

1st Forum for European Environmental Human Rights Defenders

Safe Space Protocol

Version: 02 June 2026

1. Purpose, compliance and collective responsibility

This Safe Space Protocol establishes the principles and rules governing the 1st Forum for European Environmental Human Rights Defenders (EHRDs and 'the Forum'). Its purpose is to ensure that all participants can engage in an environment that is secure, inclusive, and grounded in trust.

Safety is understood as a holistic condition that includes confidentiality, autonomy, accessibility, and psychological wellbeing. The protocol places particular emphasis on participants in high-risk situations, and those whose identities or work require heightened protection.

The Forum will take place in Strasbourg, France, between 3 and 4 June 2026, in the Council of Europe premises. Human Rights Defenders attending the Forum will come from different countries of Europe and Central Asia.

- Participants in the Forum should comply with this Safe Space Protocol.
- Failure to comply with this Protocol may result in removal from the Forum.
- Maintaining a safe and trusted environment relies on the collective commitment of all participants to uphold these principles in practice.
- These provisions apply to all individuals present at the Forum, including participants, speakers, facilitators, staff, volunteers, and contractors.

2. Core Commitments

The Forum is grounded in the following commitments:

- **Confidentiality and informed consent** underpin all interactions. Participation does not imply consent to visibility, identification, or attribution, and no information or image of others is shared or published without explicit permission.
- **Protection of at-risk defenders** is a priority. Particular care is taken to safeguard individuals facing heightened risks, including those exposed to surveillance, reprisals, or restrictive environments.
- **Zero tolerance for harassment and retaliation** applies at all times. Harassment, discrimination, intimidation, or any form of coercion are not tolerated under any circumstances. This includes conduct based on gender identity, sexual orientation, disability, ethnicity, nationality, or any other status.
- **Inclusion, accessibility, and equity** are essential to meaningful participation. The Forum ensures that diverse needs, identities, and experiences are respected and accommodated, including those related to disability, neurodiversity, and inequalities, as far as possible.

- **Participant autonomy** is respected at all times. Every individual retains the right to decline participation, refuse interaction, set boundaries, or withdraw from any situation without explanation.
- **Trust, accountability, and transparency** underpin the organisation of the Forum. Clear information is provided about processes affecting participants, concerns are addressed responsibly, and measures are in place to ensure accountability for decisions and actions.
- **Shared responsibility for a safe environment** applies to all participants. Creating and maintaining a respectful, inclusive, and secure space is a collective obligation.

3. Travel and entry to France (Schengen zone for non-EU EHRDs) and risk mitigation

- HRDs traveling from outside the Schengen zone may face elevated risks related to travel, including surveillance, questioning, visa denial, or exit/entry bans imposed by their home authorities. These risks should be assessed on a case-by-case basis during travel planning.

3.1. Device security and data minimisation prior travel

To reduce risks related to surveillance, search on devices, or data access during border crossing, participants are encouraged to review the Security in a Box guide, '[Protect your information and devices while traveling](#)'. At minimum, participants are strongly encouraged to apply the measures listed below:

- **Assume border inspection is possible:** Prepare devices on the basis that they may be searched or temporarily confiscated. Limit exposure accordingly.
- **Remove sensitive data:** Delete files, communications, and contact information that are not strictly necessary. Do not carry data that could put you or others at risk.
- **Back up data before departure:** Save important data to a secure, encrypted location that is separate from the device being carried.
- **Use a clean or low-data device where possible:** Travel with a device that contains minimal information. If using a primary device, reduce its contents to essential data only.
- **Log out of accounts and remove access:** Log out of email, social media, and other accounts. Remove saved passwords and avoid staying logged into sensitive services.
- **Delete chat history and activity traces:** Clear message history, call logs, browser history, downloads, and cached data.
- **Remove or reduce applications:** Uninstall apps that contain or provide access to sensitive information.
- **Enable strong device security:** Use a strong password, enable full-disk encryption, and activate automatic locking. Avoid biometric unlocking where it may be compelled.
- **Update systems and applications:** Install the latest security updates before travelling.
- **Encrypt sensitive files or remove them entirely:** If sensitive data must be carried, store it in encrypted form. If encryption increases risk in your context, remove the data and access it securely after arrival.

- **Reduce visible indicators of sensitive work:** Remove or rename files, apps, and group chats that reveal affiliations, organisations, or activities.
- **Download a VPN before departure:** for example, ProtonVPN is free. You can [download it here](#). You simply have to create an account with an email and password. If using a VPN increases risk in your context, refrain from connecting to public WiFi (e.g. airport).

