



RECOVER e-Hub Privacy Policy

Privacy information for visitors and members

Document detail	Information
Controller	Kovos su prekyba žmonėmis ir išnaudojimu centras, VšĮ (KOPŽI)
Company code	304486353
Registered address	Draugystės g. 8F-236, LT-51264 Kaunas, Lithuania
Service	RECOVER e-Hub at ehub.recover-project.eu
Version	1.0
Last updated	22 October 2026
Effective date	Effective upon publication

This Privacy Policy explains what personal data the RECOVER e-Hub processes, why it is processed, who may receive it, how long it is kept, and how you can exercise your rights under the General Data Protection Regulation (GDPR).

The e-Hub is a member community. Community content and member profiles are available only to authenticated members. Public pages such as registration, login, this policy, and other information pages may remain accessible without an account.

Controller contact: info@recover-project.eu

Contents

1. At a glance
2. Scope and service boundaries
3. Controller and contact
4. Who may use the e-Hub
5. Personal data we process
6. Why we process data and legal bases
7. Sensitive information and survivor confidentiality
8. Visibility and member content
9. Cookies and analytics
10. Service providers and data recipients
11. International data transfers
12. Retention and deletion schedule
13. Security and confidentiality
14. Your data protection rights
15. Account closure and historical content
16. Service communications
17. Children
18. Automated decision making and AI
19. Changes to this Policy
20. Complaints and further contact

This policy should be read together with the RECOVER e-Hub Terms of Use and Community Guidelines. If those documents describe member conduct or content rules, this Policy remains the governing document for personal-data processing.

1. At a glance

KOPŽI operates the RECOVER e-Hub as a professional online community for people and organisations interested in recovery and reintegration work connected with trafficking and exploitation. The service supports member profiles, discussions, questions and answers, resources, uploads, comments, reactions, follows, notifications, moderation, reporting, and account support.

- KOPŽI is the sole data controller for the e-Hub and can be contacted at info@recover-project.eu.
- Accounts are available only to people aged 18 or older. The service is not intended for children.
- Member profiles and community content are intended to be visible only to authenticated e-Hub members.
- The e-Hub must not be used to upload or disclose identifiable information about survivors, clients, witnesses, suspects, or service users.
- Analytics cookies are used only after consent. The e-Hub does not use newsletters, behavioural advertising, AI decision-making, or profiling for advertising.
- Personal data is normally kept for no longer than 24 months after account closure or the last active use, unless a longer period is required for legal, security, or claims purposes. Historical member content may remain after account deletion.

2. Scope and service boundaries

This Policy applies to personal data processed through the RECOVER e-Hub at ehub.recover-project.eu, including registration, login, password reset, member profiles, groups, discussions, questions and answers, resource pages, document and media uploads, comments, votes or reactions, follows, notifications, moderation, reporting, security, support, and service measurement.

This Policy does not apply to third-party websites or services linked from the e-Hub when those services have their own controller and privacy notice. A link does not make KOPŽI responsible for another organisation's processing.

The e-Hub is not an emergency service, clinical service, legal service, case-management system, or secure channel for exchanging identifiable survivor or client case files.

3. Controller and contact

For the purposes of the GDPR, the data controller is:

Item	Details
Legal name	Kovos su prekyba žmonėmis ir išnaudojimu centras, VšĮ (KOPŽI)
Company code	304486353
Registered address	Draugystės g. 8F-236, LT-51264 Kaunas, Lithuania
Privacy and rights requests	info@recover-project.eu
Website	ehub.recover-project.eu

KOPŽI determines the purposes and means of processing for the e-Hub. Authorised KMOP personnel may have limited administrative or support access where necessary for the operation, security, support, or governance of the service, subject to confidentiality and access controls established by KOPŽI.

For privacy questions, rights requests, or security concerns, email info@recover-project.eu. Do not send passwords, reset codes, or identifiable survivor or client information by ordinary email.

4. Who may use the e-Hub

The e-Hub may be used by any person who is at least 18 years old and accepts the applicable terms and community rules. The service is intended primarily for professional, educational, research, policy, civil-society, and other stakeholder participation, but eligibility is not limited to one profession or organisation type.

You are responsible for providing accurate registration information and for keeping your login credentials confidential. You must not create an account for another person or use the service in a way that violates applicable law or another person's rights.

