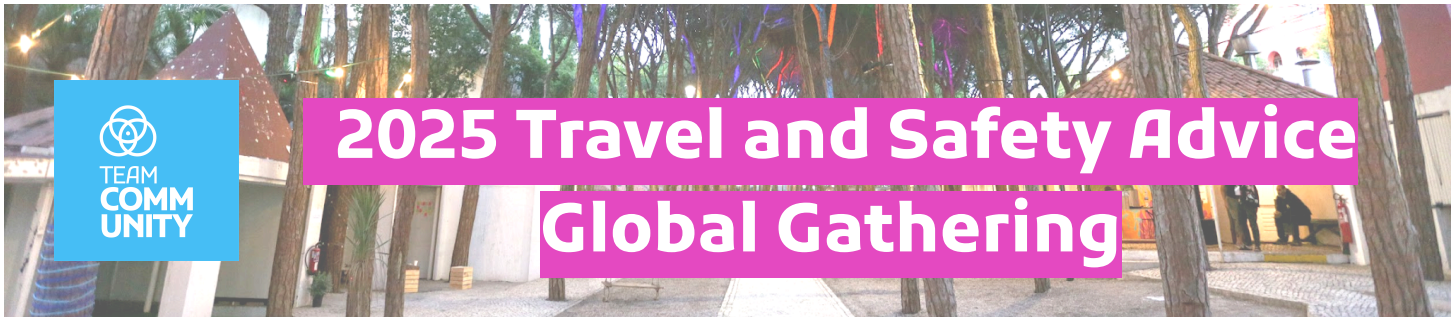

2025 Travel and Safety Advice Global Gathering

Table of Contents

As a participant of the TCU Global Gathering, you will travel to connect with fellow community members. If you need travel assistance, please contact the travel team at Global Gathering visa@digitalrights.community.

1. Travel Risk Updates for the TCU Global Gathering 2025 **2**
2. Before You Travel **2**
a. General Considerations 2
b. Local Emergency Contacts 3
c. Local Laws 3
3. During Travel **4**
a. General considerations 4
b. Border Crossing Considerations 4
c. On Arrival 5
d. Once in the Hotel 5
e. Securing Tech and High-value Items while Traveling 6
4. Re-entering sensitive countries **7**
5. Digital Security **7**
6. Other Resources Available **8**
Travel security guidelines: 8
Risk Assessment: 8
General security resources: 9
Rapid-response helplines (in case of digital security emergencies or incidents): 9
Community Tools: 9
7. Code of Conduct of the TCU Global Gathering **9**

Important Contact Information:

- For urgent matters, immediately call Portugal's emergency number 112. Most operators speak English.
- Team CommUNITY's Signal Phone Number while in Portugal +1-(914) 267-3035.

1. Travel Risk Updates for the TCU Global Gathering 2025

Due to recent policy shifts and socio-political climates in some regions, participants should be aware of evolving risks when planning travel to Portugal for the **TCU Global Gathering 2025**. The following updates are particularly relevant to those traveling from or through regions where civil society actors, activists, and developers may face scrutiny or discrimination:

- **Portugal border controls**: While Portugal remains generally welcoming, recent government actions have tightened immigration enforcement, including a planned expulsion of undocumented migrants and increased scrutiny at entry points. Participants should anticipate stricter questioning and carry **printed copies of invitation letters, hotel reservations, return flights**, and **proof of funding** for their stay. Source.
- **European transit hubs**: Although Portugal is the final destination, **transiting through European countries like France, Germany, or the Netherlands** may also involve **heightened immigration checks**. Be prepared to explain your itinerary and purpose of travel, and carry supporting documents, even if not required for visa-free transit. Source.
- **Avoid transiting through the U.S.**: Due to increased anti-immigration rhetoric and unpredictable border behavior in the United States, participants, especially those from the Global Majority or with activist profiles, are strongly advised to avoid routing flights through U.S. airports if alternatives are available.

2. Before You Travel

a. General Considerations

- Ensure your home is secure while you are away.
- Inform a loved one of your flight information, where you will stay, and your emergency contact abroad.
- If you hold a bank account, notify your credit card company of your intent to travel.
- Pack any medication and prescriptions you may need in your carry-on
- Print a hard copy of your travel itinerary, passport copy, visa information, invitation letter, hotel reservation, and keep it with you in your carry-on.

