Uup anonymous - Privacy Policy

1. Introduction

This Privacy Policy sets out how we, **DTSocialize LTD** (Registration number C 87045), based in MALTA - Kathleen Court Trip il-Kappucini, Flat 1, Zabbar (hereinafter: "DTSocialize" or “Uup”), through the "Uup" application (of hereinafter: "**Application**" or "**Uup**"), use and protect your personal data that you provide to us, or that is otherwise obtained or generated by us, in connection with your use of our cloud-based messaging services (the **“Services”**). For the purposes of this Privacy Policy, **‘we’**, **‘us’** and **‘our’** refers to UupSocial, and **‘you’**refers to you, the user of the Services.

1.1 Privacy Principles

DTSocialize has two fundamental principles when it comes to collecting and processing private data:

- We don't use your data to show you ads.
- We only store the data that Uup needs to function as a secure and feature-rich messaging service.

1.2. Table of Contents

This Privacy Policy explains the following:

- the legal basis for processing your personal data;
- what personal data we may collect from you;
- how we keep your personal data safe;
- what we may use your personal data for;
- who your personal data may be shared with; and
- your rights regarding your personal data.

2. Legal Ground for Processing Your Personal Data

We process your personal data on the ground that such processing is necessary to further our legitimate interests (including: *(1)* providing effective and innovative Services to our users; and *(2)* to detect, prevent or otherwise address fraud or security issues in respect of our provision of Services), unless those interests are overridden by your interest or fundamental rights and freedoms that require the protections of personal data.

When the User downloads the App, a pair of cryptographic keys is generated, and it is by forwarding the Public Key to their contacts that it will be possible to start a conversation. All data generated by the App, including messages received and sent, photos, audio, video and geolocation data are encrypted by asymmetric encryption algorithms and certified with a digital signature to avoid counterfeiting. Therefore, the authorization to access the microphone, camera and GPS that is requested from the User is of a purely technical nature, as it is necessary for the use of the specific hardware of the device that allows you to use the service.

The Private Keys always remain in the device of the User who downloaded Uup, but the App cannot access or decrypt the information in the infrastructure of the User's devices.

3. What Personal Data We Use

3.1. Basic Account Data

Uup is a communication service. In order to use Uup and have an account, you do not need to provide any basic account data such as your email, phone number or any other information that is attributable to you. You do not provide any basic account data either (which may include profile name, profile picture and about information) to create an Uup account, you just create a profile with your username. Uup does not require any access to your address book in order for you to communicate with other users of Uup.

The only data that we will use and process will be your username and profile photo (if you decide upload one). To make it easier for the people to reach you and recognize you, the screen name you choose, your profile pictures, and your username (that you choose) on Uup are always public. We don't want to know your real name, gender, age or what you like.

We do **not** require your screen name to be your real name. Note that users who have you in their contacts will see you by your screen name. This way your father can have the public name 'James Bond' while appearing as 'Father' to you and as 'The Boss' to her underlings at work (or the other way around, depending on how these relationships are structured).

3.2. Your Messages

3.2.1. Cloud Chats

Uup is a cloud service. We store messages, photos, videos and documents from your *cloud chats* on our servers so that you can access your data from any of your devices anytime without having to rely on third-party backups. All data is stored heavily encrypted and the encryption keys in each case are stored in several other data centers in different jurisdictions. This way local engineers or physical intruders cannot get access to user data.

For the Uup Web version (Desktop version), in order to access your account, you will need to scan the QR code. In the Web version, you will only be able to see the last 2 months' data.

3.2.3. Media in Secret Chats

When you send photos, videos or files via secret chats, before being uploaded, each item is encrypted with a separate key, not known to the server. After the files are uploaded to the server, URL is sent in a message format. Please be informed that URLs are not publicly available and only authorise users can have access to them.

3.4. Phone Number and Contacts

Uup does not use phone numbers as unique identifiers hence we will never ask to sync your contacts.

3.5. Location Data

If you share a location in a chat, this location data is treated like other messages in cloud or secret chats respectively. Uup does not have the live location function, in order to share your location, you will need to pinpoint your location on the map and share it.

3.6. Cookies

The only cookies we use are those to operate and provide our Services on the web. We do not use cookies for profiling or advertising. The cookies we use are small text files that allow us to provide and customize our Services, and in doing so provide you with an enhanced user experience. Your browser should allow you to control these cookies, including whether or not to accept them and how to remove them. You may choose to block cookies with your web browser, however, if you do disable these cookies you will not be able to log in to Uup Web.

