COP30 Guide

Brazilian Context & Holistic Security for COP Participants

CliDef
Global Climate Legal Defense

ARAYARA.org

Table of Contents

Introduction

Guide To Brazilian Context and Holistic Security for COP Participants

Designed for climate advocates and activists attending COP 30 in Brazil, this Guide provides information about the Brazilian context, legal framework, rights, culture, and available resources to navigate the local landscape; and an overview of information/digital and physical security issues, with suggestions for how to protect your information and remain safe before, during, and after COP 30.

We hope this guide enables activists, advocates, and others attending COP 30 to make informed decisions about their actions while in Belém, Pará, Brazil.

Part One: Know the Context

Brazil has seen increasing pressure on civic space in recent years, particularly in regions where environmental and indigenous rights defenders challenge powerful economic interests—most notably in the Legal Amazon. Documented incidents of surveillance, threats, and criminalization against local activists highlight the risks faced by those working on the ground. While it is unlikely that visiting delegates would be directly targeted, it is important to remain aware of these dynamics, particularly when engaging in solidarity actions or activities outside the formal COP30 venues.

While Brazil does not systematically criminalize or harass activists attending international events like COP, individuals with a history of violent protests or links to criminalized groups should be cautious as they could face heightened scrutiny from law enforcement or intelligence services. However, it is still possible that security protocols may be reinforced at points of entry, especially in the lead-up to a major international conference. As with any international travel, standard precautions are advised.

This Guide offers an overview of the legal,security, and cultural context for COP 30, with the aim of helping participants make informed decisions about how they engage before, during, and after the conference. It includes a set of holistic recommendations adapted to the Brazilian context and the specific realities of Belém and the surrounding region.

Additionally, legal advice will be available to COP30 attendees through the CliDef legal hotline, and safety and security support will be provided by the Safety Hub. This shared infrastructure is designed to ensure that all participants—whether local or international—can engage meaningfully and safely throughout the conference.

Introduction & Key Risks

1. **While participants should not expect systematic targeting or harassment from authorities, attending COP 30 in Belém may still pose certain risks**—mainly related to logistics, urban crime, and general safety. With thoughtful planning and preparation, participants can minimize these risks and focus on their engagement at the conference.
2. **Activists traveling to Brazil are unlikely to face major scrutiny at the border, especially if they are formally registered for the conference and carry the appropriate travel documentation** (e.g., visa if required). Still, taking standard precautions—such as minimizing sensitive data on devices, using secure communication tools, and storing backups before travel—is recommended for all international travel.
3. **Most safety concerns are expected to arise outside the official COP 30 venues and programming**—particularly during transit, in larger urban centers, or when visiting other parts of the country before or after the conference, particularly more remote areas in the Brazilian Amazon.
4. **During COP, the venue is divided into two key zones: the Blue Zone and the Green Zone.** The Blue Zone serves as the core for UN-related activities, including official meetings and negotiations. Its security is managed by the United Nations Department of Safety and Security (UNDSS). In contrast, the Green Zone offers a platform for broader dialogue where organizations, companies, NGOs, and academic institutions can share ideas with global stakeholders. Security in the Green Zone is overseen by the host country's authorities and participants should abide by local laws.
5. **As the Blue Zone is considered international territory—and international human rights norms are therefore notionally adhered to—arrests and detentions by UNFCCC security**

forces are very unlikely, though still possible if activists are deemed to be causing disruption or inciting violence.

6. **While participants should not expect systematic surveillance by the Brazilian government during COP 30, it is important to remain aware of the broader security environment—especially with regard to criminal activity.** Petty crimes such as pickpocketing and cellphone theft are common in many urban areas in Brazil, and in some cases these incidents can escalate into violence. These risks are generally higher outside the official conference venues and in crowded public spaces, especially at night.
7. **The risk of traffic or boat accidents and medical emergencies should be taken into account.** Familiarize yourself with local emergency services, carry essential medical information and any necessary medication, and plan ahead for reliable transportation, especially when moving around unfamiliar areas.
8. **Brazil's public health system (Sistema Único de Saúde—SUS) generally provides decent emergency care in urban areas, particularly for emergencies, and visitors can also access it if needed.** However, public hospitals can be crowded, and wait times may be long. In more remote or rural areas, access to quality medical services may be limited, so it is advisable to have medical insurance. Seeking care in private hospitals and larger cities might be needed / advisable in some cases.
9. **Remain vigilant during your time in Brazil, especially if you plan to stay beyond the official COP 30 dates or travel to other parts of the country.** While international participants are not likely to face backlash or reprisals after attending COP 30, those engaging in high-profile actions—particularly in regions with environmental conflicts—should be mindful of local dynamics, including tensions with authorities or private actors.

10. **Attendees are not expected to face surveillance or criminalization simply for participating in COP 30.** However, as in any international setting, it is important to understand the local context, maintain good digital hygiene, and assess any potential risks based on your own visibility, profile, and activities during and after the event.
11. **Being aware of and preparing for these risks can help participants navigate the conference and their stay in Brazil more safely.** The upcoming CliDef webinars aim to support participants in understanding their baseline risks and adopting appropriate measures to prevent incidents before, during, and after COP 30.

Part Two: Know the law in Brazil

How to prepare for public demonstrations and events

Introduction

Brazil's bid to host COP30 represents its desire to showcase the country's political stability and democratic governance against a backdrop of an accelerating climate crisis. The Brazilian government expects more than 40,000 visitors to attend COP, including around 7,000 people from the United Nations (UN) teams and delegations from member countries.

Given the scale and significance of the event, Brazil anticipates intense media coverage, which will shine a light on its international image. The Brazilian government expects the active participation of civil society, so security forces will seek to ensure a democratic and welcoming atmosphere. Nevertheless, activists should be prepared to take measures to ensure their own safety, particularly in public spaces and at public events.

In addition, it is important to observe measures that ensure data security, information security, and internet access security. Check out Part 3—Holistic Security—especially the topics related to digital and information security.

Use and possession of drugs in public

In 2024, the Federal Supreme Court of Brazil (STF) ruled that it is not a crime to buy, store, transport or carry up to 40g of marijuana for personal consumption. **However, during demonstrations and public events, the possession or use of illegal drugs, even in small quantities, can draw unwanted attention from police, who may be looking for a reason to repress protests.** False accusations of drug trafficking can occur if the quantity is large or if the drugs are shared with other people. The penalty for drug trafficking is between 5 and 15

years in prison, while association to drug trafficking carries a penalty between 3 and 10 years in prison. In addition to legal repercussions, drug use and possession may also be used against activists to damage their reputation or discredit their work.

Dialogue with the police: conflict prevention and/or management

At a public protest or event where police intervene, it is useful to pay close attention to the movements made by police groups, and identify the person giving instructions so that you can identify any potential risks or instructions to follow. It's important to remember that you have rights, but in escalating or violent situations, it's best to avoid confrontation.

If you come into direct contact with police, it’s to your advantage to remain calm and don't disobey, slander, insult, or threaten the officers. If someone is being arrested, don't try to stop it. You can ask questions about what is happening or why, but refrain from publicly criticizing or offending the police, as this constitutes the crime of contempt and could also lead to your arrest.

Disrespect for police authority

As noted above, Brazil still criminalizes disrespecting the authority of a public official while in the exercise of their function as a crime of contempt, with a penalty of detention from six months to two years or a fine.

The elements of the crime are: "(i) it [the offense or disrespect] must occur in the presence of the public official; (ii) the offense must be related to the exercise of the [police] function; (iii) the offense must prevent or obstruct the public official from performing their functions; and (iv) if the police official’s conduct is excessively belligerent, that must be taken into account.

It is important to note that filming police action in public spaces does not constitute contempt. However, although filming is not prohibited, keep in mind that it could provoke a negative reaction from the police.

Disobeying an order issued by a police officer also constitutes the crime of disobedience, which carries a penalty of detention from fifteen days to six months, and a fine.

