal basis: **Legitimate interest [Art. 6,1, lett. f) GDPR]**

Storage period: 12 months from cancellation of User profile

E) Profiling activities to analyze Your purchasing habits in order to address commercial proposals.

Legal basis: **Consent [Art. 6,1, lett. a) GDPR]**

Storage period: Until withdrawal of consent and in any case not later than 24 months from the date of last contact.

F) Allow the Controller to accomplish all formalities required by law.

Legal basis: **Legal obligation [Art. 6.1 lett. c) GDPR]**

Storage period: up to the time provided by a specific obligation or by the applicable provision of law.

G) Detecting or preventing fraudulent activity and exercising the Controller's rights in Court.

Legal basis: **Legitimate interest [Art. 6.1 lett. f) GDPR]**

Storage period: up to 10 years.

---

4. Processing methods

The procedure will be carried out using both automated and manual computer and telematic tools to ensure that appropriate security measures are in place, preventing unauthorized access, disclosure, loss, improper handling, illegal use, or any unauthorized use of data.

5. Place of data processing

Personal data are processed at the headquarters of the Controller, as well as in the servers that host the App. Personal data are stored on servers located in the EU. The Data Controller guarantees that when using cloud providers, services or platforms established outside the EEA, the processing of personal data by such recipients shall be made according to the applicable law. Transfers are made by means of appropriate safeguards, such as adequacy decisions, standard contractual clauses approved by the European Commission or other guarantees under the GDPR.

---

7. Who do we share Your data with?

Subjects who may learn Your personal data, to the extent strictly necessary to comply with the purposes indicated in paragraph 3, are formally appointed by the Data Controller. In addition to internal personnel - specifically authorized pursuant to art. 29 GDPR – in order to ensure the provision of the service, personal data may be disclosed to external parties that may act as independent data controllers or data processors. In particular, Your data may be communicated to:

- Internet service providers and platforms used by the Data Controller as organizational tools, communications channels and/or promotion;
- if we engage in a corporate transaction or operation, such as bankruptcy, merger, acquisition, reorganization, sale of assets or assignments, or any due diligence related to such transactions, we may disclose Your personal data to our advisers and the advisers of potential buyers. Your personal data may also be transferred to a new owner as part of the assets.
- authorities whose right of access to personal data is expressly recognized by law or regulations issued by the competent bodies.

The relationships with the subjects listed above are formalized with a contract pursuant to art. 28 GDPR (Appointment as Data Processor).

To find out who are the data processors appointed by KRNL S.r.l. You can contact us at email info@loopsie.it

---

8. I tuoi diritti privacy

💡**What are Your privacy rights?**
The GDPR grants important rights that You may exercise by contacting the Data Controller.
In order to carefully know Your rights You may read chapter 3 of the GDPR at this link.

You have the right to exercise the following rights:

- Right to access Your data;
- Right to rectification;
- Right to erasure and cancellation;
- Right to limit the process;
- Right of portability;
- Right to object;
- Right to file a complaint with the competent national authority (Data Protection Supervisor).

9. Who can You contact?

For any communication relating to the processing of Your data, including the exercise of Your rights, You can write to us by e-mail at: info@loopsie.it

---

10. Amendments

The Company reserves the right to amend, modify or simply update the content, in whole or in part, also due to changes in the applicable legislation. The Company shall inform Users of such changes as soon as they are introduced, and they shall be binding as soon as they are published on its website or otherwise transmitted. The Company therefore invites customers to pay attention to the latest version of the information displayed through these channels, in order to be always up to date on the data collected and the use made by us.

---

11. Additional information for California Consumers

This section contains supplementary information that is mandated by the California Consumer Privacy Act ("CCPA").

1. Additional Information Related to Collection, Use, and Disclosure of Personal Information

There are various ways to collect personal information, such as obtaining it directly from You (e.g. when You make purchases or participate in surveys or contests), automatically when You use the app (e.g. device information), and from other sources (e.g. mobile measurement partners). We also generate deductions about You based on Your use of the application and other information we gather.

In the preceding 12 months, we have collected the categories of personal information indicated in Section 2, in which there is also specified the purposes and the legal basis of our processing. Moreover, the Company collects personal information for the business and commercial purposes listed in the chart in Section 2 above.

In compliance with Section 7, we reserve the right to share Your personal information with third-party categories. For the last 12 months, we have disclosed various categories of personal information for business purposes, including identifiers, electronic network activity information, characteristics of protected classifications under California or U.S. federal law, commercial information, approximate geolocation information, audio and visual information, and other inferred information relating to or associated with You.

2. Rights of California Consumers

Subject to certain limitations, the CCPA provides California consumers the right to:

- Inquire for additional information regarding the types and specific details of personal data that we process..
- Ask for the removal of their personal information.
- Opt out of “sales” of personal information that may be occurring.
- Have the right not to face discrimination for exercising these privileges.

If You’re a California consumer, to exercise these rights, You can submit a request following the steps below:

- Tap Send a Privacy Request and follow the instructions.
- After You have sent Your request through Send a Privacy Request, You may uninstall the app if You don’t want to use it anymore.

In case You require any additional information on privacy or data protection at KRNL, feel free to get in touch with us via email at info@loopsie.it We

might need to authenticate Your request by asking You to provide details that correspond with the information we possess about You. Consumers from California can appoint an authorized representative to carry out these rights on their behalf, but we will need evidence of their authorization and may still require them to confirm their identity with us directly.

12. **Additional information for Illinois Consumers**

In accordance with Illinois law, this section provides additional disclosures related to Facial Data. As described in Section 2 above, we acquire and manage Facial Data for the purpose of creating AI avatars and, subject to Your authorization, to enhance our photo editing capabilities and refine our algorithms.. The Facial Data used to create new images is kept for a maximum of 7 days after Your most recent interaction with the AI avatar feature. However, if You have a subscription, the Facial Data may be kept for up to 30 days after Your last interaction with the AI avatar feature. The Facial Data You provide us with for the purpose of enhancing our photo editing capabilities and refining our algorithms will be held for a period of 24 months from the day You submitted the image that the Facial Data was obtained from. We use cloud storage providers to store Facial Data. We will never sell, lease, or trade Facial Data to third parties. As described above, Facial Data may be considered biometric data in some jurisdictions; however, Facial Data is not used for identification or authentication purposes.