4. Keeping Your Personal Data Safe

4.1. Storing Data

Your data is stored in data centers in Germany. These are third-party provided data centers in which Uup rents a designated space. However, the servers and networks that sit inside these data centers and on which your personal data is stored are owned by Uup. As such, we do not share your personal data with such data centers. All data is stored heavily encrypted so that local Uup engineers or physical intruders cannot get access.

4.2. End-to-End Encrypted Data

Your messages, media and files from secret chats (see section 3.3.2 above), as well as the data you store in your Uup account are processed only on your device and on the device of your recipient. Before this data reaches our servers, it is encrypted with a key known only to you and the recipient. While Uup servers will handle this end-to-end encrypted data to deliver it to the recipient – or store it in the case of Uup data, we have no ways of deciphering the actual information. The Uup Super Admin will have the functionality to decrypt the messages of Uup users however you, as the user, can turn off this functionality from the Settings tab. If you decide to disable this functionality, your messages will not be decrypted by Uup.

4.3. Retention

Unless stated otherwise in this Privacy Policy, the personal data that you provide us will only be stored for as long as it is necessary for us to fulfill our obligations in respect of the provision of the Services.

5. Processing Your Personal Data

5.1. Our Services

Uup is a cloud service. We will process your data to deliver your cloud chat history, including messages, media and files, to any devices of your choosing without a need for you to use third-party backups or cloud storage.

5.2. Safety and Security

Uup supports massive communities which we have to police against abuse and Terms of Service violations. Uup also will have a lot of users which makes it a lucrative target for spammers. To improve the security of your account, as well as to prevent spam, abuse, and other violations of our Terms of Service, we may collect metadata such as your IP address, devices and Uup apps you have used, history of username changes, etc. If collected, this metadata can be kept for 12 months maximum.

5.4. Cross-Device Functionality

We may also store some aggregated metadata to create Uup features (see section 5.5 below) that work across all your devices.

5.5. Advanced features

We may use some aggregated data about how you use Uup to build useful features.

5.6. No Ads Based on User Data

Unlike other services, we don't use your data for ad targeting or other commercial purposes. Uup only stores the information it needs to function as a secure and feature-rich cloud service.

6. Who Your Personal Data May Be Shared With

6.1. Other Uup Users

Other users of our Services with whom you choose to communicate with and share certain information, who may be located outside the EEA. Note that by entering into the Terms of Service and choosing to communicate with such other users of

Uup, you are instructing us to transfer your personal data, on your behalf, to those users in accordance with this Privacy Policy. We employ all appropriate technical and organizational measures (including encryption of your personal data) to ensure a level of security for your personal data that is appropriate to the risk.

6.3. Law Enforcement Authorities

If Uup receives a court order that confirms you are a terror suspect, we may disclose your IP address to the relevant authorities.

7. Your Rights Regarding the Personal Data You Provide to Us

7.1. Your Rights

Under applicable data protection legislation, in certain circumstances, you have rights concerning your personal data. You have a right to: *(1)* request a copy of all your personal data that we store and to transmit that copy to another data controller; *(2)* delete or amend your personal data; *(3)* restrict, or object to, the processing of your personal data; *(4)* correct any inaccurate or incomplete personal data we hold on you; and *(5)* lodge a complaint with national data protection authorities regarding our processing of your personal data.

7.2. Exercising Your Rights

If you wish to exercise any of these rights, kindly contact us using the detail below: privacy@dtsmail.tech

8. Deleting data

8.1. Accounts

If you would like to delete your account, you can do this by contacting customer support through your account in the App. This action cannot be undone.

8.2. Messages

- In secret chats, deleting a message always instructs the app on the other end to delete it too.
- In cloud chats, supergroups and channels, the receiving side can choose to delete a message from the message history within at least 15 minutes after receiving. Deleting a message will delete it from your message history, which means that the message is gone forever.

9. Changes to this Privacy Policy

We will review and may update this Privacy Policy from time to time. Any changes to this Privacy Policy will become effective when we post the revised Privacy Policy. Please check our website frequently to see any updates or changes to our Privacy Policy, a summary of which we will set out below.

Important changes made to this Privacy Policy will be notified to you via Uup.

10. Questions and concerns

If you have any questions about privacy and our data policies, please contact our support team.