How to act in a police approach

The police generally intervene in situations that pose a public risk and not as a way of stopping a peaceful protest. The police cannot arrest demonstrators when they are acting legally, but they can detain you for a few minutes to “check” what you are carrying, such as bombs, weapons, drugs, etc. The search, whether of you or your belongings, must be carried out in the presence of everyone, and the personal search must be conducted by a police officer of the same sex.

It is common for police to ask demonstrators to unlock their cell phones. However, since it is illegal to access cell phone data without prior judicial authorization, you have the right to refuse unlocking, but evaluate the context and potential consequences. If protecting your information is a security issue, insist on your right to privacy. However, if you are being threatened, attacked, or feel your physical security is at risk due to the police, consider agreeing to the request. If you prioritize your safety, you can still seek redress later for the violation. To that end, it would be important to record the identity of the police officer so that you can seek accountability.

How to act in the event of an arrest

You can only be arrested while committing a crime or by court order. Those making the arrest must identify themselves and have their name, rank, and position on their uniform. If they don't give their name or it's not possible to identify them by their uniform, you have the right to ask. The officer must explain the reason for the arrest. If they don't,

ask and show that you are not resisting by raising your hands. Then ask to be put in touch with a lawyer you trust.

If you are injured, seek or ask to seek immediate medical attention, even before going to the police station. If you have been physically assaulted, ask to be taken to the IML (Forensic Medical Institute) for a forensic examination. This examination is essential if you want to file a claim against the state.

If you are taken away to be detained, ask which police station you are being taken to and record the license plate number of the police car taking you there. Only answer questions that refer to your personal details. Don't argue with the police, because their job is just to take you away. If you are being arbitrarily arrested, you will have the opportunity to challenge this later.

Again, you have the right to be informed of the reason for your arrest, the right to remain silent and not to produce evidence against yourself, the right to be accompanied by a lawyer, and the right to communicate your arrest to a relative or person of your choice.

If you don't have the financial means to pay for a lawyer, you should request a public defender, who will provide full and free legal assistance. It is your right to communicate with a lawyer, family member, friend, or anyone you trust in private. Your belongings can be handed over to your lawyer or family member if you wish. Arrests during the commission of a crime must be reported immediately to the competent judge, the Public Prosecutor's Office, and the family of the prisoner or the person they have nominated. It is your right to be released if there is insufficient evidence to justify the arrest. If you remain in detention, you must be housed in decent conditions and must not be physically or psychologically mistreated.

If you are not brought before a competent judge within 24 hours, the arrest must be revoked. At the hearing, the judge will verify the legality of the arrest and decide whether you will remain in detention or go

free. The judge will also assess whether there has been police abuse, torture, or inhumane treatment.

What to do if you witness or experience police violence

If you witness aggression by police officers, protect yourself and try to get any victims away from the scene. But don't do it alone; always try to have more people who can act as witnesses. The more people there are, the less chance there is of the abuse continuing. In the event you witness police misconduct, you should have a lawyer with you before intervening with the police.

When possible, give a detailed account of what happened in writing and try to remember the names of other witnesses, who can help to contact the competent bodies, such as ombudsmen, ombudsmen's offices, public defenders and public prosecutors and can also serve as witnesses to them. Calm the victim down. In the event of a medical emergency, find a team that can provide first aid and/or call the Mobile Emergency Assistance Service (SAMU) by dialing 192, which is a free service that operates 24 hours a day.

In Brazil, registering a police report (BO) is a free procedure. You can go to the nearest police station with a photo ID (or passport) and provide information about the incident: date, time, location, detailed description, possible witnesses or suspects. If possible, provide evidence (documents, photos, messages, videos). After registering, you can ask for a copy of the police report. There are also specialized Tourist Support Police Stations, which investigate criminal offences committed against tourists.

Dispersal From the Public Act

When dispersal is a collective decision by those who are protesting, remain calm and leave in an organized manner, follow prior arrangements and check that everyone in your group is okay.

Forced dispersal can only be ordered by the law enforcement officer who is in charge of the crowd control. Non-lethal instruments and those of lesser offensive potential should not be used in peaceful demonstrations. Use of these instruments is considered a last resort, after a verbal warning with clear instructions and sufficient time for the demonstrators to disperse safely.

In the event of the use of tear gas or pepper spray, it is important that you get out of the gas cloud and move away as soon as possible. Do not crouch down or lie on the ground. If you come into contact with the gas, it is best not to run but rather move away calmly. Also, don't rub or scratch your eyes, as this can make the effects worse.

Local medical services must provide immediate medical assistance whenever the use of force results in injury. Additionally the relevant authorities, usually local law enforcement or medical assistance providers, must notify the victim’s family or the appropriate contact of what has occurred.

Police are not legally permitted to use force beyond what is strictly necessary to address the threat. Police action must not discriminate against any person on the grounds of color, race, ethnicity, sexual orientation, language, religion, nationality, social origin, disability, economic status, political opinion or otherwise.

In sum: If you are forced to disperse, protect your airways and don't run into alleys or dead-end streets. If someone is detained, immediately contact your legal network. After the dispersal, send an "I'm safe" message to your security network.

National and international standards on freedom of expression, right to protest and demonstration

Freedom of expression

The Brazilian Constitution guarantees everyone the right to freely express thoughts, opinions and information, and prohibits prior

censorship in any form. It also prohibits anonymity, each individual is required to take responsibility for what they say or publish. It is permitted to express political, religious, philosophical or personal opinions, including harsh criticism of the government, institutions and public figures. It is also legitimate to publish journalistic, academic and artistic content, even in provocative or satirical language.

Public criticism of individuals and groups is protected, as long as it does not incur slander (false imputation of a crime), defamation (imputation offensive to reputation) or libel (offense to dignity). Speaking out on social media is also permitted, as long as the existing laws and the fundamental rights of others are respected. It is not allowed to spread hate speech, personal insults, incitement to violence, discrimination or crime. It is also forbidden to disseminate disinformation with serious harmful potential, such as fake news that undermines the integrity of elections, public health or the safety of the population.

It is therefore permissible to criticize, protest, denounce and express opinions, including in a direct and public manner. What is not allowed is to use this freedom to offend, slander, spread intentional lies, incite hatred or violate the fundamental rights of other people or vulnerable groups.

The right to assembly, association, protest and demonstration

In Brazil, everyone has the right to assemble peacefully (without weapons), in places open to the public, regardless of authorization, as long as they do not frustrate another meeting previously convened in the same place. Full freedom of association is guaranteed for legal purposes, and state interference in its internal functioning is prohibited. Although the Brazilian Constitution dispenses with prior official permission to exercise the right to assembly, prior notice to the authorities is required for reasons of organizing public security—it cannot be a cause for censorship or blocking rights.

The right to protest is a fundamental expression of democracy and must be fully protected. In Brazil, it is not necessary to obtain official permission for a demonstration or a public act. However, the organizer must inform the authorities about the planned event. The Federal Supreme Court has recognized the legitimacy of protests, including those of a political or protest nature, considering that repressing manifestations is an affront to freedom of expression and democracy.

International courts to which Brazil is subject, such as the Inter-American Court of Human Rights, also reinforce this protection, emphasizing that peaceful protests must be respected even in contexts of crisis or repression. It is essential to differentiate between legitimate acts of protest from isolated acts of violence – which does not justify generalized repression.

Public acts: authorization and informing the authorities

Under Brazilian law, it is not necessary to ask for prior authorization to hold a public act, but it is mandatory to notify the authorities in advance, typically this is the Military Police (PM/PA) or the secretary of the state who is in charge of public safety. This notice must contain minimum information about the event, such as the date, time, place of concentration, route (if there is to be travel) and estimated audience. If this communication is not made, the demonstration is not automatically illegal, but may be subject to preventive or coercive measures if it creates a risk to public order or security.

Under no circumstances can the state prevent, censor or dissolve a public act based on its political or ideological content. The state's use of force is only legitimate in exceptional situations and must comply with the principles of legality, necessity, proportionality and minimum intervention.

In short, the demonstration must be peaceful, without weapons and must not frustrate another meeting previously scheduled in the same place. The state must guarantee security and protect the exercise of this right, and can only intervene with legal, proportional and

well-founded justifications. Undue repression, disproportionate use of force or abusive control of demonstrations constitute human rights violations.

