

# VolunTECH Matching Platform

## Privacy Policy

The present Privacy Policy applies to all Users of the website (<https://volunteer-match-stg.scify.org/>) (hereinafter referred to as the “Users” or the “User” and “Platform” respectively) and forms an integral part of the Platform’s Terms and Conditions. The present Privacy Policy provides the User with general information regarding how the Data Controller uses your personal data and other information required by data protection legislation. In case of future amendment, the User will be provided with necessary updates and information through the update of the present Privacy Policy, uploaded in the Platform.

VolunTECH is a European platform that connects motivated volunteers, NGOs and youth organisations. It offers digital and hybrid volunteering opportunities, training, and practical tools that support real community impact. VolunTECH is developed as part of an Erasmus+ co-funded project.

This Privacy Policy explains how personal data are collected, used, stored and protected in accordance with Regulation (EU) 2016/679 (GDPR) and applicable national laws. The Platform is made available in multiple EU languages; in the event of any inconsistency between language versions, the English version shall prevail.

### 1. Data Controller

1.1. The company “SCIENCE FOR YOU” PNPC – SciFY, address: TEPA Lefkippos – NCSR Demokritos / 27, Neapoleos str., 153 41 Ag. Paraskevi, Greece, Telephone: +30 211 400 4192, email: [info@scify.org](mailto:info@scify.org), is the Data Controller for the processing of the User’s Personal Data (hereinafter referred to as “Data Controller”).

1.2. Data Controller’s Contact Details: For any issue or concern with regards to the present Privacy Policy and to the processing of User’s personal data, the User can communicate with the Data Controller by:

- Calling at +30 211 400 4192, from Monday to Friday, 09:00–17:00 EET (Eastern European Time)
- Sending an email to: [info@scify.org](mailto:info@scify.org)
- Sending correspondence to: TEPA Lefkippos – NCSR Demokritos / 27, Neapoleos str., 153 41 Ag. Paraskevi, Greece

### 2. Purpose and Legal Basis of Processing

#### 2.1 Purpose of the Platform

VolunTECH enables registered Users to:

- Create volunteer or organisational profiles
- Publish digital and hybrid volunteering opportunities
- Publish volunteer availability
- Participate in training activities

- Access practical tools
- Communicate with other registered Users
- Contribute to initiatives supporting community impact

Personal data are processed only to the extent necessary for the proper operation, security, improvement and lawful compliance of the Platform.

## 2.2 Legal Bases for Processing

Personal data are processed under the following legal bases:

(a) Performance of a Contract (Art. 6(1)(b) GDPR) – Processing necessary for:

- Registration and account management
- Authentication and login
- Profile creation and publication
- Matching volunteers and organisations
- Internal messaging and communication
- Providing access to training and tools

Without this processing, the Platform cannot function.

(b) Legitimate Interests (Art. 6(1)(f) GDPR) – Processing necessary for:

- Ensuring security and technical stability
- Preventing fraud, spam, misuse or harmful behaviour
- Handling reports of illegal or inappropriate content
- Protecting Users and the Platform
- Improving functionality and performance

These interests do not override Users' fundamental rights.

(c) Legal Obligations (Art. 6(1)(c) GDPR) – Processing required to comply with:

- Applicable EU and national laws
- Cooperation with public authorities
- Obligations under the Digital Services Act (EU) 2022/2065 (DSA)

(d) Consent (Art. 6(1)(a) GDPR) – Where required, processing is based on consent, including:

- Installation of non-essential cookies
- Receiving newsletters
- Participation in optional surveys

Consent may be withdrawn at any time without affecting the lawfulness of processing carried out prior to withdrawal.

## 3. Categories of Data Processed

### 3.1 Account Data

- First and last name
- Email address
- Password (encrypted)

- User type (volunteer / organisation)

### 3.2 Profile Data

- Skills
- Areas of interest
- Availability
- Location (country/city level)
- Organisation details (name, legal status, website, contact person)

### 3.3 Listings and Content Data

- Volunteering opportunities
- Volunteer availability posts
- Training participation information

Users are solely responsible for the content they publish. Users must not publish sensitive personal data (e.g., health data, political opinions, religion, criminal records, full home addresses) unless strictly necessary and lawful.

### 3.4 Communication Data

- Messages exchanged within the Platform
- Support requests
- Safety reports and complaints

### 3.5 Usage and Technical Data

- IP address
- Browser type and version
- Device identifiers
- Access times
- Log files

## 4. How Data Are Collected

Data are collected:

- Directly from Users during registration
- When Users create profiles or publish content
- When Users communicate via the Platform
- Automatically through technical logs and cookies

## 5. Data Retention

### 5.1 Account Data

Account data are retained for as long as the account remains active. Upon account deletion, account data are deleted within 30 days, unless retention is required by law, for ongoing investigations, or for the establishment or defence of legal claims.

### 5.2 Communication and Content Data

Stored while the account is active. Deleted upon account deletion unless required for legal compliance, ongoing investigations, or establishment or defence of legal claims.

### 5.3 Usage and Technical Data (Logs and IP Addresses)

Technical logs and IP address data are retained for a maximum of 36 months from the date of collection, unless a longer retention period is required by applicable law or for the investigation of specific security incidents.

### 5.4 Legal Obligations

Certain data may be retained longer if required by law or by order of a competent authority.