- Consider traveling with a portable charger or backup battery for devices. **Note:** Some airlines prohibit power banks on board. Please check your airline's policy in advance and plan accordingly.
- Do not post your travel destination or check-in on social media in real time, as it alerts others that you are not home and also reveals your current location.
- Keep electronic copies (or take digital photos) of your passport and visa, credit cards, and other documents that may need to be replaced quickly if lost or stolen.
- If possible, arrange for travel health insurance coverage.
- Try to carry cash with you since many places will prefer it over cards, or cash would be the only payment method available. Euros are the only accepted currency in Portugal. If you anticipate that your local currency will be difficult to exchange in Portugal, try to exchange it before you arrive. Current Exchange Rate here.
- Research the location and contact information for your consulate or embassy before you travel.
- Ensure your mobile phone has roaming capabilities for emergency use, OR obtain a local SIM card upon arrival for in-country communication (**Note**: the local SIM will not work unless your phone is unlocked. You can also bring a backup mobile).
- Confirm you have adequate credit on your local mobile phone.
- Consider using e-SIM providers (e.g., Airalo, Holafly) as a cheap and convenient alternative to a local SIM card.
- Establish a check-in procedure with a team member not traveling with you at specific intervals during your trip.
- Stay informed about local conditions. Recent incidents, such as power outages and transportation disruptions, have occurred in Portugal and neighboring countries. Travelers should stay informed about local conditions and have contingency plans. Source.
- Review current vaccine, health, and visa requirements for your destination using the IATA Travel Centre. This tool provides up-to-date information based on your nationality and travel route.

b. Local Emergency Contacts

- **For urgent matters in Portugal, call the emergency number 112.** Most operators speak some English.
  If you are having a medical emergency, you can call **112** or go directly to the nearest hospital. Check out this list of Hospitals in Portugal. Note that Portugal also has a Healthline (known as

SNS 24) that can be used to obtain general medical advice regarding minor issues: +351 808 24 24 24. **Note**: If you are calling and experience connectivity issues, you can also visit sns24.gov.pt for online services or to access support via the **MySNS app**.

- If you need visa or emergency travel support, you can reach Team CommUNITY on the following Signal number: +1-(914) 267-3035
- If you wish to report a code of conduct violation, you can report on the following Signal number: +1-(347) 646-0379 or by emailing codeofconduct@digitalrights.community.
- For security guidance, particularly for individuals from high-risk countries or regions, please contact the Team CommUNITY Security Team's Signal number: +44 7388 469193.

c. Local Laws

VPN: There are no laws against using a VPN for legal purposes in Portugal.

Alcohol: Drinking alcohol in public is not forbidden in Portugal.

LGBTQ+: Same-sex relations are legal in Portugal, and discrimination based on gender identity and sexual orientation is illegal. Source.

Drugs: If you have prescription medications, ensure you are traveling with a copy of the prescription. Possession of recreational drugs for personal use, below a certain amount, is not criminally sanctioned. Source**. Please note:** While Portugal has decriminalized limited personal possession of certain drugs, the use of any drugs at the Global Gathering is strictly prohibited to ensure the safety and well-being of all participants.

3. During Travel

a. General considerations

- Do not pack prohibited items and/or items that may be seen as suspicious or contrary to either your home government or the government of Portugal.
- Avoid storing valuables such as laptops, cell phones, money, and jewelry in checked luggage. Distribute valuables within your carry-on, keeping cash and credit cards separate to mitigate theft risk.
- Always keep essential items with you (passport, electronic devices).
- Attach luggage tags to checked bags, omitting sensitive personal info (address, work email, job title, company). Do not openly display this information anywhere on your luggage.
- Confirm with the ticketing agent that your luggage has been checked through to the final destination.

- Avoid sharing unnecessary details about travel plans, hotel, meetings, etc, during transit conversations. In addition, do not share your information or the purpose of your trip unnecessarily with strangers.
- While Portugal is generally safe, it is wise not to count cash in public or discuss it openly.
- Keep your devices well-charged. Some flights do not have charging ports, so it is recommended that you bring a power bank so that you will not be without power when you land.
- Upon entering the country, be prepared to discuss travel purposes, duration, accommodations, etc., if immigration authorities inquire. Avoid carrying sensitive items that could prompt further questioning or searches. Review additional Border Crossing Considerations.

b. Border Crossing Considerations

This information is shared solely to assist with border crossing considerations. The final decision regarding an individual's entry into a foreign country lies with local authorities. If you have inquiries or apprehensions regarding your international travel, please do not hesitate to reach out for assistance and contact visa@digitalrights.community.