Action by NGOs and social movements

At COP30, civil society organizations have the right to actively participate in the climate debate. NGOs, movements and collectives can organize campaigns, side events and symbolic protests to raise issues such as climate justice, environmental racism, indigenous rights and energy transition. This action is legitimate and provided for in international protocols, as long as the event's accreditation criteria and security standards are respected. These demonstrations can take place in official COP spaces (pavilions, side events and thematic meetings), through accreditation with the UNFCCC (UN Framework Convention on Climate Change), observing the registration and representation criteria defined by the organization of the event.

Within the framework of COP30, social organizations can participate in the construction of common agendas, make public complaints, deliver shadow reports, promote symbolic acts and dialogue with national and international delegations, always respecting the security protocols established by the Brazilian authorities and UN bodies. Any attempts to criminalize peaceful mobilizations or arbitrarily restrict the presence of these entities would constitute a violation of the Brazilian constitutional order and the state's international obligations before the regional and universal human rights systems.

Demonstration on social media

Demonstration on social media includes posts, comments, virtual campaigns, live broadcasts, memes and other digital communication resources aimed at criticizing, mobilizing or disseminating political, environmental, social and cultural ideas. Civil society organizations, activists, popular communicators and citizens have the right to take a public stance, including a critical one, on the issues debated at the

Conference, without prior censorship, content control or arbitrary state interference.

In the digital environment, demonstration is subject to the same constitutional limits applicable to communication in any other medium. This means that anonymity is not allowed for the commission of illicit acts, nor is the malicious propagation of disinformation, slander, defamation, libel or incitement to violence.

NGOs and social movements can use social media to disseminate agendas, mobilize protests, expose rights violations and pressure authorities, as long as they comply with the legal frameworks in force. The same applies to videos, texts, cartoons and other communication resources used to denounce environmental racism, territorial violations or practices contrary to climate justice.

Religious freedom

The Brazilian state is officially secular, which means that it does not favor any religion and must guarantee equal treatment for all. The realization of this right faces significant challenges when it comes to non-hegemonic religions, particularly those of African, indigenous, riverine origin and other expressions linked to popular spirituality and Amazonian ways of life.

It is important to understand that many religious practices in Brazil take place outside temples and churches, in open spaces such as rivers, forests, squares and communities. Afro-Brazilian religions such as candomblé and umbanda, as well as indigenous and riverside spiritualities, perform rituals with dances, songs, offerings and the use of natural elements, often in places considered sacred by these communities.

These demonstrations are protected by law and cannot be repressed, ridiculed or treated as illegal. However, these religions have historically faced prejudice, discrimination and even violence. It is forbidden to film or photograph rituals without authorization, as well as to interfere

or make derogatory judgments. Any form of religious intolerance is a crime.

Rights of LGBTQ+ people

In Brazil, LGBTQ+ people have guaranteed rights under the Constitution, which ensures the dignity of the human person, equality, non-discrimination and the right to free expression of personality. During COP 30, all forms of demonstration of gender identity and sexual orientation must be respected, including the free expression of affection, use of a social name, choice of clothing and language. Failure to respect these demonstrations may constitute discrimination and violate the human rights protected by Brazilian law and international treaties ratified by the country.

It is forbidden to prevent LGBTQ+ people from accessing public or private services on the basis of their identity; to embarrass them because of their appearance or way of expressing themselves; to commit physical, verbal or symbolic violence; and to deny them service, including in commercial establishments, hotels, means of transportation or religious spaces. Discrimination against individuals who identify as LGBTQ+ is considered a crime in Brazil, covering discrimination based on gender identity and sexual orientation. Cases of violence should be reported to the local authorities, and victims have the right to legal, psychological and medical assistance.

Rights of racial minorities and indigenous peoples

Brazil is committed to promoting racial equality and repressing racism in all its forms. Despite this, discrimination and racial profiling by public security agents still affect the black and indigenous population, as they may face racial profiling, targeted attacks, searches and arrests, including in the context of demonstrations.

Racial insult is an individual offense linked to race, color, ethnicity, religion or national origin. Racism is the practice of generalized or institutional discrimination against a group of people. Both are crimes

that should be reported to the police and/or other competent authorities.

As for indigenous peoples, the rights to autonomy, free determination, prior, free and informed consultation, the right to live according to their cultures, as well as the duty of the state to, among other things, safeguard the people, institutions, goods, cultures and environment of these peoples are protected.

Criminalization and persecution

In recent years, Brazil has witnessed a worrying use of the law as a tool to intimidate environmental activists and defenders. Instead of protecting those who act in defence of collective rights, legal instruments have been used to criminalize social mobilization. One example is the Parliamentary Commissions of Inquiry (CPIs), which, under the pretext of investigating environmental crimes or the actions of NGOs, end up exposing leaders to political persecution and delegitimization campaigns.

A number of environmental defenders, especially those linked to indigenous, quilombola and riverine causes, have been the target of unfounded investigations, abusive surveillance and lawsuits that are not backed up by concrete evidence. These practices not only violate the right to freedom of expression and association, but also create an environment of fear, which hinders the legitimate engagement of civil society on urgent issues such as the climate crisis.

The Role and Rights of Lawyers

Acting as a lawyer before the public security forces

In the context of acting as a lawyer, accompanying the demonstration is important in order to ensure that it takes place and to avoid arbitrary arrests. Lawyers have the right to unrestricted access to the person they are representing, so no authority can prevent them from talking to

the person they are representing in private. If the person has been assaulted, the lawyer may ask for a forensic examination to be carried out. The lawyer will have the right to know the charges made and the evidence alleged, and may argue that there is no evidence to support an arrest in flagrante.

When accompanying the detained person to the police station, family members and/or colleagues should be instructed to provide documentation for the custody hearing. These documents are: proof of residence and proof of study/work. In the case of foreign nationals, this can include student ID, letters from employers and all relevant immigration documentation. The lawyer in charge must receive the documents before the custody hearing in order to seek provisional release.

In the event of an arrest, the custody hearing must take place within 24 hours of the arrest. There, the judge must assess the legality of the arrest, whether there has been police abuse, torture or inhumane treatment and decide whether the person will remain in custody or go free.

Lawyers should be able to fully defend their clients, with independence and autonomy. Their rights include freedom to act; inviolability of the workplace, documents and communications relating to the exercise of the profession; communication with an imprisoned client, personally and privately, even without a power of attorney; free transit in forums and courts; access to case files, even without a power of attorney; attendance at proceedings and hearings; and viewing of judicial or administrative proceedings of any kind.

Constitutional remedies

Constitutional remedies are essential for the immediate defense of freedoms and guarantees that have been threatened or violated. They allow direct access to the Judiciary, including urgent requests.

Habeas Corpus (HC) can be used to protect freedom of movement. Anyone, even without a lawyer, can file an HC. You must state the name of the person who is suffering or is threatened with violence or coercion and the name of the coercive authority, as well as the type of constraint (repressive HC) or the reasons for your fear of the threat (preventive HC). It is necessary to present evidence of the facts alleged at the time of the application.

Habeas Data (HD) is designed to ensure the right to access and rectify personal information held in government or public databases. It is open to foreigners, as long as they are in the country and are the owners of the personal information they wish to access or rectify. The entity's refusal to provide or correct the data must be proven before filing a lawsuit.

A Writ of Mandamus (MS) can be used to protect a right that has been harmed or threatened with harm (when the right is not protected by a HC or HD), whenever the person responsible for the illegality or abuse of power is a public authority or agent of a legal entity exercising public powers. The petitioner must indicate the authority responsible and present proof of the right.

To file the HD and the MS, it is essential to be represented by a lawyer.

