EMOTiC
European Multidisciplinary Organization for Training and international Consulting

ORGANISATIONAL SUPPORT

Data Protection Policy

How we handle personal data in our projects and daily work, in line with the GDPR and the Austrian Data Protection Act.

Version 1.0	Owner	Review
October 2026	Data Protection Contact	Every two years, or after a data breach or a change in the law

EMOTiC for Training and Consulting · Rauhensteingasse 7/18, 1010 Vienna, Austria · ZVR-Zahl 1026550097 · emotic.org@gmail.com

At a glance

- We collect only the personal data we need, for a clear purpose and on a valid legal basis.
- Health data and data about minors get extra protection; parents or guardians consent for participants under 18.
- We share data only with those who need it, such as partners, National Agencies, venues and travel agencies.
- We store data securely, keep it only as long as needed and then delete it.
- Anyone who notices a data breach tells the Data Protection Contact immediately.

Document	Data Protection Policy
Organisation	EMOTiC for Training and Consulting (European Multidisciplinary Organization for Training and international Consulting), ZVR-Zahl 1026550097
Version	Version 1.0, October 2026
Owner	Data Protection Contact
Issued by	EMOTiC Board (Vorstand), October 2026
Review	Every two years, or after a data breach or a change in the law

Contents

1. Purpose and scope
2. Key terms
3. Principles we apply
4. What personal data we process and why
5. Special categories of data
6. Data of minors and parental consent
7. Sharing personal data
8. International transfers
9. Storage and security
10. Retention
11. Photos and videos
12. Rights of data subjects
13. Data breaches
14. Training
15. Roles and responsibilities
16. Review and contacts

1. Purpose and scope

EMOTiC handles personal data every day: in applications, travel bookings, reports to the National Agency and photos of activities. This policy explains how we do this lawfully, fairly and safely, in line with the EU General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and the Austrian Data Protection Act (DSG).

It applies to everyone who handles personal data for EMOTiC, including at our branches in France and Croatia, and to data in any form: files, emails, messages, paper forms, photos and videos. It is our internal policy; the privacy notice on our website informs the public.

2. Key terms

Term	Meaning
Personal data	Any information about an identifiable person, such as a name, email address, photo or date of birth.
Special categories	Sensitive data, such as health, disability, ethnic origin or religious beliefs.
Controller	The organisation that decides why and how data is processed. EMOTiC is the controller for its own work.
Processor	A service provider that processes data on our behalf, such as an IT or mailing service.
Data breach	Any loss, unauthorised access, disclosure, change or destruction of personal data.

3. Principles we apply

GDPR principle	What it means for us
Lawfulness, fairness, transparency	We tell people what we collect and why.
Purpose limitation	Data is used only for its original purpose; participant data never for marketing without consent.
Data minimisation	Forms ask only what we need; ID details only when travel or a venue requires them.
Accuracy	We correct data when people tell us it has changed.
Storage limitation	We delete data when its retention period ends (section 10).
Integrity and confidentiality	Access rights, strong passwords and secure storage.
Accountability	We document what we do and can show it.

4. What personal data we process and why

Who	Typical data	Purpose	Legal basis
Applicants and participants	Name, contact details, date of birth, nationality, motivation, travel and ID details, bank details for reimbursement, emergency contact	Selection, organising the activity, travel, accommodation, reimbursement, Youthpass, grant reporting	Contract; legitimate interest in grant reporting
Minors and their parents or guardians	As for participants, plus parents' names, contacts and signatures	As for participants; parental consent; emergency contact	Consent of a parent or guardian; contract
Staff, trainers, volunteers and interns	Contact details, application documents, contract, bank and social security details, criminal record certificate	Recruitment, contracts, payment, safeguarding	Contract; legal obligation; legitimate interest in safeguarding
Partner contacts	Name, role, organisation, email, phone	Running joint projects	Legitimate interest; contract
Newsletter subscribers	Email, name if given	Sending our newsletter	Consent
People downloading from our Library	Name, email, organisation and country	Providing documents	Consent
Photo and video material	Images and voices	Documentation, reporting, dissemination	Consent; for minors, a parent or guardian

5. Special categories of data

To keep participants safe and included, we sometimes need to know about health conditions, allergies, medication, dietary needs or disability-related support. We treat dietary needs with the same care, as they can reveal health or religion.