Mitigating Risk of Detention or Arrest

While some of the risks associated with detention or arrest at a border crossing are not within an individual's control, some actions can be taken to minimize the risk and prepare for potential inquiries or requirements:

- **Research all entry and exit requirements:** Familiarize yourself with entry and exit requirements, and ensure essential materials like visa information, insurance, accommodation details, invitation letters, and registration certificates are printed out prior to travel, which can aid in case of border scrutiny.
- **No photographs:** Do not take pictures at airports or of official government/military installations in any country. Delete any such photos from your phone before crossing borders or checkpoints.
- **Backup of critical documents:** Always maintain photocopies and digital backups of key travel materials such as your passport or national identification card.
- **Purpose of travel:** Clearly articulate your travel purpose and be ready to provide supporting information if officials request it. This includes explaining your entry or departure rationale and the applicable visa type.
- **Attitude:** Remain polite and courteous with all immigration officials. Remember that they are ultimately in control of border crossings.

- **Sensitive materials:** Do not travel with any materials or items that may be illegal or sensitive in another country.

If questioning, arrest, or detention occurs

The following recommendations offer guidance to consider in the event of an arrest or detention situation during international travel:

- ➔ Stay calm and avoid getting defensive or angry with authorities.
- ➔ Ensure you retain possession of your identification documents and request to hold onto them. If declined, avoid resistance.
- ➔ Ask for a translator if you do not speak the local language.
- ➔ If further engagement or responses are required, request to consult with legal counsel. Avoid signing anything without legal consultation and a translation in a language you understand.
- ➔ Ask for communication to be made with your Embassy.
- ➔ Exercise caution before immediately handing over personal belongings (such as a laptop, tablet, cell phone, luggage, wallet). If requested, politely inquire about the authority to confiscate. If insistence persists, comply.
- ➔ If devices are retained/confiscated and you believe they might have been searched without your presence or awareness, try to check the times when they were taken and returned to you.
- ➔ Attempt to note down the names and contact details of the authorities overseeing your case.

RETURNING TO THE UNITED STATES (non-U.S. citizens)

U.S. Customs & Border Protection (CBP) officers may inspect your luggage and the full contents of your electronic devices without a warrant at any port of entry, using advanced forensic searches that can copy your data and keep it for up to 15 years. Refusing to unlock a phone can result in secondary inspection, device seizure, or even denial of entry for visa holders. In some cases, officers may deny admission or initiate expedited removal proceedings, which can lead to deportation even for travelers with valid visas or green cards. How to prepare:

- ➔ Travel, if possible, with a "clean" or loaner device.
- ➔ Back up and remove sensitive files; keep the device encrypted and powered off while in transit.

- ➔ Review social media content, including saved items (e.g., posts, memes, videos), especially if they may be perceived as political or critical of U.S. policies.
- ➔ Sign out of, or uninstall, social-media and messaging apps you don't need.
- ➔ Disable biometric unlock, and use a strong password instead.
- ➔ Carry hard-copy proof of status (I-20/DS-2019, EAD, green card).
- ➔ If taken to secondary inspection, stay calm, ask to call an attorney, and note the officer's badge number.
- ➔ **Regulations change quickly;** consult the latest CBP policy or an immigration lawyer before departure. Good resources include the FAQ EFF Border-Search Pocket Guide, and the ACLU's Enforcement at the Airport.

c. On Arrival

- **Exchange money:** Before you leave the airport, exchange some money into local currency (at least double the amount of a taxi fare).
- **ATM and currency exchange:** Cash can be taken out at ATMs inside the airport, and other currencies can be exchanged at the airport if you arrive during the day.
- **Taxis:** Taxis from Lisbon Airport are generally reliable and trustworthy. Most taxis do not accept credit cards, so you must pay in cash. The cost of a taxi from Lisbon Airport to Estoril (Fiartil) is around 30 euros, but it may be more or less depending on traffic. Make sure to ask to put on the meter.
- **Wi-Fi and SIM cards:** Free Wi-Fi is available at the airport and in many restaurants and cafes. Temporary data or phone SIM cards can be purchased from any major provider (MEO, Vodafone, NOS). There is a Vodafone vendor in the airport arrivals area. For more information about the internet in Portugal, visit: Internet in Portugal.
- **Risk of Pickpocketing at Lisbon Airport:** Pickpockets have been known to operate actively in and around Lisbon Airport. We advise all travelers to remain vigilant upon arrival.
- **Ground travel options:**

  Train and Bus: More information can be found at Rome2Rio.