EMERGENCY CONTACTS		
Institution	Tel.	Addresses
Ambulance (SAMU)	192	-
Police	190	**Delegacia de Proteção ao Turista:** Avenida Boulevard Castilhos França, S/N, Belém/PA (Complexo Estação das Docas, 2º Mezanino do Armazém 2)
Public Defender's Office of the State of Pará	129	Rua Padre Prudêncio, n° 154, Belém/PA

Part Three: Holistic Security

This section provides an overview of potential risks and key holistic security considerations for attendees travelling to Belém for COP 30. It outlines measures participants may want to consider before, during, and after the conference. The guidance addresses both physical and digital/information security, recognizing the interconnected nature of these risks—especially in a large international event held in a complex urban setting.

Managing security risks at COP 30 should not be approached as an "all or nothing" task. Instead, participants are encouraged to adopt practical, context-appropriate precautions that reflect their own risk profile and the goals they hope to achieve during the conference.

Introduction & Key Risks

1. **In the weeks and months leading up to COP30, take time to reflect on the "baseline" security risks you may face when travelling to Belém.** Understanding your baseline risk is essential as it will shape which security strategies and precautions are most relevant for you before, during, and after the conference.
2. **To assess your baseline risk in the context of COP 30, consider:**
    - What could realistically go wrong during your travel or stay in Brazil; and
    - How exposed or vulnerable you are to those risks.
3. **The most relevant security risks in the Brazilian context for COP30 participants include:**

- Theft of phones, bags, or equipment—particularly in public or crowded areas—which may result in physical harm and loss of sensitive information or tools.
- Violent petty crime, such as robbery, especially in certain urban zones or at night.
- Traffic or boat accidents and medical emergencies, especially when moving between cities or engaging in on-the-ground activities.
- Stomach infections and mosquito-borne diseases (such as dengue, yellow fever; chikungunya, or Zika) are also common in some regions of Brazil—participants should take standard precautions, including using insect repellent and drinking only safe or bottled water.
- Online or in-person harassment, particularly toward individuals from marginalized groups.
- Reputational attacks via social media, especially if your visibility or advocacy work is high-profile.
- Intimidation or hostility from non-state actors (e.g., extractive industry supporters, anti-environmental groups), especially if participating in direct actions or solidarity activities.
- Exposure to risks after the conference, particularly if your country of origin monitors international advocacy or has tense relations with environmental defenders.

4. **To better understand your exposure to these risks, ask yourself:**
    - Who might oppose my work or presence at COP 30? What resources, motivations, or networks do they have?

- Does my identity (e.g. gender, race, nationality, sexual orientation) increase my visibility or vulnerability in this context?
    i. Although racism is an unbailable crime (bail is not available once arrested for racism) in Brazil, racist incidents are unfortunately quite common—particularly during interactions with public security forces, which can become violent.
    ii. LGBTQ+ rights in Brazil have seen significant legal progress in recent years, including equal marriage rights for same-sex couples, adoption rights, gender identity recognition, and anti-discrimination protections established by the Supreme Court. However, societal challenges persist, and LGBTQ+ individuals—particularly transgender people—remain at risk of intimidation, attacks, and disproportionately high rates of violence.
    iii. Women, especially those travelling or walking alone, may face gender-based violence and harassment in public spaces, particularly at night or in poorly lit areas. While not all women experience the same level of risk, it is important to remain aware of your surroundings and take precautions when navigating unfamiliar areas, especially at late hours.
- Whether your role or activities planned at COP 30 or after make you more susceptible to these security threats in Brazil and/or in your home country.
- Am I carrying data or materials—like campaign strategies, research findings, or partner contacts—that could be misused if accessed?

- How would a security incident affect me, my work, or my allies? What level of risk is acceptable for me or others I work with?

5. **In considering the above, do not assume:**
    - That safety strategies you use at home will be sufficient or relevant in Brazil's context.
    - That law enforcement or security services will always be responsive or helpful—especially outside formal conference zones.
    - That being accredited for an official UN conference completely shields you from risk.
    - That your actions, presence, or communications are immune from observation—whether by individuals, companies, or groups with an interest in disrupting or discrediting advocacy work.
6. **Consider taking 10–30 minutes to reflect on:**
    - What matters most to protect (wellbeing, data, collaborators, access to tools).
    - Which risks concern you most (theft, intimidation, visibility).
    - Any factors that might increase your exposure (your identity, role, networks).
    - Any existing protections you already have in place (digital tools, travel plans, emergency contacts).

7. **While the checklist and recommendations in the following section are broadly applicable**, grounding yourself in your own baseline risk will help you prioritize the advice that matters most and make more informed, personal decisions about things like data protection, movement, and visibility at COP 30.

Before Travel

Once you have identified your “baseline” security risks, you should plan the security measures you want to implement before travelling. We do not anticipate widespread device inspections or seizures by Brazilian customs or border authorities. Although the use of non-consensual forensic tools should only occur with a court order, you will still have the most control over your security before you board a plane—once you arrive, your control diminishes. Therefore, it is strongly recommended that you take the time to properly prepare for your trip.

Step 1: Minimize the footprint of the devices you take with you

The lowest-risk strategy would be to travel without any devices or data. This may not be feasible for everyone, in which case you have the following options:

- Bringing wiped or “burner” devices
- Manually cleaning sensitive information from your existing devices
- Bringing your regular devices with all your data

The option you choose should balance your objectives and risk (e.g. how sensitive is the data you're carrying? What are the consequences if you lose access to it or your online accounts?) against the potential downsides, such as cost, inconvenience, or time. Regardless of the option you choose, it is essential that any devices you bring comply with the guidance provided in ‘Step 2’ of this guide.

Option 1: “Burner” Devices

If you are considering bringing a “burner” device: Reset the device to factory settings before it is used, and wipe the disk using a commercial tool (if the device was previously encrypted this will be simplest);

- Install the minimum software needed to do your work.
- Consider what information you put on the device and make available to the burner device (such as cloud accounts);
- Consider how you will record and store information you collect during COP30.

To minimize the risk of search or seizure when crossing borders, sign into accounts once you arrive and reset your device once you leave.

Option 2: Clean Devices

If the option of manually cleaning information from your devices is the only option available, consider the following:

- It will generally not be possible to remove all copies of valuable and sensitive information—as modern computers store data in many places, including hidden areas of the operating system. It will not be possible to remove all evidence of previously used online accounts, as your login history will similarly likely be stored.
- Keep only the minimum software needed to do your work.
- Files may contain metadata such as tracked changes or collaborators which are not immediately obvious to you.
- Access to logged-in accounts (such as cloud storage or social media) will grant an attacker with access to your devices access to data stored in these as well – potentially including backed-up data from other apps, even if not installed (e.g. WhatsApp)

Option 3: Bringing all information

If you are not concerned about information or accounts on your device—if you store no information which could pose harm or risk, or you do not believe there is any chance of an adversary being interested in your work, this is likely to be your most appropriate choice.

In any case, keep only the minimum software needed to do your work. Due to the targeting of cell phones by pickpockets consider uninstalling any financial or banking app and make use of debit/credit cards and some cash.

Step 2: Protect your data, communications and accounts

To protect your devices and the data you take with you, you should:

- Use only up-to-date software and devices/software that are still within the manufacturer's support lifecycle.
- Install full-disk encryption as a first line of defense (how you enable full-disk encryption on your laptop or phone depends on the make, model, and operating system version, but many modern devices enable it by default when you set up an alphanumeric password to unlock the screen.)
- Use strong passwords for both your devices and accounts, and avoid sharing accounts or devices with others.
- Keep devices fully powered off as often as possible, especially when unattended.
- Consider disabling (or knowing how to quickly disable) biometric authentication, as it may allow devices to be unlocked without a password.
- Be cautious when using paper notes, audio recorders, or e-readers/tablets, as these typically lack encryption and are easy to misplace or lose.