- We ask only what we need, usually with one open question: "Is there anything we should know to keep you safe and included?"
- We process this data with the explicit consent of the participant or, for minors, a parent or guardian, or where needed to protect someone's life or health in an emergency.
- Only the Project Coordinator and those who need it, such as the group leader, see it. It is kept apart from participant lists. Venues receive dietary requirements, not the reasons.
- For participants with fewer opportunities, we record only what grant reporting and the support itself require.

6. Data of minors and parental consent

Many participants in our school workshops, career orientation days and youth exchanges are under 18.

- A parent or legal guardian signs the registration and consent forms, including consent for photos and for sharing health information.
- We explain to young people, in words they understand, what we do with their data, and respect their wishes, for example not to be photographed even when a parent has consented.
- For school workshops and career orientation days, we agree with the school in advance what data, if any, we receive.
- Minors' contact details are used only for the activity, never for marketing.
- We never publish a minor's full name with a photo.

7. Sharing personal data

We share only the minimum needed, with recipients who protect it. We never sell personal data.

Recipient	What and why
Partner organisations	Lists, travel details and emergency contacts for their own group. Partnership agreements include data protection duties.
National Agencies and the European Commission	Participant data the grant agreement requires, entered in the Beneficiary Module for reporting; participants then receive an EU survey for their participant report. These bodies follow their own data protection notices.
Venues, such as youth guest houses	Names, dates, room allocation and dietary requirements.
Travel agencies and transport providers	Names, dates of birth and ID details needed for tickets.
Service providers	Only under a data processing agreement.
Authorities and emergency services	Where the law requires it or in an emergency.

8. International transfers

Some partner organisations are outside the EU and the European Economic Area (EEA). Before transferring data to them, we:

- share only what the partner needs for its own participants
- check whether the European Commission has recognised the country as having adequate data protection (an adequacy decision)
- otherwise use appropriate safeguards, such as the European Commission's standard contractual clauses in the partnership agreement, or, where none is possible, only the limited exceptions the

GDPR allows, after informing the people concerned
- use access-controlled folders rather than email or messaging apps.

The Data Protection Contact advises before any new transfer outside the EU and EEA.

9. Storage and security

- **Access rights:** each person accesses only the folders their role needs. Access ends with the role.
- **Passwords and two-factor authentication:** strong, unique passwords and two-factor authentication on every account holding personal data. Passwords are never shared.
- **Devices:** work laptops and phones are encrypted, locked with a password or PIN and kept updated. Report a lost device at once.
- **Private devices:** no personal data on private devices or accounts without approval from the Data Protection Contact; approved data is deleted once the task is done.
- **Paper records:** forms and health information are kept locked, in the office and during activities.
- **Everyday care:** check recipients, use blind copy for external group emails and never post health data or participant lists in messaging groups.

10. Retention

When a project closes, the Project Coordinator checks the project folder and deletes what is no longer needed.