Uber / Bolt: Uber and Bolt are available from the airport, but less easy to locate. The pick-up area is in the P2 parking garage, and the Kiss&Fly area near departures.

d. Once in the Hotel

Ensure the safety of your belongings by following these precautions during your stay:

- Stay close to your luggage during check-in and keep your personal bag or backpack within reach.
- While checking in, avoid loudly sharing your name and reservation details. If your room number is mentioned aloud, consider requesting a different room or call the front desk for a change after settling in.
- Remove the sleeve containing your name and room number from the room key and keep them separate.
- Acquaint yourself with your room and floor, noting phone locations, the presence of connecting doors, window locks, fire exits, and escape routes.
- Avoid leaving housekeeping requests on your door, as this signals the room is unoccupied. Instead, call for housekeeping when needed.

e. Securing Tech and High-value Items while Traveling

Whether traveling internationally or around a city, it is critical to safeguard your technology. Device and valuable theft are a global concern, irrespective of location. The practices below empower you to enhance security for you and your possessions as you navigate event venues, towns, flights, or local trips.

Only travel with work devices (i.e., laptop, phone, tablet) or other devices when your organization explicitly approves. Items are safest in the office or personal homes and least safe in transit. If you are carrying high-value items or technology, consider these mitigation measures:

- **Be aware of your surroundings.**

  Never leave devices and high-value belongings alone, even for a short period of time. Avoid publicly showing off your phone, tablet, or laptop, or taking it out in unfamiliar places. Keep them out of sight of others and store them in a non-transparent bag.

- **Secure your equipment.**

  Devices should be fully powered down and not kept in 'sleep' or 'hibernation' mode when not in use. They should also be powered down before leaving the home or office.

- **Exercise caution on public transport.**

  Whenever possible, avoid using work-sponsored devices or high-value items on public transportation. If unavoidable, travel before sunset to avoid using equipment after dark. Keep items close, ideally on your lap, and hidden from others' view. As a last resort, if items must be left in a vehicle briefly, ensure doors are locked, covered, securely stowed, and well out of sight. Confirm doors and windows are locked when leaving.

- **All high-value/work-sponsored devices must be password-protected and encrypted to protect personal and confidential data.**

  Make a habit of ensuring your files are stored in the cloud so that, in the event of a loss or theft, you only lose the hardware. Record your devices' serial numbers and store them in a safe place. Serial numbers can be used to identify your belongings in the event a device is stolen and later found. If your device is lost or stolen, remember to report it to the police if possible.

What are low, medium, and high risk areas?

Low Risk: Basic security measures are sufficient in most cases.

Medium Risk: Risk level is elevated due to factors like increased cybercrime rates, potential for targeted attacks, or the presence of organized threat actors.

High Risk: These areas are characterized by high cybercrime rates, advanced security threats, and potential for surveillance by malicious actors. Comprehensive security measures are necessary to mitigate risks.

It is important to note that individual risk factors, such as the nature of the attendees' work, personal connections, and the sensitivity of the information we manipulate, can also influence the overall risk level.

The key is to assess your risk level based on your origin and take appropriate steps to mitigate threats. Consult with our security professionals if you have specific concerns. Stay vigilant and prioritize protecting sensitive data and communications.

4. Re-entering sensitive countries

Political contexts: Participants traveling from countries with restrictive laws, particularly LGBTQ+ activists or those working in human rights, may face additional scrutiny when traveling or upon return. While the TCU Global Gathering is a non-political, community-based event, we recommend the following precautions:

- **Re-entering countries with autocratic governments**. Activists returning to their home countries may be questioned about their participation. If needed, you may request an anonymized confirmation of attendance from the Global Gathering team.
  - Prepare template answers for "Why were you in Portugal?" (e.g., for a tech community event, not a political gathering). For example: "I attended a community event on digital tools and learning."

- **Consider additional precautions.** If you anticipate risks due to your identity or professional background. If you have questions or concerns, don't hesitate to contact our support team before or after your trip.

5. Digital Security

Risk levels refer to the origin of the traveler's country. The risk level in Estoril, Portugal, is low.