If data must be on your laptop, but you believe these controls are likely to be ineffective (for instance, if you are compelled to give someone access to your laptop), you may need to consider other measures, such as concealing information or files to make them difficult to find. You may also consider using Cryptomator to create encrypted concealed folders or VeraCrypt to create encrypted hidden volumes

To protect your online accounts and devices while in use:

- Use a strong password composed of multiple words with special characters and numbers. Enable multi-factor authentication using authenticator apps or security keys (preferable), or an authenticator app if security keys are not possible. Avoid SMS-based authentication, as it is easiest to bypass, and keep backup codes in a safe location to ensure you won't lose access to your account.
- Properly configure firewall software and anti-malware software—ideally modern (“EDR or NGAV”) software supported by a team or service provider who hunts for sophisticated attacks. Pay attention to warnings and alerts from your device or software that may indicate an attack is in progress.
- Pay attention to your surroundings when using your device (such as knowing that others may be looking at your screen when in public or that it could be snatched away by petty criminals).

Device theft and pickpocketing are fairly common in large cities in Brazil. Previous to any incident ensure devices have Lost Mode, backup, lock and hide, and Find my Phone features that your specific device maker offer, with either a second password or, preferably, facial recognition biometrics. This is especially recommendable to apps you hide or lock. If possible any application you won’t need, including bank apps. Ensure that all your Internet accounts and bank apps have 2FA/MFA set;

SIM Cards: Technically, SimCards in Brazil can be bought only by providing ID information and a valid ID document with photo. You might want to bring your own SIM Card with roaming capabilities to avoid disclosing this information in point of sales. Also, take note of your mobile device’s IMEI and your SIMCard’s IMSI numbers. They will be useful in case your device is lost, stolen or your SIM Card is cloned. The exact way to check these varies depending on the mobile operator and the device model.

In addition to these measures, if you believe you are likely to be targeted personally by spyware software or sophisticated surveillance, consider:

- Separating (well-known, easier to target) personal devices from dedicated work or advocacy devices whose number you do not widely circulate making it harder to target you and less likely for contagion to spread from one app or area of life to another
- Enabling the Google Advanced Protection Programme, or Apple Lockdown Mode
- Watching out for any unexpected changes in device behavior or functionality
- Being especially cautious about opening messages (or downloading/opening attachments or images) from untrusted contacts
- Knowing where to go in the event you believe you've been targeted

When it comes to protecting the confidentiality of information you transmit or send over public networks, via apps, or store online:

- Ensure you know any applications you use leverage End-To-End Encryption, and that you know how to configure and operate them. Avoid apps such as telegram which do not fully encrypt communications
- Use features such as 'view once', expiring messages, and verification of safety numbers in tools such as Signal.
- Where available, use tools which render stored material unreadable to the platform provider—such as Proton Mail / Drive, or Apple iCloud with Advanced Data Protection enabled
- Install and regularly use a VPN such as NordVPN, Proton VPN, or Mullvad—these tools are legal in Brazil.

- Be cautious about any apps which, even if you do not use them, may be sending data in the background (or will be visible if your phone is viewed by law enforcement) or may disclose aspects of your life or activity: e.g. apps specific to activist communities or aspects of your identity you may not wish to be public, data collection tools, or digital security tools, if not in use.
- Research the limitations of end-to-end encryption when using communication platforms like Signal, Zoom, WhatsApp or iMessage—including how they store metadata or perform backups, which may undermine your safety

Step 3: Ensure Your Personal Documentation is in Order

Make sure your passport is valid for at least 6 months from the moment of arrival, and that you have at least two blank / unused pages left for the entry and exit stamp.

Ensure you have been issued with or applied for any appropriate accreditation badges or similar documents proving your participation in COP 30, which might be needed for your visa application / entry to Brazil or access to restricted zones at the conference venue.

Ensure you have proof of return flight tickets, accommodation, and sufficient funds for length of stay as this might be requested during the visa process and at the border as proof that you are not planning on prolonging your stay in Brazil. Bring all relevant documents in your carry-on bag and have backup photocopies or digital scans in a secure folder.

Brazil follows a principle of reciprocity for visas—if your country requires a visa from Brazilians, you'll likely need one to enter Brazil (e.g.: American and Canadian citizens would need to process a visa). Check official requirements in advance and secure the appropriate visa before travel.

Yellow fever vaccination is not mandatory for entry into Brazil but is strongly recommended for those visiting inland areas or the Amazon.

Get vaccinated at least 10 days before travel and carry your International Certificate.

Step 4: Consider Purchasing Travel Insurance

Purchase travel and personal accident insurance that at a minimum provides coverage for emergency medical treatment (ideally up to a limited amount), medical repatriation, evacuation, any longer term medical expenses incurred upon return to your home country (resulting from an accident that occurred during your trip), lost baggage and flight cancellation or delays.

Make sure you understand and have acknowledged any exclusions that would invalidate your travel and personal accident insurance policy (e.g. geographical exclusions, prohibited activities). Always keep a copy of the insurance policy with you and have the emergency number saved in your devices and written down somewhere safe.

Try to arrange access to funds to cover any emergencies, uninsured situations, or where cash deposits for medical treatment may be required.

Step 5: Safe Packing, Clothing, and Finance

When traveling to Brazil for COP 30, ensure you do not carry any items that are illegal under Brazilian law. This includes certain medications—especially those containing controlled substances—which should be accompanied by a doctor's prescription and clearly labeled.

In terms of clothing, Brazil is generally relaxed and diverse in dress. However, be mindful of the heat and humidity—lightweight, breathable fabrics are essential. Also consider packing long sleeves and pants for protection against mosquito bites, especially in areas where dengue or other mosquito-borne illnesses are a concern.

Avoid packing valuables (especially electronics) in checked luggage due to the risk of airport-related theft in Brazil. Tampering with

checked bags—even when locked—is relatively common, with frequent reports of incidents, particularly at São Paulo Guarulhos airport (GRU). Carry valuable items in your hand luggage.

Brazil's currency is the Brazilian Real (BRL). While digital payments and cards are widely accepted in urban areas, cash may be needed for taxis, markets, and smaller vendors—especially in more remote or informal settings. In case of a financial emergency, services like Western Union or Wise can be used to receive funds safely.

For added financial security, consider disabling the contactless feature on your debit or credit cards during your stay. While convenient, this feature can make you more vulnerable to theft or unauthorized transactions, particularly in crowded areas.

Step 6: Establish Your Support Network

A support network is a list of allies that you can contact where immediate support is required in the event of an incident or emergency, or who can take action on your behalf when you are unable to (such as if you become incapacitated due to medical incident or being detained).

It is advisable to form small groups in which members look out for one another throughout the action. It is recommended that they move together, plan meeting and regrouping points, and remain in constant communication. It is also wise to have someone monitoring externally who can be contacted in case of an emergency (such as a lawyer, the press, family members, or a support network).

Consider a network with three types of contact:

- **Trusted individuals outside of Brazil:** This could be colleagues, friends, or family that are not physically present in Brazil, and who would be aware of your schedule and movements. Having a trusted contact outside the country that you check-in with once daily is recommended as they will be better positioned to respond to an incident, take action to mitigate consequences, or

activate external support, if this cannot be done from Brazil. Ensure the external contact has access to your itinerary, hotel contacts, contacts of other people in your delegation and other relevant colleagues attending the event who they could contact to try to locate you. Make sure that any check-in arrangements with contacts outside Brazil are clearly understood by both parties, and that your contact knows what to do if check-in is missed and repeated attempts to establish communication with you have failed. Such actions may increase with urgency the longer that communication cannot be made.

- **Trusted individuals amongst COP 30 attendees:** This could be colleagues, friends, or fellow delegates who are attending COP 30, who you will maintain regular communication with throughout the conference, including before and after activities outside of COP 30 (such as sightseeing, going to a restaurant). If you are part of a delegation, you may choose to communicate collectively (as part of a Signal or WhatsApp group), or to pair up individually with a “buddy”. These communications can be used to confirm safe movements and account for delegates or “buddies”, as well as to alert them to specific security threats or incidents.
- **External support providers:** It is important to know any external providers you can contact in the event of an emergency (and have their contact details programmed into your devices and in a physical copy). This may include, but is not limited to: Travel and personal accident insurance providers; Legal assistance or representation; Well-being support and accompaniment; Local medical facilities; Security risk advisory and support.

Before arrival check whether your country's embassy or consular services are available in Brazil and save contact and address details to seek help in case of necessary.

