NATO HQ SACT Innovation Branch Matrix Homeserver Privacy Notice

Please read this document carefully before accessing or using this service!

1. Introduction

1.1 English, Not Legalese

Most Terms of Use and Privacy Policy documents are unreadable. They are written by lawyers and for lawyers, and in our opinion are not very effective.

Data privacy is important, and we want you to understand the issues involved. For that reason we decided to use plain English instead as much as possible, to make our terms as clear as possible. Some sections still have room for improvement - we plan to tackle these over time.

Where you read 'the NATO HQ SACT Innovation Branch homeserver' or 'the Service' below, it refers to the services made available at https://matrix.ilab.zone which store your account and personal conversation history, provide integrations such as bots and bridges, and communicate via the open Matrix decentralised communication protocol.

Innovation Hub ACT is the Data Processor for the Service. We can be contacted as per the details below:

Email: info@innovationhub-act.org

1.2 Scope of This Document

This document explains Data Privacy to the Users of the NATO HQ SACT Innovation Branch homeserver.

1.3 The User Definition

Put simply, if you have an account registered on the NATO HQ SACT Innovation Branch homeserver that you use to send and receive messages, you're a User.

1.4 Using The Service Means Accepting These Terms

By accessing or using the Service in any way, whether you have created a Matrix account on the NATO HQ SACT Innovation Branch homeserver, or whether you are accessing content federated from the NATO HQ SACT Innovation Branch homeserver to another Matrix homeserver, or are just browsing rooms as an unauthenticated guest, you agree to and are bound by the terms and conditions written in this document.

If you do not agree to all of the terms and conditions contained in this document, please use a Matrix server provided by someone else and refrain from accessing content federated from this server.

2. Access to Your Data / Privacy Policy

2.1 What is the legal basis for processing my data and how does this affect my rights under GDPR (General Data Protection Regulation)?

2.1.1 Legal Basis for Processing

NATO HQ SACT Innovation Branch processes your data under *Legitimate Interest*. This means that we process your data only as necessary to deliver the Service, and in a manner that you understand and expect.

The *Legitimate Interest* of our Service is the hosting and management of the NATO HQ SACT Innovation Branch Matrix homeserver, providing decentralised, openly-federatable and (optionally) end-to-end encrypted communication services. The processing of user data we undertake is necessary to provide the Service. The nature of the Service and its implementation results in some caveats concerning this processing, particularly in terms of GDPR Article 17 *Right to Erasure (Right to be Forgotten)*. We believe these caveats (discussed in the section below in detail) are in line with the broader societal interests served by providing the Service.

In situations where the interests of the individual appear to be in conflict with the broader societal interests, we will seek to reconcile those differences guided by our Exceptional Erasure Policy.

2.1.2 Data Ownership

NATO HQ SACT Innovation Branch owns and controls all messages and files submitted to the homeserver by User accounts registered on the homeserver. This ownership does not extent to messages and files submitted over federation or bridging.

This means that, in addition to the usual data access controls defined by the Matrix protocol, all unencrypted messages and files can be accessed by NATO HQ SACT Innovation Branch, and that access will be retained even after no User account within the system retains access to the data.

2.1.3 Right to Erasure

You can request that the Data Controller (see above) forget your copy of messages and files by instructing them to deactivate your account (using a matrix client such as https://element.ilab.zone) and selecting the option instructing them to forget your messages. What happens next depends on who else had access to the messages and files you had shared.

Any messages or files that were only accessible by your account will remain accessible to the NATO HQ SACT Innovation Branch for the duration of the homeserver. These messages and files will be inaccessible to all other Users.

Where you shared messages or files with another registered Matrix user, that user will still have access to their copy of those messages or files. Apart from state events (see below), these messages and files will *not* be shared with any unregistered or new users who view the room after we have processed your request to be forgotten.

State events are processed differently to non-state events. State events are used by the Service to record, amongst other things, your membership in a room, the configuration of room settings, your changing of another user's power level and your banning a user from a room. Were we to erase these state events from a room entirely, it would be very damaging to other users' experience of the room, causing banned users to become unbanned, revoking legitimate administrator privileges, etc. We therefore share state events sent by your account with all non-essential data removed ('redacted'), even after we have processed your request to be forgotten. This means that your username will continue to be publicly associated with rooms in which you have participated, even after we have processed your request to be forgotten. We are actively working on a solution to work around this restriction and allow you to be fully forgotten while maintaining a high quality experience for other users. If this is not acceptable to you, please do not use the Service.