5. Personal data we process

Category	Examples	How it is used and who can see it
Account and authentication	Username, email address, password hash, account ID, registration date, login and recovery records.	To create and secure your account. Email address, password data, and recovery records are restricted to authorised administrators and service providers. Other members do not see your password or email address.
Professional profile	Name, organisation, role, country, biography, profile image, languages, and other fields you choose to provide.	To help members identify and connect with one another. Profile information is available only to authenticated members, subject to the visibility settings and fields provided by the service.
Member content	Posts, questions, answers, comments, resources, documents, images, links, reactions, votes, follows, and edits.	To operate the community and preserve useful discussions. Content is intended for authenticated members and may remain as historical content after account closure.
Community and notification activity	Group membership, follows, reactions, subscriptions, notification preferences, and activity records.	To deliver requested community functions, notifications, and moderation. Access is limited to the people and systems that need it.
Moderation and reports	Reports, reasons, evidence, reporter details, decisions, restrictions, appeals, and related notes.	To enforce the rules, protect members, investigate abuse, and respond to safety or legal concerns. These records are restricted to authorised personnel.
Technical and security data	IP address, timestamps, browser and device information, session data, requested URLs, login attempts, CAPTCHA and security events, and error logs.	To operate, secure, troubleshoot, and improve the service. This information is not displayed as member content.
Consent and communications data	Cookie choices, analytics consent, service-message delivery status, and correspondence about support or rights requests.	To record choices, send necessary service messages, and handle requests. The e-Hub does not send newsletters.

We do not intentionally collect or request special-category personal data through the e-Hub. You must not upload it or include it in a profile, post, question, answer, comment, resource, message, report, or file.

6. Why we process data and legal bases

We process personal data only for defined purposes and on a lawful basis under Article 6 of the GDPR. The main purposes and bases are:

Purpose	Examples of data	Legal basis
Provide and secure accounts	Registration, login, password reset, required account fields, acceptance records.	Article 6(1)(b) GDPR: to provide the requested e-Hub service and manage the account.
Operate member profiles and community features	Profile information, posts, questions, answers, comments, resources, uploads, reactions, follows, groups, and notifications.	Article 6(1)(b) GDPR for requested features and Article 6(1)(f) GDPR for compatible service administration and community integrity.
Moderate content and protect members	Reports, content, account information, technical signals, decisions, restrictions, and appeals.	Article 6(1)(f) GDPR: legitimate interests in safety, abuse prevention, and rule enforcement; Article 6(1)(c) where a legal obligation applies.
Maintain security and reliability	IP address, device and session data, logs, security events, backups, and error information.	Article 6(1)(f) GDPR: legitimate interests in keeping the service secure and available; Article 6(1)(c) where required by law.
Measure service use	Consent records and analytics events that do not intentionally identify members.	Article 6(1)(a) GDPR: consent for non-essential analytics cookies and similar technologies.
Handle support and rights requests	Correspondence, account information, identity-verification information, and request history.	Article 6(1)(c) GDPR where needed to meet a legal obligation and Article 6(1)(f) GDPR for accountable service administration.
Produce project and service reporting	Aggregated or anonymised participation and engagement measures.	Article 6(1)(f) GDPR where necessary for legitimate project and service evaluation, with aggregation or anonymisation used wherever possible.

Where processing is based on consent, you may withdraw consent at any time. Withdrawal does not affect processing that took place lawfully before withdrawal.

7. Sensitive information and survivor confidentiality

The subject matter of the RECOVER project means that community content could easily reveal highly sensitive information, including a person's health, trauma, ethnicity, immigration status, criminal allegations, sexual life, or status as a trafficking victim or survivor. The e-Hub is not designed to receive identifiable case information.

- Do not post or upload personal data about a survivor, client, witness, suspect, family member, or service user.
- Use anonymous, composite, or fictionalised examples that cannot reasonably be linked to a real person.
- If sensitive or identifying information is submitted, KOPŽI may restrict access, remove it, anonymise it, and take safeguarding, security, or legal steps that are necessary and proportionate.
- A general account acceptance or privacy acknowledgement is not permission to submit special-category data.

If you believe that a person may be identifiable from content already submitted, contact info@recover-project.eu promptly and do not forward the material to additional people.

8. Visibility and member content

Member profiles, posts, questions, answers, comments, resources, uploads, and other community activity are intended to be available only to authenticated e-Hub members. The e-Hub is designed to prevent unauthenticated visitors and search engines from accessing member-only areas, but no online service can guarantee that an authorised viewer will not copy, download, quote, or screenshot information.

Do not treat member-only visibility as a promise of professional secrecy. Share only information that you are authorised to share and that does not identify a survivor, client, witness, or service user.

Your email address, password, password-reset information, security logs, and private account-management records are not displayed to other members. Moderators and administrators may access content and account data where necessary to operate the service, investigate reports, provide support, or comply with law.

9. Cookies and analytics

The e-Hub uses strictly necessary cookies and similar storage for login, authentication, security, consent preferences, and requested service functions. These technologies may be used without consent where the law permits because the service cannot function as requested without them.

Google Analytics 4 may be used only after you give consent to non-essential analytics. Analytics is intended to provide aggregated information about service use. KOPŽI does not intentionally send your password, email address, private messages, survivor or client information, or other direct identifiers to Google Analytics.

You can refuse or withdraw analytics consent through the cookie settings available on the e-Hub. Withdrawing consent does not disable necessary account and security cookies.

For more information about Google privacy practices, see [Google Privacy Policy](#).

10. Service providers and data recipients

KOPŽI shares personal data only when necessary for the purposes described in this Policy, under appropriate confidentiality and security arrangements. Recipients may include authorised KOPŽI administrators and moderators, authorised KMOP personnel acting within their assigned role, public authorities where required by law, and the following service providers:

Provider	Role	Data that may be processed	Transfer and safeguards
Hetzner Online GmbH	Hosting and infrastructure	Account data, profile data, member content, technical logs, and service databases.	Hosting and infrastructure services. KOPŽI uses contractual, technical, and organisational safeguards and limits access to what is needed for the service.
Brevo	Transactional email delivery	Email address, account and password-reset messages, service notifications, delivery status, and support correspondence where sent through the service.	Used for necessary service communications. Provider processing and any sub-processors are subject to applicable GDPR safeguards.
Google Analytics 4	Consent-based service	Consent status and	Used only after consent. Any

Provider	Role	Data that may be processed	Transfer and safeguards
	analytics	pseudonymous analytics events after consent.	processing outside the EEA is subject to the safeguards required by Chapter V GDPR.
Google Drive	Encrypted backup storage	Backups of service data and configuration needed for recovery and continuity.	Backup access is restricted. Any processing outside the EEA is subject to the safeguards required by Chapter V GDPR.

Provider names and processing arrangements may change when the service changes. KOPŽI will update this Policy or the related service information when a change materially affects how personal data is processed.

11. International data transfers

Some service providers or their approved sub-processors may access or process personal data outside the European Economic Area, depending on the service configuration and support arrangements. Where such a transfer takes place, KOPŽI uses a lawful transfer mechanism required by Chapter V of the GDPR, such as an adequacy decision, standard contractual clauses, or another permitted safeguard, together with appropriate technical and organisational measures.

You may contact info@recover-project.eu to ask for general information about the safeguards applicable to a particular provider or transfer. Provider privacy notices may also describe their own processing and transfer arrangements.

12. Retention and deletion schedule

We keep personal data only for as long as it is needed for the purposes described in this Policy. Unless a longer period is required by law, necessary to investigate a security incident, or needed to establish, exercise, or defend legal claims, the maximum standard retention period is 24 months after account closure or the last active use of the account.

Record	Standard retention	What happens afterwards
Active account and profile	While the account is active. If inactive or closed, normally no longer than 24 months after the last active use or closure.	Delete or anonymise account and profile data, subject to legal, security, and historical-content exceptions.
Posts, questions, answers, comments, resources, and uploads	While published or otherwise needed for the community; historical content may remain after account closure.	Keep as historical content where necessary for discussion integrity, remove or detach personal profile information where feasible, and remove content that violates the rules or law.
Moderation reports, appeals, and security records	Normally no longer than 24 months after the matter is closed.	Delete or anonymise unless a documented legal hold, repeat-abuse prevention need, or active security matter requires longer retention.
Service correspondence and rights requests	Normally no longer than 24 months after resolution.	Delete or retain only the minimum audit record required by law or accountability needs.

Record	Standard retention	What happens afterwards
Analytics and consent records	Analytics events only after consent; consent evidence is kept for as long as needed to demonstrate compliance, normally no longer than 24 months after the relevant consent ends.	Delete or aggregate, keeping only what is necessary to demonstrate the choice and its withdrawal.
Backups	Rolling backups are retained for no longer than 24 months unless needed for an active recovery or legal hold.	Backups expire or are securely overwritten. Restored systems must reapply deletion and access restrictions.

13. Security and confidentiality

KOPŽI applies technical and organisational measures appropriate to the risks of the e-Hub, including secure transport, protected password storage, role-based access, restricted administrator permissions, security monitoring, backups, patching, and incident-response procedures. Access is limited to people and providers who need it for a defined purpose.

No online service is completely secure. You should use a unique password, enable available security controls, keep your devices updated, and notify KOPŽI promptly if you suspect account misuse or a personal-data exposure. Do not include passwords, reset codes, or sensitive case details in a security report.

If KOPŽI becomes aware of a personal-data breach, it will assess the incident and notify the competent authority and affected individuals where required by the GDPR.

14. Your data protection rights

Subject to the conditions and limitations in the GDPR, you may have the following rights:

Right	What it means
Access	Ask whether we process your personal data and request a copy and information about the processing.
Rectification	Ask us to correct inaccurate or incomplete personal data.
Erase	Ask us to delete personal data when the legal conditions apply.
Restriction	Ask us to limit processing while a legal or factual issue is resolved.
Data portability	Receive data you provided in a structured, commonly used, machine-readable format where the legal conditions apply.
Object	Object to processing based on legitimate interests for reasons relating to your situation.
Withdraw consent	Withdraw consent for future consent-based processing, without affecting earlier lawful processing.
Complaint	Complain to a competent data protection supervisory authority and seek a judicial remedy where available.

To exercise a right, email info@recover-project.eu. Please describe your request clearly. We may ask for proportionate information to verify your identity and protect other people's data. We normally respond within one month. If a request is complex, the response period may be extended as permitted by the GDPR, and we will explain why.

15. Account closure and historical content

You may request account closure by contacting info@recover-project.eu. Account closure removes or disables the account and starts the applicable deletion or anonymisation process. It does not automatically erase every contribution that forms part of a shared discussion or resource history.

Posts, questions, answers, comments, resources, and other member contributions may remain as historical content after account closure when removing them would damage the context or integrity of the community. Where feasible, KOPŽI will detach historical content from the active profile or anonymise the author. Content that is unlawful, unsafe, or prohibited by the Community Guidelines may be removed or restricted.

Search-engine caches, downloads, screenshots, quoted text, and other copies made by members may not disappear immediately or be within KOPŽI's control.

16. Service communications

The e-Hub may send messages necessary to provide and secure the service, including account verification, password-reset messages, security alerts, replies, mentions, notifications, and important policy or service notices. These are operational communications, not newsletters.

Brevo may be used to deliver these messages. Delivery information such as timestamps, delivery status, bounces, and limited technical information may be processed to keep communications reliable and secure.

17. Children

The e-Hub is intended only for people aged 18 or older. If KOPŽI learns that an account was created by a person under 18, it may restrict or close the account and delete personal data that has no lawful reason to remain.

18. Automated decision making and AI

The e-Hub does not use AI, profiling, or solely automated decision-making to determine eligibility, access, moderation outcomes, or other decisions with legal or similarly significant effects. Moderation and safety decisions are handled by authorised people. Member content is not used to train an external AI model through the e-Hub.

19. Changes to this Policy

KOPŽI may update this Policy when the service, legal requirements, providers, processing purposes, visibility settings, or security arrangements change. The updated version will show a new date or version number. If a change materially affects your rights or the way your data is used, KOPŽI will provide an appropriate notice before the change takes effect where required by law.

20. Complaints and further contact

Please contact KOPŽI first at info@recover-project.eu so that we can review and address your concern. You also have the right to lodge a complaint with a data protection supervisory authority. There is no single European Union authority that handles individual GDPR complaints. You may contact the authority in the country where you live, work, or where the alleged infringement occurred.

For a controller established in Lithuania, the relevant authority is the [State Data Protection Inspectorate \(VDAI\)](#).

Supervisory authority	Contact
State Data Protection Inspectorate (VDAI)	L. Sapiegos str. 17, LT-10312 Vilnius, Lithuania Email: ada@ada.lt Phone: +370 5 271 2804 / +370 5 279 1445 Website: vdai.lrv.lt/en/

The European Data Protection Board provides guidance and coordination but does not handle individual complaints or conduct individual investigations.

Document information

Controller: Kovos su prekyba žmonėmis ir išnaudojimu centras, VŠĮ (KOPŽI) | Company code 304486353 | Draugystės g. 8F-236, LT-51264 Kaunas, Lithuania

Privacy contact: info@recover-project.eu | Version 1.0 | Last updated 22 October 2026 | Effective upon publication