If you are planning to take part in protests or demonstrations, inform your security network of your route, arrival and departure times, and the purpose of the action. Always stay close to familiar routes and escape paths. Agree on a cut-off time—if you haven't checked in by then, your network should begin trying to locate you. Consider leaving your device's GPS on to send your location to a contact and in case of emergency. When you leave the demonstration, turn off the GPS as soon as you get to a safe place. Avoid sharing photos of yourself at protests or even geotagging your photos. Never publish photos that make it possible to identify other participants in a protest.

Upon Arrival

Digital and Information Security

As mentioned previously, we don't anticipate widespread device inspections by Brazil's customs and border authorities. Still, you should consider switching off all devices before leaving the plane and when transiting security checkpoints. If you are traveling with a burner device, avoid signing into any accounts until you reach your destination. Once there, turn your devices back on and check that your chosen apps and services are functioning as expected. Download only the data and files you need from the cloud—and only when you need them.

Internet penetration is high in Brazil, but geographic coverage is uneven. The gaps in coverage are larger in Center-west and North regions, and Internet connectivity in most of the Amazon Basil is limited. Sites like NPerf can give a general idea on coverage and speed in different places with limited precision, the less populated a region, the less accurate data will be. Mind that electricity can also be scarce in these regions, so make sure to bring your own power banks.

Border Control

While border control is generally expected to be light for those mentioning their attendance at COP 30, it is advisable to be prepared for possible questioning. Officials may ask about your travel route, previously visited countries and the reasons for those visits, length of stay, accommodation in Brazil, your job and activities in your home country, financial means, and occasionally even personal matters. Having a reliable translator app, with offline capabilities, and physical phrasebook, is advised.

Be ready to respond clearly and confidently without drawing unnecessary attention if you are asked personal questions. Keep in mind that, even if you have obtained a visa, entry into Brazil is ultimately at the discretion of the immigration officer.

Have relevant documents readily available (passport and visa, invitation letter, proof of funds and accommodation, return flight tickets, and travel insurance). Remain calm, answer only what is asked, and provide only what is requested.

General Safety

Be cautious of illegal taxis or fake ride-hailing apps. It is common for unlicensed drivers at the airport to hold signs saying “uber” or “taxi”—do not use these services. Use only authorized taxi services or verified rides through apps like Uber, 99, or inDrive. Within Belém, there are several official taxi stands located throughout the city.

In case of theft, robbery, or pickpocketing, prioritize your physical safety—move to a calmer and safer location. Then notify the contacts you were planning to meet.

In case of device theft, assuming you followed the preparation steps in the “Before Travel” section, you should be able to lock your devices remotely as soon as possible. The likelihood of perpetrators accessing your data will then be relatively low (though not zero). Notify your cellular provider immediately to report the phone and SIM card as

stolen, and request temporary blocking,which you may want to make permanent if the device is not recovered. Change your passwords and ensure 2FA/MFA is activated for accounts linked to the device (e.g., iCloud, Google). If you don't recover your phone within 48 hours, remotely wipe or reset it.

Consider filing a police report (either online or in-person) to document the incident and the status of the device in case it is used for any illegal activities.Each Brazilian state has its own police department and reports must be filed with the department where the incident happened. E.g. for Pará state, at https://delegaciavirtual.pa.gov.br/

If you do recover your device, follow the recommendations in the "What to do if..." section.

During the Conference

Digital and Information Security

Keep all devices powered off, locked, and in a secure location whenever possible, especially when charging or not in use. Avoid using chargers that are not your own, USB outlets in public spaces, or plugging in any external peripherals or storage devices, as they can be tampered with. Consider acquiring and using a power bank for your exclusive use

Unattended Devices: Do not leave your devices unattended, as they can be stolen or tampered with. For example, an increasing trend is police and judicial authorities abusing digital forensic tools to unlock and extract data from mobile devices that were either left unattended, or surrendered under false pretenses such as "protecting officer privacy and confidentiality" during interviews, traffic stops and other situations. There are also reported cases of devices – as well charger and cables – being tampered or switched to malicious doubles when left unattended in hotel rooms during conferences and other events.

If you need to surrender your device, or leave it unattended, turn it off and check for signs of compromise upon return (battery level, energy consumption, file access, new application, storage size, markings and ents).

If you suspect your device may have been compromised or tampered with, do not use it. Contact a trusted digital safety provider (e.g., Access Now Digital Security Helpline) to assess the situation. You may also consider discreetly marking your chargers and cables to detect if they have been switched.

Keep all wireless features disabled if not required as they can be used to passively track you and link you with those around you. Do not connect to public WiFi unless emergency communication is required or you are confident in your use of end-to-end encryption.

When using social media or traditional media, be aware that you are publicly broadcasting information. Consider how your messages, locations, and associations may be interpreted or used by others.

Avoid installing any domestic apps for the conference, taxi services, etc (unless on a device you can intentionally ‘not trust’).

If you are holding sensitive conversations or gathering with other attendees where your meeting or association may be intrinsically sensitive:

- Be mindful that public space is likely to be subject to CCTV which tracks movement and can identify individuals leveraging biometrics. Both national and local level authorities have deployed “Control / Operational Rooms” and integrated data systems with extensive surveillance capabilities.
- Be aware that Wi-Fi and mobile networks can be used to ‘triangulate’ or track where you are based on your phone or other devices interacting with them—only by fully powering down devices (or disabling all wireless features) will this not be

possible, as even the information the device discloses when scanning for a network can be used for surveillance

Even if your conversations or messages are not intercepted, these tools (CCTV or location tracking) may be easily used to identify gatherings or association of groups. CCTV use is widespread and "normalized, with camera surveillance and entry control used by both public and private parties, with an increase in the use of cameras and systems capable of some level of facial recognition.

Instant Messaging: Keep in mind that WhatsApp usage in Brazil is extensive and much more embedded in daily life than in most countries, to the point of many businesses and public services being available only via WhatsApp. Telegram also has a large base of users in Brazil, although to a lower degree, with its group/channel features being relatively popular, including illegal and criminal activity, and political extremists, as well as its use for scams and phishing attempts and it should be avoided completely.

Because of WhatsApp's prevalence, maintaining operational security while using it—especially when handling sensitive data or communication with local stakeholders—can be difficult. Be extra cautious in identifying phishing and SCAM messages, and avoid clicking on hyperlinks on messages in the platform.

Internet Shutdowns and censorship: On the one hand, widespread Internet traffic interception and shutdowns by State forces is unheard of, although the technical means are available.

Political surveillance: since the end of the last dictatorship in the country, political surveillance has dwindled considerably. That said, the surveillance mentality is still embedded within the Brazilian State, which has the capacity and resources for conducting it, with a few cases of misuse and abuse of these resources in the last 10 years or so by State agents or groups at national, state and local level against grassroots social movements, civil society organisations, and political adversaries. At the national level, unofficial and illegal surveillance of

internal actors grew during the previous administration. The use of this apparatus against civil society organizations and activists seems to have eased, but not disappeared in the current administration, but the capacity is still there and rogue actors within the state could use these resources.

Traditionally, the most common methods for this surveillance on digital environments occur via infiltration and surveillance on social media and other online platforms, but the use of ISMI catchers, tools for automated gathering of OSINT signals, cellphone network data and systems for integrating and amassing large volumes of data has grown in the last few years. As such, caution should be exercised when publishing posts, comments and divulging any real time information that might disclose your location and plans.

Disinformation and online harassment related to environment and climate crisis related topics are common. As well the narratives about NGOs being used as foreign agents, globalism and any display of left-wing, liberal or progressive positions.

Because online harassment can easily escalate into physical harassment or even harm, and lawfare tactics have been used as retaliation against activists and journalists, we recommend caution when publishing something in social media and always back your claims with hard, verifiable facts to avoid attacks by the way of anti-defamation laws.

Police can seize devices during protests and other cases where there is “reasonable or probable cause”, which is thinly overseen, but not compel anyone to disclose passwords.

Use of forensics tools for accessing digital devices of activists are unheard of, but use of such tools by law enforcement in investigations have become common, including the use of Cellebrite’s forensic tools. Use of non-consensual forensic tools should occur only with a court order, but these have become increasingly common.

