

# COP 28 Guide

# Guide to United Arab Emirates Law and Holistic Security at COP

## Keeping Safe for Activists Attending COP 28

This Guide is designed for climate advocates and activists attending COP 28 in the United Arab Emirates (UAE), and provides basic information about the legal framework and available resources to navigate the local legal landscape in the UAE; and an overview of information/digital security issues, with suggestions for how to protect your information and remain safe before, during, and after COP.

We hope that this guide will enable activists, advocates, and others attending COP 28 to make informed decisions about their actions while in the UAE.



[www.climatelegaldefense.org/COP28](http://www.climatelegaldefense.org/COP28)

# COP 28 Attendee Checklist

**Before leaving for the UAE**, please reference this six-point checklist in order to make informed decisions and keep safe during your stay in Dubai.

- Make and prepare to implement a plan for communicating safely while you are in the UAE (which may include downloading Signal if you don't already have it).
- Establish a personal safety network to enable others to find you and to track fellow activists. Verify the safety numbers on Signal of the members of your personal safety network before going to the UAE.
- Secure a companion or "buddy" to travel with, ideally at all times, within the UAE, but especially to, from, and outside the conference Blue Zone. This buddy can help you to avoid problems and also help to address them should they arise. Verify the safety number on Signal of your buddy before going to the UAE.
- Develop and carry with you a list of critical resources:
  - Contact information for your country's embassy/consular services in the UAE
  - Phone numbers of your safety network contacts
  - Legal Protection Hotline number: +41 767 635 765  
**(Hotline open for Signal & WhatsApp texts November 28-December 14)**
  - Legal Protection Hotline email: [cop@climatelegaldefense.org](mailto:cop@climatelegaldefense.org)  
**(Email open November 28 - December 14)**
  - Safety Hub email: [safetyhub@proton.me](mailto:safetyhub@proton.me)  
**(Fully operational November 23-December 19)**
- Review your published statements online or on social media; those that are critical of the UAE as well as other States may violate UAE laws restricting speech.
- Review digital security measures and settings on [Page 11](#).

---

To learn more about CliDef's COP 28 legal protection center, please visit:

[www.climatelegaldefense.org/COP28](http://www.climatelegaldefense.org/COP28)

CliDef's Legal Protection Hotline will be available between November 28 and December 14 by toll-free Signal or WhatsApp text (phone calls may be blocked) at +41 767 635 765, and by email at [cop@climatelegaldefense.org](mailto:cop@climatelegaldefense.org).

The Safety Hub Hotline will be available a week before and a week after COP 28 (November 23 - December 19) at +49 177 684 4896, and by email at [safetyhub@proton.me](mailto:safetyhub@proton.me).

# What's in this Guide

## PART ONE: Know the Law

### I. A Brief Overview of Important UAE Laws and Related Considerations

1. Stops, personal searches, and arrests
2. Freedom of expression
3. Media freedom
4. Pre-Trial detention
5. Public protest
6. National security
7. Freedom of movement
8. Right to a lawyer and to consular protection
9. Fundraising and related activities

### II. How to Comply with the Law and Stay Safe

### III. Frequently Asked Questions

1. Entry and exit issues from the UAE
2. Issues related to protests, gatherings, and public demonstrations
3. Your rights in case of search and arrest
4. Your rights in relation to LGBTQ cases

## PART TWO: Information and Digital Security

### I. Understanding your “baseline” security risks

### II. Before Travel

Step 1: Set Your Information Security Foundation

Step 2: Take Information Security Measures with Respect to Your Data

Step 3: Ensure Your Personal Documentation is in Order

Step 4: Take Information Security Measures with Respect to Your Data

Step 5: Safe Packing & Clothing

Step 6: Establish Your Support Network

Step 7: Prepare Yourself to Face Identity-Based Questions and Address Cultural Sensitivities

### III. Upon Travel

# Know The Law

UAE law relating to the kinds of issues COP attendees might be concerned about—searches, arrests and detentions, freedom of expression, personal identity and security—is complicated by the fact that some of the laws are published, and others are not. Additionally, some of the most relevant laws, including the State Security Law (which deals with crimes and terrorism) and the Criminal Code, contain language that is often interpreted broadly by authorities.

It is important to know that **UAE law is in full effect across the country, except in the Blue Zone, which is regulated by the UN.** In other words, the Green Zone (“the central hub for action...open to the public, private sectors, media, youth, NGOs, as well as delegates and guests of the UNFCCC-managed Blue Zone”) is governed by UAE law. Therefore, **any activities participants undertake outside the Blue Zone, including in the Green Zone, are subject to the restrictions and considerations described in this Guide.**

While legal advice will be available to COP activists and advocates through the Legal Protection Hotline, local legal support on the ground for activists is extremely limited. Because visitors to the UAE are subject to its laws, this Guide seeks to explain the legal context, which we hope will enable COP participants to make informed choices about the actions they take and how they will engage during their time in the UAE.

## I. A Brief Overview of Important UAE Laws and Related Considerations:

### 1. Stops, Personal Searches, and Arrests

Under normal circumstances, a typical police

officer in the Emirates is strictly prohibited from searching or arresting an individual without prior judicial permission. However, members of the State Security Apparatus (SSA) have unique powers that regular police officers do not have under the State Security Service Law. This law allows SSA officers to stop and search individuals and their homes and detain them for extended periods of time.

In particular, SSA officials (including the head of the SSA) have the authority to:

- Search and detain individuals without permission from a court to do so.
- Authorize the detention of a suspect beyond a few days; if the head of the SSA is involved, he may order detention for up to 3 months before getting an order from court.
- Order the deportation of a foreign suspect.
- Investigate cases related to any activity of a person, organization, party, or association that seeks to harm the safety and security of the UAE State; this is a broad mandate and is interpreted broadly by the SSA.

### What does this mean for COP participants?

- **Before you go:** Read the State Security Services Law, available at <https://en.edacrights.com/post/108>, before you leave home, so you know your rights if you are stopped.
- **Before you go:** Protect the data on your devices as much as possible by taking measures for data at rest and data in use in [Part II, Step 2](#) of this Guide.
- **While you are at COP (or in the UAE, including at the airport):**
  - ▶ **If you are stopped,** try to figure out if it is

a regular police officer or a member of the SSA who has stopped you.

- Regular police officers tend to wear gray, green, or khaki uniforms.
- SSA officers wear all-black uniforms and black masks covering their faces, but they may also wear civilian clothes.

- ▶ **If you are not sure who has stopped you, or if you are stopped by someone in civilian clothes**, respectfully ask for verification of his identity. This is a common practice, and it can help you confirm whether the person approaching you is indeed a legitimate law enforcement officer.
- ▶ Know that you can always ask for an interpreter.
- ▶ **If you are stopped by a regular police officer**, you can respectfully assert your right not to be searched or arrested without an order from a court. However, consider whether it is possible to easily comply with the search, as the consequences of refusal may escalate the encounter. If you are detained, you should immediately call your embassy or consular services if you can, and also text the Legal Protection Hotline and your safety network to let them know what has happened.
- ▶ **If you are stopped or detained by a member of the SSA**, you should immediately call your embassy or consular services to seek help if you can, and also text the Legal Protection Hotline and your safety network to let them know what has happened. By promptly notifying others of your situation, you create a record of what has happened, which allows for legal intervention (if necessary).

## 2. Freedom of Expression and Information

UAE laws contain broad restrictions on freedom of expression, and make it a crime for anyone to:

- Criticize the UAE government, its institutions, or leaders;
- Criticize other States;
- Publish “false news” that disturbs public security or incites public opinion;
- Publish any of the above online (in which case it becomes a cybercrime)

The UAE also has a national firewall in place to block banned websites, limiting access to information contained on these websites. Using a VPN to access these sites is illegal and does not always create a continuously secure connection.

### What does this mean for COP participants?

- **Before you go:** Think about whether you have published statements online or on social media that are critical of the UAE as well as other States, as those may violate UAE restrictions on speech and/or may constitute a cybercrime if those statements are linked to you after you enter the UAE.
- **While you are there:**
  - ▶ Before using a VPN to circumvent the local censorship, ask yourself if accessing the content immediately is worth the risk. Evidence of accessed content may remain on your device and be available to authorities if they gain access to the device. Not using a VPN may expose communicated data, but the firewall should prevent you from accessing unlawful content.
  - ▶ Using a VPN does not guarantee a continuously safe connection. If you ignore security warnings when connecting, you may not establish a safe connection to your VPN provider in the first place. Your connection to a VPN provider may drop due

to errors or interference and your device may ignore this and continue to send and receive data without the VPN. Finally, you may not have configured the VPN to ensure all traffic is sent over the connection leaving some very sensitive data exposed, such as a list of all sites you access.

- ▶ If you use a VPN as an end-around to access banned web content (and you will know if it is banned by trying to access it without the VPN, and hitting a firewall), you may be criminally prosecuted for breaking UAE law.
- ▶ Think about how you will be able to communicate privately during COP. It is recommended to use Signal text, with WhatsApp as the second-best option. (Make sure to verify the safety number of your contacts on Signal before you go to COP.) Video and voice calls on Signal may be blocked. Normal voice calls and SMS texts will be intercepted as a matter of course and retained for months or years. Telegram is not recommended as it is based in the UAE and is likely surveilled.
- ▶ Consider that if you make comments that violate the restrictions described above, either orally and in public where you are overheard by UAE officials, or online/through social media, you could be arrested, detained, and prosecuted.

### 3. Media Freedom

According to the [UAE's media strategy published on its government website](#), the media must operate with restraint and must comply with the following:

- Not criticize or insult the President or rulers of the UAE, the UAE system of government, the head of another Arab or Islamic State, or any other State
- Not publish anything that would offend national unity, social cohesion, and the national currency

- Not publish anything that incites or insults Islam or other religious beliefs or stirs up sectarian or tribal strife
- Not spread rumors and malicious and misleading or false news
- Respect the cultural heritage of the UAE
- Not publish information that offends children, women, and other social groups, or violates the sanctity of public morals or privacy
- Not publish news, photos, or comments related to the private or family life of individuals
- Not challenge the work of a public official or a person with a public prosecutorial capacity

### What does this mean for COP participants?

- Journalists not from the UAE who are covering COP should familiarize themselves with prohibited media content and be aware that violations of these prohibitions may lead to arrest and detention.
- Exercise care when posting content. UAE laws give authorities broad discretion to censor or ban content that falls within broadly-worded prohibitions.
- Find out if you are considered a media outlet for “fake news” purposes. UAE law penalizes anyone who broadcasts, publishes, republishes, circulates, or recirculates false news or statements or that publishes content that deviates or violates “what has been officially announced.” It is also illegal to “broadcast any sensational propaganda that may incite or provoke public opinion, disturb public security, spread terror among the people, or harm the public interest, the national economy, public order or public health.”

### 4. Pre-trial Detention

If an individual is arrested and accused of violating one of the crimes or restrictions described in the non-exhaustive list above, the

Public Prosecution can order that person to be detained for up to 21 days, after which time the Public Prosecutor must obtain a court order if he wants to extend the detention. UAE law does not provide an upper limit for the period of pre-trial detention, as the court can renew the defendant's detention every 30 days.

### **What does this mean for COP participants?**

- Know that you can always ask for an interpreter.
- Do not sign any document that you cannot read and understand.
- If you are arrested, you should ask to confirm the identity of the person arresting you and immediately reach out to your embassy or consular services, the Legal Protection Hotline, and your safety network.

## **5. Public protest**

UAE law restricts public protest in the following ways:

- It is illegal to protest without a permit, and permits are rarely issued.
- Weapons, fireworks, or anything that might harm people, buildings, or property may not be brought to a protest.
- Demonstrators are not allowed to obstruct road traffic or prevent others from carrying out their work by protesting (as this is a violation of public safety).
- Participants in or organizers of a gathering of five people or more, which disturbs public safety, are subject to imprisonment.
- Anyone who uses digital means to plan or organize a protest without permission from "the competent authority" is subject to imprisonment and fines.

### **What does this mean for COP participants who engage in public protests?**

- The Blue Zone is governed by the UN. The Green Zone is governed by UAE law. This means that IF you participate in a protest, it matters WHERE that protest is.
- Seriously consider **not participating** in a public demonstration or protest outside the conference Blue Zone, as you will be subject to UAE law.
- If you participate in a protest even within the Blue Zone, act with care and discretion.
- If you decide to participate in a protest outside the conference Blue Zone—which is not recommended—make sure not to obstruct access or picket outside a government building.

## **6. National Security**

UAE law broadly defines the crime of terrorism as any act that terrorizes or kills people, causes serious bodily harm or damage to property, and disturbs the security of the State. Terrorism also includes possessing materials that contradict or criticize the principles on which the Islamic religion or its teachings are based, or any action that threatens the stability, unity, or sovereignty of the State. Anyone who publicly declares their hostility to the State or its regime or their disloyalty to its leadership risks imprisonment.

### **What does this mean for COP participants?**

- Educate yourself about the expanded definition of terrorist organizations in the UAE and consider the serious consequences if you are found to protest the UAE government while you are in the country. The law defines "terrorist organizations" as groups of two or more people working to cause a "direct or indirect terrorist outcome" and provides for severe penalties for anyone who establishes, funds, organizes, manages, or leads a terrorist organization. With these definitions, political groups or human rights organizations protesting against the government may be at risk of prosecution as terrorists.

## 7. Freedom of movement

While the UAE Constitution guarantees Emirati citizens freedom of movement and residence within the limits of the law, it also allows the Security Services to prevent anyone from entering or leaving the country.

### What does this mean for COP participants?

- **If you are stopped**, try to figure out if it is a regular police officer or a member of the SSA who has stopped you.
  - ▶ Regular police officers tend to wear gray, green, or khaki uniforms.
  - ▶ SSA officers wear all-black uniforms and black masks covering their faces, but they may also wear civilian clothes.
- **If you are not sure who has stopped you, or if you are stopped by someone in civilian clothes**, respectfully ask for verification of his identity. This is a common practice, and can help you confirm whether the person approaching you is indeed a legitimate law enforcement officer.
- **If you are stopped by a regular police officer**, you can respectfully assert your right not to be searched or arrested without an order from a court. If you are detained, you should immediately call your embassy or consular services if you can, and also text the Legal Protection Hotline and your safety network to let them know what has happened.
- **If you are stopped or detained by a member of the SSA**, you should immediately call your embassy or consular services to seek help if you can, and also text the Legal Protection Hotline and your safety network to let them know what has happened. By promptly notifying others of your situation, you create a record of what has happened, which allows for legal intervention (if necessary).

## 8. Right to a Lawyer and to Consular Protection

Under UAE law, a person accused of a serious felony may ask the court to assign them a lawyer to defend them if they are not able to pay. However, this access to a lawyer is only available during a trial, and it does not allow for the appointment of a lawyer for less serious crimes. UAE law also provides that foreign detainees have the right to communicate with their consular authorities after obtaining permission from the competent public prosecutor.

### What does this mean for COP participants?

- Know that you can always request an interpreter.
- If you are detained by any UAE authorities, ask respectfully to speak with your embassy or consular services and keep asking if you are not permitted to do so right away. During COP, you should also text the Legal Protection Hotline and your safety network to inform them of your situation.
- Do not sign any document that you cannot read and understand.

## 9. Fundraising and Related Activities

Under UAE law, fundraising activities can only be carried out by charities, NGOs, or governmental entities who are licensed and/or authorized by the UAE government to do so, and individuals are forbidden by law from fundraising. As well, any nonprofit organization that seeks to raise funds in the UAE must do so through a licensed UAE entity and must follow a number of steps. Those who violate these restrictions may be punished with imprisonment or heavy fines.

### What does this mean for COP participants?

- Consider that UAE law is in effect everywhere outside the Blue Zone. Within the Blue Zone, activities are regulated by the UN.



- Understand that UAE law strictly limits legal fundraising activities, and what qualifies as such may be interpreted broadly by UAE authorities. It is recommended to only undertake activities that might be construed as fundraising—discussions about proposals and grants, donor organizing, collecting funds—inside the Blue Zone, as that area is regulated by the UN.
- If you do undertake activities that might qualify as fundraising, within a broad definition, inside the Blue Zone, it is recommended that you do so privately and with care and attention to your surroundings.
- Know that digital fundraising efforts, if carried out while in the UAE, subject the individual or organization undertaking these activities to UAE law. For example, a COP participant who tweets about fundraising while at COP exposes themselves to punishment under UAE law. Even fundraising efforts designed to obtain support for activities outside the UAE, if undertaken through digital means, are regulated by UAE law.
- Even if you undertake digital fundraising efforts within the Blue Zone or outside the country, it may be difficult to prove this to UAE authorities. Therefore, consider that if a COP participant is associated with or accredited by an organization engaged in online or social media fundraising while that participant attends COP, it may create additional risk for that attendee.

## II. How to Comply with the Law and Stay Safe While at COP

- **Establish a personal safety network:** Ensure that you have an active and accessible support network while you are at COP. This includes developing secure communication methods and a secure system to track fellow

activists and be tracked, for everyone's safety. (See Information/Digital Security section, Part II of this guide). Ensure that you have verified the safety numbers of your personal safety network on Signal before entering the UAE.

- **Have a companion or “buddy”:** Traveling anywhere outside the Green Zone is safer if you are not alone. This can help to avoid problems and help to address them should they arise.
- **Develop and carry with you your list of critical resources:** These include
  - ▶ The number/email for your country's embassy/consular services in the UAE
  - ▶ The Legal Protection Hotline number/email
  - ▶ The numbers of your safety network contacts
- **Access to web content and communication:** Consider that you may be breaking the law if you use a VPN. Signal text or WhatsApp text is your best method of communication.
- **Carry ID:** Carry identification at all times, preferably a copy of your passport and visa, as random ID checks are possible.
- **Refrain from bringing or using drugs:** Know that penalties for possession or use of illegal drugs, even in small quantities, can be very severe. Bring prescriptions for all medications. Note that a special permit is required for antidepressants.
- **Be careful about taking photos with your phone:** UAE law strictly regulates the taking of photos and requires permission to do without penalties. When you are outside the conference Blue Zone, it is recommended that you not take pictures with your phone or a camera. Never take photos of police or security officials.
- **Be mindful of social media:** Know that if you use your social media presence as a way for

your support network to keep track of your whereabouts, others outside your network are being similarly informed. Therefore, it is recommended that you use your personal safety network and, ideally, the buddy system, to let others know of your whereabouts rather than social media. Also, be mindful about what you post; TikTok influencers have been prosecuted under obscenity laws for posted content.

- **Consider local norms around dress:** For men, this generally means wearing long trousers and avoiding sleeveless shirts in public areas. For women, this generally means covering shoulders, cleavage, and knees. While Western-style clothing is acceptable in many areas, more conservative attire is prevalent in rural or traditional neighborhoods.
- **Be respectful of local cultural norms:** Public displays of affection, such as kissing and hugging, are not culturally acceptable, regardless of gender or sexual orientation. It is also customary to refrain from public displays of affection. Handshakes between men and women are typically acceptable in professional settings but physical contact beyond that is not viewed as acceptable.
- **LGBTQIA+ Identity:** Sexual and gender identities other than heteronormative/binary are either illegal or not recognized. Given the legal restrictions, open expression of LGBTQIA+ identity in public (including through dress, symbols, behavior, or actions) creates legal risk. Public expressions of gender identity may be criminalized under the public morality law.
- **Political Discussions:** Given the strict prohibitions on freedom of expression, political discussions by foreign visitors create risk. Criticizing the government or its policies can lead to significant legal problems.
- **Language:** While many people in the UAE

speak English, learning a few basic Arabic phrases can be helpful and appreciated. In general, if you know English, you do not need to be accompanied by an Arabic speaker. However, if you are stopped by an official or police officer who does not speak a language you can understand, know that you can always ask for an interpreter.

### III. Frequently Asked Questions

#### Entry and exit issues from the UAE

##### 1. Can the government prevent me from entering or returning to the country and can they deport me?

Yes, the government can prevent you from entering or returning to the country, even without a court decision. If an officer prevents you from entering or orders you to leave, it is best to comply. Arguing or resisting such decisions could lead to further complications or legal issues. UAE laws allow UAE authorities to deport you from the country if you pose a threat to their security without a judicial decision.

##### 2. What documents do I need to enter the country?

Your passport must be valid for at least six months from the date you travel to the UAE. Make sure to obtain a visa to the UAE if you are a citizen of a visa-requiring country.

##### 3. If I am stopped at the airport, does a law enforcement officer have the right to search my phone or computer?

They do not have the right to search your mobile phone or computer without permission from the prosecutor or judge. However, be aware that you may be separated from your possessions, including your phone and laptop, and this may give them the opportunity to copy the data or place something into the device. If you are stopped, ask to communicate in a language

you understand. Ask to verify the identity of the person who stopped you. If they ask to search your phone or laptop, ask to see the document that allows them to do so. Consider whether it is possible to easily comply with the search, as the consequences of refusal may escalate the encounter. If the officials insist on searching you without a warrant, you should request embassy/consular assistance, contact the Legal Protection Hotline, and notify your safety network. Regardless of the situation, it is vital to maintain composure and show respect when interacting with authorities. Avoid confrontation and [refrain from touching authorities](#). And remember you can always ask for an interpreter.

#### **4. What should I do if I am detained and interrogated at the airport?**

If you are asked questions about anything other than basic information (your passport, why you came to the UAE), contact your country's embassy/consular services and the Legal Protection Hotline. If you are able to reach your embassy, explain that you need help from a lawyer, interpreter, and/or representative from your embassy. It is not helpful to provide information other than the basics to Emirati security officers without the presence of a lawyer or representative from your embassy.

### **Issues related to protests, gatherings, and public demonstrations**

#### **1. What are the legal requirements to organize a march during COP 28?**

The UAE constitution recognizes the right to peaceful assembly and demonstration in accordance with the law (which means that, among other things, a permit is required for a protest), although note the significant limitations on freedom of expression which create legal risk if the demonstration has a political purpose. Protests or marches that occur without permits are illegal where UAE applies, which is everywhere

in the country except for the Blue Zone (which is regulated by the UN). If you use online means (websites, social media, email networks) without permission from the “competent authorities”, you may be accused of a cybercrime.

#### **2. What should I do to comply with UAE law during a demonstration/march/rally?**

Strongly consider the risks of participating in a demonstration/march/rally in the UAE outside the UN Blue Zone before attending. It is not recommended that you protest outside the Blue Zone, and consider the importance of conducting yourself carefully even inside the Blue Zone.

#### **3. Is it legal for UAE police to disperse a demonstration/march/rally?**

Yes, the gathering can be dispersed if protesters behave in a way that the police believe is a punishable crime, or if the demonstration is no longer peaceful. Security forces are required to ask participants to leave voluntarily by issuing repeated verbal warnings telling participants how to leave. If protesters do not leave peacefully, UAE law allows them to use force.

### **Your rights in case of search and arrest**

#### **1. Is there a requirement for a warrant from the prosecution or the judiciary to arrest me?**

The police can detain you for 48 hours without a warrant or a warrant from the prosecution, after which you must be brought before the judiciary. If you are arrested by the State Security Apparatus, you can be detained for up to 90 days without a court warrant.

#### **2. What should I do if I am searched or arrested by UAE police or security officers?**

If a police officer stops you, you should ask for his identity verification. He only has the right to ask you to prove your personal identity, why you are in the place, and where you are going. He does not have the right to search you without

permission from the prosecution authorities and he has no right to search your mobile phone or computer. If he nonetheless attempts to search you, you should consider whether a refusal to submit to the search will create more problems than if you submit. In any event, remain calm. If you refuse to be searched, or if the police insist on searching you, you should call your embassy/consular services and text the Legal Protection Hotline. Remember that you can always ask for an interpreter if needed to understand what is being asked of you.

### **3. If I am arrested and not an Emirati, what should I do?**

Remain calm and immediately state that you want help from your embassy. Ask your embassy to provide a representative, interpreter, and lawyer. If you are unable to reach your embassy, text the Legal Protection Hotline. It is possible that the UAE authorities will not allow you to communicate with anyone, which is why it is important to always be accompanied by another person, who can contact the embassy or the Hotline on your behalf.

### **4. If I am arrested and detained, do I have the right to speak privately with a lawyer before being questioned?**

Yes, you have the right to be alone with your lawyer in private without anyone present before the investigation begins, although UAE law allows the security services to prevent you from being alone with a lawyer if they believe you have violated the Security Services (anti-terrorism) law.

### **5. Do I have the right to have a lawyer present during my interrogation?**

Yes, you have the right to request the presence of your lawyer during the interrogation. However, UAE law allows you to be interrogated without the presence of a lawyer if the “interest of the investigation” requires that.

### **6. Do I have the right to remain silent?**

Yes, you have the right to remain silent and you have the right to refuse to sign a statement. While you do have these rights, consider the circumstances and the questions you are being asked. In some cases, if you are simply being asked basic questions (your name, why you are in the UAE), you may decide that answering will resolve the issue. However, if you are being asked about anything more than basic information, you should ask to speak with your embassy/consular services and/or ask for a lawyer.

### **7. Am I allowed not to open my phone or computer for the prosecution’s investigations if they so request?**

Yes, you have the right not to hand over your password; the UAE constitution guarantees you this right based on the constitutional principle that the accused is innocent until proven guilty. If the authorities insist, politely inquire about the legal basis for the request, express your willingness to cooperate within the bounds of the law, and ask for legal counsel to protect your rights and interests. It is essential to remain calm and respectful when dealing with law enforcement or security forces.

## **Your rights in relation to LGBTQ cases**

### **1. Does the UAE constitution protect people who are part of the LGBTQIA+ community?**

No, the UAE penal code criminalizes same-sex relations between adult males and trans women, in particular, are at high risk of criminalization. People can also be arrested for a wide range of behaviors that violate UAE law, including public expression of emotions, gender-incompatible expressions, and campaigns for LGBTQIA+ rights. “Public expression of emotions” and “gender-incompatible expressions” refer to actions or behaviors that are perceived as violating traditional gender norms or expressions that are seen as non-conforming to the socially accepted norms of behavior. This can include

public displays of affection or emotions between individuals of the same gender, dressing or presenting oneself in a way that does not align with one's assigned or perceived gender, or advocating for LGBTQIA+ rights and equality.

## **2. How can I reduce the likelihood of my rights being violated based on actual or perceived gender, gender identity, sexual expression, and sexual orientation?**

Consider the consequences of bringing and displaying/wearing banners, flags, posters,

T-shirts, or other forms of expression in pro-LGBT language. In general, adopting a low profile (avoiding attention-drawing behaviors, refraining from public displays of affection, being discreet about clothing choices) is helpful. Participating in any meeting or event except in the place designated for this purpose by the UAE authorities may also expose you to unwanted police attention.

## **Part Two**

---

# **Information & Physical Security**

This section outlines what security risks and measures that attendees traveling to the UAE for COP 28 may want to consider and act on before, during, and after the conference. It has been designed with both digital / information and physical security risks in mind, recognizing the interconnections between the two.

Managing security risks at COP 28 should not be seen as an "all or nothing" endeavor. Any security measures that attendees adopt should balance the risks against other goals that attendees seek to achieve at COP 28.

## **I. Understanding your "baseline" security risks**

In the months and weeks leading up to COP 28, take time to understand the "baseline" security risks you may face when travelling to the UAE for COP 28. This is important as it determines the foundation for what security measures and strategies you will implement.

Understanding your "baseline" security risks when attending COP 28 requires (1) thinking

about what could go wrong and (2) determining how exposed or susceptible you are.

The main security threats to consider within the context of the UAE and COP 28 may include:

- Being arrested or detained and forced to provide access to information on devices or services.
- Having your devices or belongings stolen or lost
- Interference with your devices without your knowledge
- Interference with your communications without your knowledge
- Blocking access to secure services
- Being harassed or intimidated (online or physically)
- Facing convictions or fines for criminalized activities
- Being deported
- Experiencing aggression or intimidation from authorities / law enforcement agents
- Facing attacks against your reputation like

smear campaigns and defamation

- Being subjected to any of the above upon return to your home country

To understand how exposed you may be to these security threats, you should consider:

- Who are the **actors** behind each of these security threats, and what are their capabilities and motivations to inflict harm on you?
- Whether your identity/**individual or collective profile** (e.g. gender/perceived gender, sexual orientation or other protected characteristics) makes you more or less susceptible to these security threats?
- Whether your **role** or **activities planned** at COP 28 and in the UAE make you more or less susceptible to these security threats?
- What are the potential **consequences** of these security threats for you and any allies or partners, and how acceptable would these be for you and/or your allies/partners?

In considering the above, you should not assume:

- That the same security measures, actions or behaviors that you would apply at home would be effective or legal in the UAE
- That UAE laws or practices are the same as in your home country
- That because you are attending an UN international conference you are shielded from any risks or incidents
- That your actions and communications are immune from monitoring and scrutiny from authorities and other key actors

## II. Before Travel

After your “baseline” security measures have been established, this should inform the security

measures you want to implement before traveling. You will have the most control over the security measures you take before you get on a plane; once you are there, your control diminishes. As such, it is strongly recommended to take time before travel to properly prepare.

### Step 1: Set Your Information Security Foundation

Effective information security involves setting a foundational security strategy, and then layering specific security measures on top of that.

The **lowest risk foundational information security strategy** you could adopt for travel to COP 28 would be to travel without any devices or forms of information. However, this may not be feasible, or even recommended, given the importance of maintaining communication and accessing critical information during your trip, particularly in the event of an emergency.

With this in mind, other alternative information security strategies include:

- **Option 1:** Bringing “burner” devices (if resources permit)
- **Option 2:** Wiping all your devices prior to travel and only have access to information you need
- **Option 3:** Manually cleaning copies of information you don’t need from your devices
- **Option 4:** Bringing all information currently on your devices and accessible from them

As you consider these options, keep in mind:

- What your **primary objective** is: Is it to preserve confidentiality, integrity, availability, or anonymity of your information?
- What are the potential **negative consequences** with the different options (such as cost or effort), and what are the

security risks that remain even if you take certain measures? (such as others recording information about you at COP 28).

### **Option 1: “Burner” Devices**

If you are considering bringing a “burner” device (Option 1), it is recommended to:

- Reset the device to factory settings before it is used (note that not all factory resets will achieve a fully “clean” device).
- Make sure that minimum software is installed to allow the device to function properly.
- Only install and configure applications on your burner device that are critically needed during your trip and are permitted in the UAE.
- 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 COP 28

### **Option 2: Reset Devices**

If you are considering wiping all your devices prior to travel and only having access to information you need (Option 2), consider the advice given for Option 1 as well as the following:

- Ensure that any reset being performed is to the whole device, not just the data contained within it or its operating system. It is worth noting that it may only be possible to reset the device to the operating system that was originally installed at the time of purchasing the device.
- If your device is not encrypted, then you can try “filling up” the device with non-sensitive and large files and deleting them when it reaches capacity. This will help with erasing old or hidden data that may remain on your device, even after it has been wiped. Ensure that the device is encrypted during the reset.

- If your device is not currently encrypted, there will likely be significant amounts of data that you will not be able to manually erase. Modern devices use SSDs instead of Hard Disks. SSDs have a significant amount of additional storage capacity than its stated maximum. It uses this extra storage to increase the lifetime of the device, however, you cannot access this extra storage to delete the data, but your adversaries can. You can follow the advice above to force this to be overwritten but you will need to do this repeatedly

### **Option 3: 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. Modern systems scan your data, build search indexes and may keep backup copies of your data in locations other than the files you work on.
- It will not be possible to remove all evidence of previously used online accounts because caches and history will likely include data of the accounts you were signed in as.
- Files that may currently seem to present a low risk may contain tracked changes, comments, and metadata. Adversaries can purchase (or develop) tools that can perform a comprehensive scan of everything available on your device.
- You may also wish to clean sensitive and valuable information from your services keeping in mind the effectiveness of the above

## **Step 2: Take Information Security Measures with Respect to Your Data**

With a foundational information security strategy in place, you can begin thinking about specific

security measures you will take when your information is:

- **At rest** (such as on a powered off device)
- **In use** (such as on powered on device)
- **In motion** (such as being sent or shared between devices)

This section specifically focuses on protecting the confidentiality of data. But note that tools and technology alone won't protect your information; the way you and others act is also critical.

### **Confidentiality of Data At Rest (when you are not using it)**

To protect the confidentiality of information at rest, you should consider:

- Installing full disk encryption as a first line of defense (full disk encryption for your laptop and phones will depend on the make, model and operating system version)
- Using a strong password for your devices and accounts by selecting 3-6 random words or a song title/lyric and then:
  - ▶ Capitalize some of the words
  - ▶ Replace some letters with numbers
  - ▶ Add symbols such as `_`, `-` and `!` between some words
- Keeping devices powered off as frequently as possible
- Making sure your devices are up-to-date with official software
- Using end-to end encrypted platforms for communications and data storage, and familiarizing yourself with what is encrypted and not encrypted on these platforms

### **Confidentiality of Data In Use**

When it comes to protecting the confidentiality of information in use, you should consider:

- Disabling (or know how to quickly disable)

biometric reading or other wearable devices that may unlock your devices without a password

- Using up-to-date software
- Properly configuring anti-malware and firewall software
- Using a strong password
- Enabling two-factor authentication
- Paying attention to warnings and alerts from your device or software that may indicate an attack is in progress
- Paying attention to your surroundings when using your device (such as knowing that others may be looking at your screen when in public spaces)

### **Confidentiality of Data In Motion**

When it comes to protecting the confidentiality of information in motion, you should consider:

- Researching the security measures that any features of the Operating System, applications, or services that you use on your devices have, particularly ensuring that they are communicating your information in an encrypted form and that they are securing any data required to establish secure communication with the service
- Consider not installing, uninstalling, or not using applications or services for the duration of COP 28 that you are not sure are using the highest strength of security
- Researching the limitations of end-to-end encryption when using communication platforms like Signal, WhatsApp or iMessage. For example, such services will not only encrypt your data to and from your devices but also on the service provider's hardware. However, metadata required to route your communication by the system cannot be encrypted and this may jeopardize anonymity if an adversary accesses data on these platforms.



- End to end encrypted services do not protect information on your device or the devices you communicate with. To address this, consider the advice regarding information in use and at rest above.

### 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 one blank / unused page left for the entry stamp.
- Check the visa requirements for entry to the UAE for your specific citizenship and reason for visiting the UAE.
- Apply for your visa in advance to avoid any inconveniences, especially considering visa applications and processing times may increase due to COP 28.
- Ensure you have been issued with or applied for any appropriate accreditation badges or similar documents proving your participation in COP 28, which might be needed for your visa application / entry to the UAE 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 for both visa process and immigration / border control as proof that you are not planning on prolonging your stay in the UAE.
- Bring all relevant documents with you in your carry-on bag and have backup photocopies or digital scans in a secure folder

### Step 4: Take Information Security Measures with Respect to Your Data

- Purchase travel and personal accident insurance that at a minimum provides coverages for emergency medical treatment (ideally up to a limited amount), medical repatriation, political evacuation, any longer-

term medical expenses incurred upon return to your home country (resulting from an accident that occur 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).
- Try to arrange access to funds to cover any emergencies, uninsured situations, or where cash deposits for medical treatment may be required.
- Always keep a copy of the insurance policy with you and have the emergency number saved in your devices and written down somewhere safe.

### Step 5: Safe Packing & