CRYPE Privacy Policy

General

CRYPE offers users a service for exchanging multimedia data with other end devices via a secure, encrypted connection. The privacy policy explains how CRYPE uses and protects personal data provided for the execution of the CRYPE service.

Data protection by design

The CRYPE design has the following basic principles for a trustworthy use of this service:

- CRYPE can be used completely anonymously as a guest or as a registered user.
- All user data exchange and storage takes place exclusively in encrypted form. Communication data is exchanged directly between the respective users' end devices wherever technically possible.
- CRYPE only stores information for registered users that is either absolutely necessary for the operation of the CRYPE service or that has been explicitly provided or released by the user.
- CRYPE only publishes data in the public CRYPE contact directory that is either required to be publicly available or has been explicitly authorized for public use by the CRYPE user.
- CRYPE does not store communication content on central servers, neither permanently nor temporarily. If a direct peer-to-peer connection between end devices is technically not possible, encrypted communication data may be transmitted via TURN/T2T infrastructure solely as a relay for the active connection. No intermediate storage of communication content takes place on TURN/T2T systems.

Data Protection Contact for the EEA

If you are located in a country of the European Economic Area (EEA) and the General Data Protection Regulation (GDPR) applies, our designated data protection contact can be reached at: scs.dpo@crype.eu

Processing of your personal data

We process your personal data on the basis that such processing is necessary to provide the CRYPE Services and to detect and prevent fraud or security issues.

Guest user

CRYPE services can be used as a guest without providing personal data. In this case, the user enters an anonymous username and confirms the terms of use for this service. As a guest user, session-related data is processed only for the duration of the active session or locally on the device and is automatically deleted when the service is properly terminated.

Registered users

The user provides their email address along with the basic mandatory account details to create a CRYPE account. The registration process differs between a private account and an organization (business) account. In a business account, more information can be entered and published in the CRYPE directory.

During user registration, mandatory fields must be filled in, which are marked with an asterisk (*) in the upper right corner. All other fields can be left blank or filled in with data. If an open lock symbol appears next to an input field, this data will always be published in the central CRYPE directory. For all other profile data entered, the user can choose at any time whether to allow or prevent its publication.

Automatic account deletion

If a user no longer uses CRYPE and has not been online for at least 6 months, the account will be deleted automatically.

CRYPE contact directory - Profile data

Any type of profile data provided and shared by the user will be published in the global CRYPE contact directory. Other participants can search for and find additional CRYPE users there to add them to their personal CRYPE contact book.

For each account type (Private User, Organization – Division – Members), certain mandatory details must be entered in the profile. These required fields are marked with an asterisk (*), for example: **Name of organization ***

Additional input fields can be filled in optionally. On the right side of each data field, a symbol appears with the following meaning:

This information is always published by CRYPE in the CRYPE contact directory.

This information is never published by CRYPE in the CRYPE contact directory.

This information has been released for public visibility.

This information has been blocked from publication by the user.

In the CRYPE contact directory, a user can search for all data that has been published or shared by users or by CRYPE. All profile data that has not been shared by the user is stored in encrypted form on central servers in the data center.

Personal CRYPE contact book

Each user's personal contact book in CRYPE is stored exclusively on local devices in encrypted form. These data can be manually synchronized with other devices of the user.

Communication and Data Transmission

For all types of communication, CRYPE uses a **Peer-to-Peer (P2P)** network connection, directly between end devices via a private encrypted communication channel.

If a direct connection between end devices is not possible due to firewall or NAT settings, media information is relayed through a TURN server (T2T) as a gateway to enable a secure encrypted connection between the end devices. The TURN/T2T infrastructure acts solely as a transmission relay during the active session and does not store the communication content**.** Statistically, this is required for approximately 20–30% of connections.

During a **live video or audio call**, the user can immediately see after the connection is established which type of connection is being used with a communication partner.

Due to the nature of **secure P2P technology**, CRYPE **never stores messages, photos, videos, or documents from your chats on central CRYPE servers. All user data exchange and storage takes place exclusively in encrypted form and, where applicable, directly between the respective users' end devices.**

Push Notifications

On Android and iOS devices, CRYPE may use the operating system push notification services solely to inform users that a call, message, or other communication event is waiting. The push notification itself does not contain the communication content. Message content, documents, and call data are not transmitted via push notification and are only retrieved directly by the user's device after the user opens the app.

For this purpose, CRYPE may use technical notification identifiers or push tokens provided by the respective operating system or push service solely to deliver such notifications.

User Email Addresses

CRYPE uses email addresses as unique identifiers for internal communication with users. Such information is treated confidentially unless explicitly shared by the user.

Cookies / Tracking

CRYPE does not use cookies for app-based tracking and does not use third-party advertising tracking tools within the app. CRYPE does not use personal data for third-party advertising purposes.

Secure storage of your personal data

Data Storage

CRYPE does not store communication content or communication history on central CRYPE servers. IP addresses and device-related network information may be technically required during connection establishment, peer-to-peer mediation, TURN/T2T relay, fraud prevention, and operational security. Such data is used only as technically necessary for providing and securing the service and not for creating communication profiles.

What we definitely do not store – not even temporarily for statistical purposes:

- Communication content such as messages, photos, videos, documents, audio, or video calls
- Communication history in the sense of centrally stored records of who communicated with whom, when, and what was communicated
- Personal contact books
- Personal profile pictures (avatars), unless explicitly published by the user as profile data

In the central CRYPE contact directory, which allows you to find other users, all data is encrypted unless it has been explicitly shared by you in your profile.

Our servers are hosted exclusively in secure data centers certified according to ISO/IEC 27001.

Encryption

All user communication with the CRYPE service is **secured with 256-bit TLS/DTLS encryption**. Additionally, SRTP encryption is used for all forms of data communication between users.

Technical details about encryption algorithms, protocols used, and ports can be downloaded from the CRYPE website: www.crype.eu under the Downloads section.

Peer-to-Peer Mediation

CRYPE is a Peer-to-Peer (P2P) service and **acts only as a mediator** for communication between different participants. **CRYPE does not store the communication content of its users.**

Furthermore, CRYPE only processes the technical mediation data necessary to enable an efficient and secure communication service.

Information to Users and User-Published Profile Content

CRYPE does not share personal data with third parties. CRYPE may use account-related contact data to provide service-related information to CRYPE users.

CRYPE users can independently publish advertising within their profile data. These advertisements are only shown to other CRYPE users who specifically search for them in the CRYPE contact book or if the contact is saved in their personal contact book.

Other Collected User Data

To provide, maintain, and secure the CRYPE services, CRYPE may process limited technical information about the user's device and application environment, including app version, operating system, browser type/version where applicable, and technical parameters of display, audio, or video components where necessary for compatibility, call setup, troubleshooting, and service security.

- App version
- Operating system
- Browser type and version
- Technical parameters of the display device, where necessary for the use of CRYPE
- Technical parameters of communication devices (video/audio)

Your Rights Regarding the Personal Data You Provide to Us

Under applicable data protection laws, you have certain rights regarding your personal data.

Your rights:	You can exercise these rights as follows:
Request information about the personal data stored by us	All personal data that we store can be viewed in your own profile. No other personal data is stored
Delete or modify personal data	All personal data can be modified or deleted in the profile. If this is not possible, the CRYPE account can be completely deleted. This results in the deletion of the stored account data associated with the CRYPE service.
Restricting or objecting to the processing of personal data	As part of the CRYPE service, personal data must be processed. To restrict or object to this, such data can be deleted from the profile or the CRYPE account can be fully removed.
Correct inaccurate or incomplete personal data	All personal information is under the user's control and responsibility. Users can independently modify, complete, or delete their data at any time
Filing a complaint about the processing of personal data with national data protection authorities	By agreeing to the terms of use, users consent to the processing of their data to the extent necessary for the provision of the CRYPE service. Without this consent, the CRYPE service cannot be used. Consent can be revoked by deleting the CRYPE account. This will erase all data, making any further processing of personal data naturally impossible.
Contact the CRYPE Data Protection Contact	The CRYPE Data Protection Officer can be reached at scs.dpo@crype.eu

CRYPE customer service

SCS employees may have access, to the extent necessary, to operationally relevant systems and stored data in order to ensure the secure operation of the CRYPE services. All SCS service employees are trained in the responsible and sensitive handling of personal data and are legally bound in writing to comply with applicable data protection regulations.

It is ensured that no employee has access to CRYPE data without signing a confidentiality agreement and acknowledging their legal liability in case of a violation.

Email: mail@crype.eu