To mitigate these risks, you should make similar risk assessments from section “ii. Before Travel” and follow the same recommendations shared on the section “Step 2: Protect your data, communications and accounts”, with emphasis on data minimisation, keeping software and devices updated, using a strong password/passphrase and Multi-factor authentication.

Personal Safety & Security

The security and political situation in Brazil is generally stable in major cities, including Belém, where COP 30 will take place. However, urban crime remains a concern, particularly theft, robbery, and scams targeting foreigners. Violent crime against foreigners is not common in central areas but can occur, especially in less secure neighborhoods. Stay informed through local news and any security alerts issued by your embassy or the United Nations security team.

Be particularly cautious in nightclubs, bars, or poorly lit areas, especially when unfamiliar with your surroundings. Avoid using unofficial taxis or accepting rides from strangers—use trusted apps like 99, Uber, or inDriver.

Be cautious when interacting with strangers in bars or public places. Incidents of drink spiking followed by robbery or assault have been reported, particularly in nightlife settings. Avoid accepting unsolicited invitations or drinks from people you’ve just met, and never leave your drink unattended.

Avoid moving around alone, especially at night and outside designated COP zones or in less busy areas. There is greater safety in numbers, especially when accompanied by other trusted COP 30 participants.

In Brazil, you are legally required to carry identification at all times, but it does not need to be your original passport. It is advisable to carry a copy of your passport photo and visa/ entry stamp pages and leave the original in a secure location.

Carry another valid photo ID (like a national driver's license) and your official COP30 badge/accreditation, and check in with a trusted colleague, delegate, or buddy when arriving at or leaving events.

While Brazil is a diverse and relatively open society, it is currently experiencing a highly politically polarized moment, which can heighten tensions in conversations. Avoid speech or behavior that could be perceived as offensive or inflammatory—especially when discussing politics, religion, or other sensitive topics, particularly in unfamiliar settings or rural areas.

Keep valuables secure: use zipped bags worn in front or interior pockets for phones and wallets. Avoid displaying high-value items (e.g. expensive phones, jewelry, or electronics) in public, including earphones / airpods. In hotels, store anything non-essential in the room safe or deposit box when available.

Practice situational awareness at all times. Stay alert to your surroundings, follow local news updates, and identify emergency exits and meeting points in hotels, venues, and restaurants. Trust your instincts—if something feels off, move to a safer area or notify someone in your delegation.

Attending public gatherings or protests outside the COP 30 Blue Zone can pose increased risks, including exposure to opportunistic theft.

While it is not forbidden to take photos or videos in public spaces in Brazil, you should avoid photographing or filming police, military personnel, or their activities, including during patrols, operations, or at protest sites. Although not illegal, such actions can trigger tense or even aggressive responses, including being approached, questioned, or asked to delete the footage. To minimize risk, be discreet with photography in sensitive settings and avoid drawing attention to yourself with visible filming equipment or gestures.

Accommodation Security

Choose reputable and secure hotels: consider proximity to the venue, ratings and reviews, and security measures—like a 24-hour reception desk, access card to the room, and a safe deposit box

Keep your hotel room number confidential, and keep the access card hidden and with you at all times. Secure your room every time you leave by checking doors and windows. Consider using a 'Do Not Disturb' sign to deter access to your room when both occupied and unoccupied.

Transportation / Road Travel

Only use transportation recommended or arranged by your delegation, your hotel or the event organizers. Taxi services like Uber are affordable and recommended. Avoid unofficial or unmarked taxis, and do not accept invitations from taxi drivers.

If using private transportation services, confirm with a trusted local source—such as your hotel reception or a local contact—that the company is reliable. When using ride-hailing apps like Uber, 99, or inDriver, always check the driver's ratings and reviews, and verify the license plate and driver photo before entering the vehicle. These platforms are widely used in Brazil, but as with any app, be aware that they may collect and store location and usage data. If you're relying on your phone to maintain a high level of confidentiality, consider using these apps cautiously or through a secondary device.

Uber moto is a popular and low-cost option in Belém, it is not advisable due to the increased risk of road accidents and limited protection for passengers. Stick to cars or official taxis for safer travel.

Road travel in Brazil, especially in and around the Amazon, carries significant risks due to armed robberies, vehicle hijackings, and poor road conditions, including unpaved or degraded routes. River transport also poses hazards: voadeiras (small motorboats) are commonly used but often unsafe due to overcrowding, lack of safety equipment, and

exposure to severe weather. Travel with caution and assess routes and providers in advance.

Upon Returning

Information Security

If you are using “burner” devices or wiping devices, then you should perform the reset at the end of the conference and before leaving for the airport. If you are manually cleaning devices, then you should give yourself sufficient time to do this before leaving for the airport.

In all cases, you should go through security / border control with your devices powered off and any biometric access disabled.

Exporting Goods

Exporting cultural artifacts or wildlife products from Brazil is strictly prohibited without official authorization. This includes antiques, religious objects, fossils, and any items made from protected plants or animals.

Re-assessing “baseline” security risks at home

Reassess your “baseline” security risk at home and how your participation in the conference might have raised your profile and/or exposure to certain security threats. Pay particular attention to situations that may occur at home that would indicate you are at heightened risk (unsolicited calls, direct threats, physical or digital surveillance).

Where you believe your risk profile has been heightened, consider temporarily limiting public activities, including demonstrations and legal cases that may aggravate the lawsuit. Reinforce security measures, particularly at your home and for children going to school

If you believe a credible threat from a capable actor exists, do not disregard the potential for escalation. Consider temporary relocation or evacuation.

What To Do If...

Your devices are confiscated and subsequently returned to you:

- Check for physical tampering with the case
- Do not turn on or use the device
- Notify your colleagues, partners, and peers by alternative means
- Try to secure a new device if possible
- Your devices are stolen or lost and subsequently returned to you:
- Reset all passwords for online services
- Notify anyone who could be affected by the data on the device or accessible from the device
- Do not assume adversaries will not be able to access encrypted data on your devices because they may have your password, for example, from CCTV footage of you entering it or through physical surveillance

Your planned measures for protecting the confidentiality of digital information at rest, in use, and in motion are not working:

- Do not select insecure alternatives without first considering the risk and likelihood that this is exactly what an adversary wants you to do
- Determine from others if this is just affecting you or also everyone using the app or service; in this situation, people can mistakenly interpret it as a targeted attack
- Reach out to your support network to identify alternatives
- Give serious consideration to the option of performing the activity upon your return if it can wait

You think someone else may have attempted to access your social media, technology platforms, or digital tools:

- Make sure this access attempt was not, in fact, yours;
- Review your previous activity in relation to other services, as they also may have had an attempt at access but not notified you
- Change your password(s) for affected services only if you are certain that your communications with the service are secure.

You suffer attacks to your reputation like smear campaigns:

- Do not respond to the posts / defamatory content directly—you might be giving more visibility to the perpetrator
- If relevant, consider engaging in a positive campaign in collaboration with allies reinforcing your reputation and good work but without addressing the attack
- Document the attacks and gather evidence—they might be useful in the future either for legal purposes or to ask the platforms and social media used to remove content
- Monitor the situation to identify an escalation or further attacks
- Seek well-being support if relevant
- Seek support from official media and journalists

If you suffer any attacks or reprisals (or are at immediate risk of attack or reprisal) upon return to your home country, you may be eligible for fully-funded holistic security support through Open Briefing. You can make a referral for holistic security support to Open Briefing by completing the referral at the bottom of this web page.

If eligible, you will receive contact from an assigned consultant within 72 hours of your referral being made, who will discuss your situation with you (e.g. risks, support needs etc) and possible support options.

Further information can be found here.

Part Four: Cultural Sensitivity

Political and Territorial Context

Pará is a socio-environmental frontier state, marked by land conflicts, violence against peasants, the advance of the mining industry, the expansion of agribusiness, and the presence of illegal activities, such as illegal mining. At the same time, Pará is a territory of resistance for indigenous peoples, quilombolas, river dwellers (known as ribeirinhos, in Portuguese) and peripheral urban communities, who have been articulating essential struggles for climate justice and the realization of human rights.