Low Risk

- **Keep devices secure.** Always keep your devices with you and avoid leaving them unattended in public places.
- **Be wary of suspicious emails.** Be cautious of emails related to your travel, especially if they contain links or attachments. Verify the source before opening.
- **Keep your devices updated with the latest security patches and features**. This means regularly updating your operating system, browser, and other software. However, try not to perform these updates while connected to untrusted networks, such as airport Internet. Just as you should be suspicious of unusual emails, be cautious of updating your devices on public or untrusted Wi-Fi networks to prevent potential security risks.
- **Use strong, unique passwords for all accounts and store them in a password manager.** These tools can also help you create complex passwords. To add an extra layer of security, enable two-factor authentication (2FA) wherever possible, and avoid using SMS as your second factor.
- **Be cautious of public Wi-Fi networks and consider using a VPN**. Public Wi-Fi networks can be vulnerable to hacking. Consider using a Virtual Private Network (VPN) to encrypt your internet connection and protect your data.
- **Avoid accessing sensitive accounts or information on public computers**. Public computers can be compromised with malware or keyloggers. Avoid accessing sensitive accounts or information on public computers.
- **Back up your data regularly in case your devices are lost or stolen**. Regularly back up your data to a secure location, such as an external hard drive or cloud storage service, to ensure you can recover your data in case your devices are lost or stolen.

Medium Risk

- **Use a dedicated travel device.** Consider using a separate device for travel that has minimal sensitive information stored on it.

- **Enable full disk encryption**. Encrypt your device's hard drive to protect data in case of loss or theft.
- **Be cautious of shoulder surfers**: Be aware of your surroundings when accessing sensitive information, such as passwords or financial data.
- **Avoid discussing sensitive topics in public.** Refrain from discussing sensitive topics, such as business or personal secrets, in public places where you may be overheard.
- **Encrypt sensitive data on your devices and use full disk encryption if possible.** Using software like TrueCrypt or BitLocker.
- **Be extra vigilant for shoulder surfers and eavesdroppers when accessing sensitive information**. Be aware of your surroundings when accessing sensitive information, such as passwords or financial data. Avoid sharing sensitive information in public places.
- **Consider using a privacy screen filter on your devices**. Use a privacy screen filter to prevent others from viewing your screen, which can help protect sensitive information.

High Risk

- **Encrypt communications.** Use end-to-end encrypted messaging apps like Signal or WhatsApp to protect your communications from interception.
- **Be aware of potential surveillance**. Be mindful of potential physical surveillance and take countermeasures such as using secure communication methods and avoiding discussing sensitive topics in public.
- **Be prepared for the possibility of device seizure or interrogation at borders.** Be ready for the possibility of device seizure or interrogation at borders, and have a plan in place for how to handle such situations.
- **Consider using a burner phone to minimize risk to your primary devices**. If you need to use a device in a medium-risk area, consider using a burner phone that can be easily disposed of or wiped clean if compromised. Use a dedicated secure device for travel that is wiped clean before and after the trip to minimize the risk of data compromise.
- **Consider leaving sensitive devices at home and only bring what is absolutely necessary to minimize the risk of data compromise.**

6. Other Resources Available

While we are not experts in travel security, we have compiled a list of recommendations that covers a range of essential aspects to consider both before and during your trip.

Travel security guidelines:

- Travel Security Guide - Grey Dynamics
- Travel Security Guide - Clayton University
- Travel Security Guide -Embassy of Canada
- Travel Security Guide -LinkedIn

Risk Assessment:

- Risk matrix assessment - Hong Kong Emergency Response Team
- Risk matrix assessment - National Institute of Standards and Technology.
- Guide to Getting Started with a Cybersecurity Risk Assessment - Cisa Safecom
- Assessment tool and personalized digital safety plan for individuals

General security resources:

- Tactical Tech's Data Detox Kit, a detailed guide to reducing your digital trail.
- Totem Project Courses for free, self-paced sessions on the basics.
- Freedom of the Press Foundation digital security guides and trainings
- EFF's Surveillance Self-Defense
- The holistic security manual by Tactical Tech, for a holistic approach to your security strategy.
- Shelter City resources for human rights defenders.

Rapid-response helplines (in case of digital security emergencies or incidents):

- Access Now Security Helpline
- Front Line Defender Emergency Contact
- SMEX Digital Safety Helpdesk (MENA-focused)
- Get Help - DefendDefenders

Community Tools:

- Digital Security Community Directory for compilation of tools and resources available.
- For organizational-security-focused resources

7. Code of Conduct of the TCU Global Gathering

https://wiki.digitalrights.community/index.php?title=Code_of_Conduct