Data	How long we keep it
Applications not selected	Until the activity has taken place, in case a place becomes free
Participant evidence: lists, attendance, travel documents, consent forms, Youthpass data	As required by the grant agreement, until the end of its record-keeping period
Health information and emergency contacts	Until the activity and any follow-up are finished
Safeguarding and incident records	As long as needed to protect the people involved and to meet legal and funding obligations, then deleted securely (see the Safeguarding Policy)
Staff, volunteer and intern files	As required by Austrian employment, tax and social security law
Criminal record certificates	We note the date we saw the certificate and do not keep copies
Financial records	As required by Austrian law and the grant agreement, whichever is longer
Partner contacts	Until the last joint project's record-keeping period ends

Data	How long we keep it
Newsletter subscribers	Until they unsubscribe
Library download contacts	Two years after the last download, or earlier if the person asks us to delete them
Photos and videos	Published: while used for reporting and dissemination, unless consent is withdrawn. Unpublished: deleted two years after the end of the project
Records of data requests and breaches	Three years after the request or breach is closed

11. Photos and videos

- The registration form asks for consent, with separate choices for internal documentation and public use.
- At each activity, participants who do not want to appear wear an opt-out sticker, which photographers respect. At public events, signs say that photos are being taken and whom to tell.
- We never take photos in bedrooms, bathrooms or changing areas, or of anyone in distress.
- Photos on private phones are moved to the shared drive after the activity and deleted from the phone.
- Anyone can withdraw consent at any time by writing to emotic.org@gmail.com. We then stop using the material and remove it from our channels as soon as possible. Printed material or posts shared by others cannot always be recalled.

12. Rights of data subjects

People whose data we process can:

- access their data and receive a copy
- have inaccurate data corrected
- have data deleted when we no longer need it or have no legal basis to keep it
- restrict its use or receive it in a portable format
- object to processing based on legitimate interest, and to direct marketing at any time
- withdraw consent at any time, without affecting earlier processing
- complain to the Austrian Data Protection Authority (Datenschutzbehörde) in Vienna.

How to make a request: write to emotic.org@gmail.com or tell any team member, who passes it to the Data Protection Contact the same day. We respond within one month; for complex requests we may extend this by up to two further months and explain why within the first month. Requests are free of charge.

13. Data breaches

Examples: a lost phone with participant lists, an email sent to the wrong group or a hacked account.

1. **Contain it:** limit the damage at once, for example by changing a password or asking a recipient to delete the data.
2. **Report it immediately** to the Data Protection Contact and the Project Coordinator. Do not wait for all the details.
3. **Assess:** the Data Protection Contact checks what data and how many people are affected, and the risk to them.
4. **Notify the authority:** where the breach is likely to put people's rights and freedoms at risk, the Data Protection Contact and the Board notify the Austrian Data Protection Authority within 72 hours of us becoming aware of it.
5. **Inform the people affected** without undue delay where the risk is high, with advice on protecting themselves, and inform partners whose participants are affected.
6. **Record and learn:** every breach, notified or not, goes into the breach log with what we changed to prevent a repeat.

Lost a device or sent data to the wrong person? Tell the Data Protection Contact immediately.

14. Training

Everyone who handles personal data completes data protection training during onboarding and a refresher every two years. Before each activity, the Project Coordinator briefs trainers, group leaders, volunteers and interns on the practical rules.

15. Roles and responsibilities

Role	Responsibilities
Board	Overall responsibility; approves this policy; appoints the Data Protection Contact; provides resources; decides on notifications to the authority with the Data Protection Contact.
Data Protection Contact	Advises the team; keeps the record of processing activities and the breach log; handles requests and breaches; organises training.
Project Coordinator	Applies this policy in each project: forms, consents, storage, sharing and deletion at closure; briefs the project team.
Everyone	Uses personal data only for their tasks, keeps it secure, and passes on requests and breaches at once.

16. Review and contacts

The Data Protection Contact reviews this policy every two years, or after a data breach or a change in the law. The Board approves changes.

Item	Details
Issued by	Board (Vorstand), October 2026
Data Protection Contact	emotic.org@gmail.com (subject: Data protection)
General contact	emotic.org@gmail.com
Supervisory authority	Austrian Data Protection Authority (Datenschutzbehörde), Vienna

This document is part of EMOTiC's organisational support materials. Other organisations are welcome to adapt it for their own work with credit to EMOTiC. Questions and feedback: emotic.org@gmail.com