Political Context

The government of Pará has sought to present itself as a leader of the "green economy" and host of COP30. However, it has been criticized for maintaining close relations with large mining companies and agribusiness sectors. At the municipal level, since the beginning of 2025, Belém has been under the mandate of a new mayor. The change from a left-wing to a center government raises uncertainties about the continuity of participatory policies previously implemented.

The current legislative composition, both at municipal and state levels, is marked by a conservative majority, with parliamentarians who often act in defense of interests linked to the predatory exploitation of the Amazon, such as extensive agribusiness, mining and large infrastructure projects. However, despite the unfavourable correlation of forces, counter-majoritarian parliamentarians play a strategic role in building fairer and more sustainable alternatives for the region by promoting debates, denouncing setbacks, and articulating resistance both inside and outside parliament.

Economy

Pará's economy is mainly structured on extractive and large-scale activities, such as: iron, bauxite and copper mining; agribusiness focused on soybeans and livestock; as well as logging and industrial fishing. Although these activities generate billions in revenue, most of the wealth generated is exported as commodities, benefiting large companies and leaving the state with little return. The result is a model that concentrates profits outside the region and imposes serious social and environmental liabilities on local populations. Added to this, is the advance of illegal economic activities, such as clandestine mining, which threatens indigenous lands, conservation units and traditional communities, further aggravating conflicts and environmental destruction.

Population and Culture

Pará has a profound ethnic-racial diversity. The state is home to more than 60 indigenous peoples, quilombolas, riverside dwellers (ribeirinhos), extractivist populations, peripheral urban communities, as well as a large Afro-descendant population. In Belém, there is a population marked by internal migration, especially from the countryside and from Amazonian regions. These are people who resist exclusion and transform the city into a living space of culture, struggle and creativity.

This diversity is expressed through Para's social customs, which are deeply marked by the affective relationship with food, music and faith. The cuisine constitutes typical plates from local ingredients (ie. cassava and açai) prepared in different ways, such as tacacá and maniçoba. Eating is a collective and symbolic act, it is common to share a very thick açaí with fried fish or have coffee with tapioca at the market with friends and acquaintances. Besides the cuisine, there are also a variety of cultural manifestations. Carimbó, a Cultural Heritage of Brazil, packs music, dance and get-togethers in squares and communities; while techno brega, a musical and aesthetic production

from the peripheries, drives a powerful and authentic creative economy. Popular religiosity, especially the catholic procession of Círio de Nazaré, mobilizes thousands in a great manifestation of faith. Respecting these customs is fundamental to understanding and experiencing Pará's culture with sensitivity and empathy.

Security Forces and Public Demonstrations in Pará

Police actions in Pará are marked by a history of violent repression, especially in the southern and southeastern regions of the state, where conflicts over land are intense. Emblematic cases, such as the Eldorado do Carajás massacre in 1996, when 19 landless rural workers were murdered by the military police, show the brutal face of public security in the countryside. In the urban peripheries, the militarized logic persists, with high police lethality and systematic criminalization of social movements, marginalized populations, popular leaders and human rights defenders. The structure of public security favors confrontation over dialogue. Social demonstrations, especially those denouncing large enterprises or criticizing the actions of the state, are often met with hostility by the security forces.

Despite constant repression, popular resistance in Pará is still alive. Social movements continue to occupy the streets and public spaces with courage, articulation and hope. Their presence is fundamental to guaranteeing the visibility of the struggles for socio-environmental justice, human rights and the protection of territories. Amidst the context of inequality and authoritarianism, collective organization continues to be a powerful tool for confrontation and transformation.

COP30 in Belém

The COP30 in Belém represents a historic opportunity to put the Amazon at the center of the global climate debate, not as a territory to be saved from the outside, but as a place where people live with knowledge, practices and powerful proposals for another model of life.

It is an exciting moment to witness forests, peoples, and social movements articulating an active, critical and propositional presence.

Points of attention for Defenders/Activists at COP30:

In terms of structural public participation issues, a major problem has been the criteria for access to COP30. For instance, to register for a credential, one needs to have a passport. This excludes most people from traditional communities, the majority of whom don't have this document due to its reasonably high cost, and are often disenfranchised, without access to basic rights and public policies. This is an institutional barrier that hinders the central participation of those who live in the real Amazon.

Belém faces serious social inequalities, with a lack of basic sanitation, extreme poverty, limited accessibility and urban violence. For personal safety, pay attention to your surroundings and security forces, especially at public events. Avoid walking alone, be careful of predatory pricing of goods, especially if you don't know the native language or have basic knowledge of the local currency. Establish direct communication channels with local organizations, with phone numbers and addresses saved beyond your cell phone. Get to know the urban territory and its challenges. It is essential to network with local movements and leaderships, prioritize listening to host communities and denounce any attempt of greenwashing or co-opting popular narratives.

Active cultural and political spaces at COP30

Defenders will be mobilized, networking, defending the forest, territories and human rights. Various initiatives are being organized to guarantee spaces for effective listening. These include the People's COP (COP do Povo, in portuguese), the Peoples' Summit (Cupula dos Povos, in portuguese) and the COP das Baixadas, which are ways of ensuring that the voices of those who live in peripheral areas and traditional communities have a leading role. These parallel spaces are

strategic for confronting the exclusionary and elitist logic of the official COP.

In addition to the official COP space, the following will be active: The People's COP House, which is organizing artistic and cultural interventions, with local artists, and immersions. In addition, the Federal University of Para (UFPA), social movements such as the MST, CPT, MAM, MAB, urban collectives, such as Ponto de Cultura IACITATA, peripheral and indigenous youth networks, will all have their agendas. Cultural and political activities will also take place in spaces such as Casa Preta Amazônia, the Arraial Institute, the Curro Velho Foundation Cultural Centre, as well as public squares, which will be the stage for mobilizations and symbolic acts.

What Not To Do in Belém To Avoid Being Disrespectful

During COP30 and in any visit to the Amazon territories, it is essential to adopt a posture of respect, listening and humility towards traditional peoples and communities. This means recognizing their leaders, valuing their ways of life, rituals and their own forms of organization. External presence in communities must always be mediated by consent, avoiding invasive attitudes such as taking photographs without authorization, not treating the peoples as "attractions" or using colonizing and salvationist language. These peoples are not objects, nor do they need to be treated as exotic or eccentric; they are political subjects, holders of ancient knowledge and protagonists in the defense of the forest and the climate. Respecting them is an essential ethical commitment if COP30 is not to reproduce inequalities, but strengthen fair and decolonized alliances.

Moreover, avoid attitudes that show superiority or that treat locals as mere objects of study. Respect the local accent, cuisine and traditions, without belittling them. Furthermore, never refer to the forest or the Amazon as an unoccupied or lifeless place, as they are territories full of history, culture and political significance for those who live there.

Valuing and recognizing this wealth is essential for respectful interaction.

Global Climate Legal Defense (CliDef) believes that no one should be sued or jailed for speaking out. We embolden climate defenders to challenge the corporate and governmental drivers of climate change, knowing that lawyers will have their backs. CliDef operates on a hybrid model, offering legal advice and strategy, coordination, and funds for legal defense. We build and strengthen a network of diverse lawyers and legal organizations to serve the global climate movement.

Learn More

The Arayara International Institute is a non-profit civil society organization formed by scientists, engineers, urban planners, and environmentalists dedicated to promoting quality of life for Brazilians, justice, and sustainability in resource management. For over 30 years, Arayara has developed innovative activism for a just energy transition, influencing public policy, legislation, litigation, knowledge production, communication, advocacy and campaigns to pave the way for energy transition in Brazil and reducing greenhouse gas emissions. With its own technology, it operates in all Brazilian states and Latin American countries, producing technical analyses, defending rights, strategic litigation in diverse environments. Its work has prevented more than 3.3 gigatons of CO2, about 744,700 premature deaths, and about US$1.37 trillion in potential damages.

Learn More