2.1.4 Data Portability

Under GDPR you have a right to request a copy of your data in a commonly-accepted format. If you would like a copy of your data, please send a request to the Data Controller (see above).

2.1.5 Your Rights as Data Subject

You have rights in relation to the personal data we hold about you. Some of these only apply in certain circumstances. Some of these rights are explored in more detail elsewhere in this document. For completeness, your rights under GDPR are:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

If you have any questions or are unsure how to exercise your rights, please contact us at info@innovationhub-act.org.

2.2 What Information Do You Collect About Me and Why?

The information we collect is purely for the purpose of providing your communication service via Matrix. We do not profile users or their data on the Service.

Be aware that while we do not profile users on the Service, Matrix clients may gather usage data - for instance Element (the Matrix client provided by Element) optionally gathers anonymised opt-in usage data in order to improve the app.

2.2.1 Information you provide to us:

We collect information about you when you input it into the Service or otherwise provide it directly to us, and process it in accordance with the Customer's instructions.

Account and Profile Information

We collect information about you when you register for an account. This information is kept to a minimum on purpose, and is restricted to:

- Username
- Password
- Display Name (if you choose to provide one)
- Your email address (if you choose to provide it)
- Your verified telephone number (if you choose to provide it)

Your username and password is used to authenticate your access to the Service and to uniquely identify you within the Service.

Your email address and/or telephone number, if you choose to provide them, are used so that other users can look up your Matrix ID from these identifiers. We will also use your email address to let you reset your password if you forget it, and to send you notifications about missed messages from users trying to contact you on Matrix if you enable the option. We may also send you infrequent urgent messages about platform updates.

Content you provide through using the Service

We store and distribute the messages and files you share using the Service (and across the wider Matrix ecosystem via federation) as described by the Matrix protocol. Storing and sharing this content is the reason the Service exists.

This content includes any information about yourself that you choose to share.

2.2.2 Information we collect automatically as you use the service:

Device and Connection Information

Each device you use to access the Service is allocated a (user-configurable) identifier. When you access the Service, we record the device identifier, the IP address it used to connect, user agent, and the time at which it last connected to the service.

This information is gathered to help you to manage your devices - you can view and manage the list of devices by connecting to the Service with a Matrix client such as https://element.ilab.zone.

Currently, we log the IP addresses of everyone who accesses the Service. This data is used in order to mitigate abuse, debug operational issues, and monitor traffic patterns. Our logs are kept for not longer than 180 days.

2.3 What Information is Shared With Third Parties and Why?

2.3.1 Sharing Data with Connected Services

The NATO HQ SACT Innovation Branch homeserver is a *decentralised* and, if federation is enabled, *open* service. As federation is enabled, to support communication between users on different homeservers or different messaging platforms, your username, display name and messages and files are sometimes shared with other services that are connected with the NATO HQ SACT Innovation Branch homeserver.

Federation

As federation is enabled on the NATO HQ SACT Innovation Branch homeserver, user data will be shared with the wider ecosystem over federation:

- When you send messages or files in a room, a copy of the data is sent to all participants in the room. If these participants are on remote homeservers, your username, display name, messages and files may be replicated across each participating homeserver.

- We will forget your copy of your data upon your request. We will also forward your request to be forgotten onto federated homeservers. However - these homeservers are outside our span of control, so we cannot guarantee they will forget your data.

- Federated homeservers can be located anywhere in the world, and are subject to local laws and regulations.

Access control settings are shared between homeservers, as well as any requests to remove messages by "redactions", or remove personal data under GDPR Article 17 *Right to Erasure (Right to be Forgotten)*. Federated homeservers and Matrix clients which respect the Matrix protocol are asked to honour these controls and redaction/erasure requests, but other federated homeservers are outside of the span of control of NATO HQ SACT Innovation Branch, and we cannot guarantee how this data will be processed. Federated homeservers can also be located in any territory, and will be subject to the local regulations of that territory. We recommend the use of end-to-end encryption to protect your message and file data over federation.

If the way in which data is shared is not acceptable to you, please use a different server or service.

Bridging

Some Matrix rooms are bridged to third-party services, such as IRC networks, twitter or email. When a room has been bridged, your username, display name, messages and file transfers may be duplicated on the bridged service where supported.

- It may not be technically possible to support your management of your data once it has been copied onto a bridged service.

- Bridged services can be located anywhere in the world, and are subject to local laws and regulations.

Access control settings, requests to remove messages by "redactions" or remove personal data under GDPR Article 17 *Right to Erasure (Right to be Forgotten)* are shared to bridging services, which are expected to honour them to the best of their ability. Be aware that not all bridged networks or bridges support the necessary technical capabilities to limit, remove or erase messages. If this is not acceptable to you, please do not use bridged rooms.

Integration Services (Bots and Widgets)

The NATO HQ SACT Innovation Branch homeserver provides a range of integrations in the form of Widgets (miniature web applications accessed as part of a Matrix Client) and Bots (automated participants in rooms). Bots and Widgets currently have access to all the messages and files in any room in which they participate, although we are adding a more sophisticated access control system.

2.4 Sharing Data in Compliance with Enforcement Requests and Applicable Laws; Enforcement of Our Rights

In exceptional circumstances, we may share information about you with a third party if we believe that sharing is reasonably necessary to

(a) comply with any applicable law, regulation, legal process or governmental request,

(b) protect the security or integrity of our products and services (e.g. for a security audit),

(c) protect NATO HQ SACT Innovation Branch and our users from harm or illegal activities, or

(d) respond to an emergency which we believe in good faith requires us to disclose information to assist in preventing the serious bodily harm of any person.

2.5 How Do You Handle Passwords?

We never store password data in plain text; instead they are stored hashed (with at least 12 rounds of bcrypt, including both a salt and a server-side pepper secret). Passwords sent to the server are encrypted using SSL.

It is your sole responsibility to keep your user name, password and other sensitive information confidential. Actions taken using your credentials shall be deemed to be actions taken by you, with all consequences including service termination, civil and criminal penalties.

If you become aware of any unauthorised use of your account or any other breach of security, you must notify NATO HQ SACT Innovation Branch immediately. Suspicious devices can be deleted using the User Settings management tools in a Matrix client such as https://

element.ilab.zone, and users should manage good password hygiene (e.g. using a password manager) and change their password if they believe their account is compromised.

If you forget your password (and you have registered an email address) you can use the password reset facility to reset it.

You can manage your account by using a Matrix client such as https://element.ilab.zone.

We will never change a password for you.

2.6 Our Commitment to Children's Privacy

We never knowingly collect or maintain information in the Service from those we know are under 16, and no part of the Service is structured to attract anyone under 16. If you are under 16, please do not use the Service.

2.7 How Can I Access or Correct My Information?

You can access all your personally identifiable information that we collect by using any compatible Matrix client (such as https://element.ilab.zone) and managing your User Settings. You can download a copy of all your data as per section 2.1.3.

2.8 Who Can See My Messages and Files?

All unencrypted messages and files submitted to the homeserver are visible to the NATO HQ SACT Innovation Branch.

In unencrypted and encrypted rooms, users connecting to the NATO HQ SACT Innovation Branch homeserver (directly or over federation) will be able to see messages and files according to the access permissions configuration of the relevant room. This data is stored in the format it was received on our servers, and can be viewed by NATO HQ SACT Innovation Branch engineers (employees and contractors) under the conditions outlined below.

In encrypted rooms, the data is stored in our databases but the encryption keys are stored only on your devices or by yourself. We allow users to optionally backup an encrypted copy of their keys on the Service to aid recovery if they lose all their keys and devices. This key backup would be encrypted by a recovery key that only the user has access to. This means that nobody, even NATO HQ SACT Innovation Branch engineers (employees and contractors) can see your message content in our database, and if you lose access to your encryption keys you lose access to your messages forever.

We use HTTPS to transfer all data. End-to-end encrypted messaging data is stored encrypted using AES-256, using message keys generated using the Olm and Megolm cryptographic ratchets.

2.9 What Are the Guidelines NATO HQ SACT Innovation Branch Follows When Accessing My Data?

- We restrict who at NATO HQ SACT Innovation Branch (employees and contractors) can access user data to roles which require access in order to maintain the health of the Service.

- We never share what we see with other users or the general public.

3. Making a Complaint

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention at info@innovationhub-act.org if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.