## 6. User Rights

Users have the following rights under GDPR:

- Right of Access (Art. 15 GDPR)
- Right to Rectification (Art. 16 GDPR)
- Right to Erasure (Art. 17 GDPR)
- Right to Restriction of Processing (Art. 18 GDPR)
- Right to Data Portability (Art. 20 GDPR)
- Right to Object (Art. 21 GDPR)
- Right to Withdraw Consent (Art. 7(3) GDPR)
- Right to Lodge a Complaint with a Supervisory Authority (Art. 77 GDPR)

To exercise any of the above rights, Users may contact the Data Controller at [info@scify.org](mailto:info@scify.org). The Data Controller will respond within one (1) month, unless an extension is legally justified.

Complaints may be lodged with the competent supervisory authority. Since the Data Controller is established in Greece, the primary supervisory authority is:

Hellenic Data Protection Authority (HDDPA)

Kifissias 1–3, 115 23 Athens, Greece

Telephone: +30 210 6475 600

Website: [www.dpa.gr](http://www.dpa.gr)

Email: [contact@dpa.gr](mailto:contact@dpa.gr)

Users who reside in another EU Member State also have the right to lodge a complaint with the supervisory authority of their Member State of residence.

## 7. Partner Organisations and Data Access

VolunTECH is developed as part of an Erasmus+ project involving multiple partner organisations. Partner organisations do not have direct access to Users' personal data through the Platform's systems unless they are individually registered as Users in accordance with these policies.

Any aggregated or anonymised data that may be shared with partners for project reporting and evaluation purposes will not permit the identification of individual Users. Where any individual personal data were to be shared with partners for specific legitimate purposes, a

joint controllership agreement or data processing agreement compliant with Art. 26 or Art. 28 GDPR would be put in place prior to such sharing.

## 8. User-Generated Content and Safety

The Platform does not systematically pre-moderate content. Users are fully responsible for the accuracy and legality of content they publish.

The Platform provides a notice-and-action mechanism in accordance with the Digital Services Act (EU) 2022/2065, allowing Users to report:

- Illegal content
- Harassment
- Fraud
- Privacy violations
- Misleading information

Upon receiving a report, the Platform will aim to review it within 10 working days and may:

- Review the content
- Restrict visibility
- Remove content
- Suspend or terminate accounts
- Notify competent authorities where required by law

The person who submitted the report will be informed of the outcome and of their right to appeal the decision. Affected Users whose content is removed or accounts suspended may challenge such decisions through the Platform's internal complaint-handling mechanism (see the Terms and Conditions, Section 7.4).

## 9. Data Security

The Platform implements appropriate technical and organisational measures, including:

- HTTPS encryption
- Secure authentication
- Encrypted password storage
- Restricted access to authorised personnel only
- Regular software updates and security reviews

Absolute security cannot be guaranteed due to factors beyond the Data Controller's control. In the event of a personal data breach that is likely to result in a risk to Users' rights and freedoms, the Data Controller will notify the HDPA and, where required, affected Users in accordance with GDPR Arts. 33–34.

## 10. Data Recipients

Personal data may be shared with:

- Hosting providers
- IT service providers
- Email service providers
- Analytics providers (only if consent is given)

All service providers act under contractual safeguards as data processors in accordance with Art. 28 GDPR.

If data are transferred outside the EU/EEA, appropriate safeguards (e.g., Standard Contractual Clauses under Art. 46 GDPR) are implemented to ensure an adequate level of protection.

## 11. Links to Third-Party Websites

The Platform may contain links to third-party websites. The Data Controller is not responsible for their content or data processing practices. Users should review the privacy policies of those websites separately.

## 12. Cookies

The Platform uses cookies that are:

- Strictly necessary for operation
- Optional (analytics or functional), subject to consent

Non-essential cookies are installed only after User consent through a cookie management panel. Users may withdraw consent at any time.

If third-party services (e.g., embedded videos) are used, related cookies may be set by those third parties in accordance with their own policies.

### 12.1 Strictly Necessary Cookies

The strictly necessary cookies are essential for the proper operation of the Platform. These cookies allow Users to browse and use Platform features such as access to secure areas. They do not recognise the User's individual identity and without them the smooth operation of the Platform is not possible.

Cookie	Description	Duration	Transfer to 3rd Parties
cf_clearance	Set by Cloudflare to identify trusted web traffic and mitigate DDoS attacks. Determines if the visitor is human or a bot.	1 month	No
voluntech_matching_cookies_consent	Set by the GDPR Cookie Consent plugin. Stores whether the user has consented to the use of cookies. Does not store personal data.	1 year	No
volunteer_management_system_session	Set by Laravel to identify a session	2 hours	No

Cookie	Description	Duration	Transfer to 3rd Parties
	instance for the user.		
XSRF-TOKEN	Set by Laravel to prevent Cross-Site Request Forgery (CSRF) attacks.	2 hours	No

### 13. Children’s Privacy

The Platform does not address anyone under the age of 18 (“Children”). The Platform does not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your child has provided personal data without your consent, please contact the Data Controller at [info@scify.org](mailto:info@scify.org). Upon confirmation, steps will be taken to remove that information from the Platform’s systems.

### 14. Amendments to this Privacy Policy

The Data Controller reserves the right to amend this Privacy Policy, for example when necessary to comply with new requirements imposed by applicable laws, guidelines or technical requirements, or in the course of a revision of the Data Controller’s processes and practices.

The User will be notified of any material amendment to this Privacy Policy through the Platform. The User should regularly review this Privacy Policy for any amendments.

### 15. Language Versions

This Privacy Policy is made available in multiple EU languages to ensure accessibility for all Users. In the event of any inconsistency or conflict between language versions, the English version shall prevail, unless otherwise required by applicable law.