5. Disability-inclusive venue design & Safety

- Accessibility is a prerequisite for safety (please refer to [Protection International's document on inclusion, protection and well-being HRDs with disabilities](#)).
- Physical navigation: Ensure step-free access to all stages, breakout rooms, and dining areas. Reserve seating specifically for wheelchair users and those with mobility aids.
- Sensory & rest zones: The Forum will have a designated quiet space, equipped with dim lighting and low noise levels, to allow for rest. Participants who feel uncomfortable or overwhelmed can withdraw from sessions and access a quiet environment.
- Emergency evacuation: in case of emergency and evacuation alarm, follow instructions by CoE staff. Designated staff will assist participants with disabilities.

6. Confidentiality and Safe Dialogue

6.1. Expected behaviour during the Forum:

- Treat all individuals with respect, courtesy, and consideration.
- Listen actively and engage constructively with diverse perspectives.
- Use inclusive language and
- Refrain from any form of harassment or discrimination based on race, gender identity, sexual orientation, disability, religion, age, nationality, or any other ground.
- Uphold confidentiality when requested and avoid exposing sensitive personal information.
- Report concerns promptly to the Safety Team (*see section 7 below*) and cooperate with any resulting inquiry.

6.2. Identification

- Upon arrival at the Forum, each participant will be required to undergo a security screening and collect their official Council of Europe conference name badge in order to access the premises.
- After entering the Council of Europe entrance hall, participants are requested to collect their specialised Forum badges at the reception desks. Participants will be invited to write their chosen name and pronouns on the badge.
- There will be three types of specialised Forum badges:



Participant Badge



Badge for participants who do not consent to being photographed, filmed, or recorded, any time



Organisers badge

- Communication Sticker system (Optional): Participants can add small, colored stickers to their specialised Forum badges to indicate their social energy or interaction preference:
 - **Blue Sticker:** "I am open to networking and new introductions."
 - **Orange Sticker:** "I am only speaking with people I already know."
- These two badges (official Council of Europe badge and the specialised Forum badge) must be worn at all times within the Forum premises.

6.3. Media, Photography, and Visibility

- The Forum is a **no-camera** Photography, video recording, and audio recording are not permitted in plenary rooms, breakout sessions, or other indoor discussion spaces.
- Photography, video recording, and audio recording are not permitted in plenary rooms; breakout sessions, corridors or other indoor spaces. The no-camera in designated areas will be identified with signs.
- All individuals present at the Forum – including participants, speakers, facilitators, staff, volunteers, and contractors – are expected to strictly comply with this policy.
- When taking photos or videos in permitted spaces, participants must ensure that individuals who have opted not to be photographed do not appear in the background or are otherwise identifiable in the content.
- Before publishing or sharing any photographs, videos, or recordings, participants are required to review the material carefully to confirm that individuals who have opted not to be photographed are not visible or identifiable.
- If you witness any unauthorized photography, video recording, or audio recording within no-camera areas, or involving individuals who have opted not to be photographed, please report it immediately to the Safety Team.

6.4. Official photographers and accredited media:

- An exception applies only to designated official photographers. Official photographers and accredited media will be present on 4 June (Day 2) and clearly identifiable.
- Photography and filming by official photographers and accredited media remain subject to participants' consent and fully adhere to the "no photo" identification system.

- All official event footage and photographs will be reviewed to ensure that participants who have opted not to be photographed are not visible in the background before publication. After review, official photos will be shared with participants.
- Audio recording is strictly prohibited during the Forum, including for official photographers and accredited media.
- Prior to publishing or sharing any photos or recordings, accredited media are required to conduct appropriate due diligence by reviewing the content to ensure that individuals who have opted not to be photographed are not visible or identifiable in the material.

7. Incident Reporting, Response, and Non-Retaliation

- A designated team is present and identifiable throughout the Forum. This team serves as the primary contact for any safety-related concerns.
- The Safety Team is formed by Forum's co-organisers and coordinating civil society, who will be clearly identifiable.
- Incidents may be reported in person or via email (environment@coe.int). These include concerns related to harassment, discrimination, security threats, breaches of confidentiality, or psychological distress.
- All reports are handled confidentially and with sensitivity. The response prioritises the safety and wellbeing of affected individuals and includes immediate measures where necessary.
- Responses may involve intervention, mediation, removal of individuals from the event, or referral to appropriate services.
- Retaliation against any individual who raises a concern or is involved in an incident is strictly prohibited. This protection extends beyond the duration of the Forum.
- All reported concerns will receive follow-up from the organising team.

8. Reprisal response and forum care

- Risks associated with participation may persist beyond the Forum.
- Participants remain attentive to potential reprisals, including increased scrutiny or pressure upon return to their contexts.
- Incidents can be reported to the Forum's co-organisers through the email (environment@coe.int).

9. Communication about this protocol

- At the beginning of the Forum and throughout the 2 days of the event, the co-rapporteurs and moderator(s) will remind all participants of the need to respect the rules presented in this protocol.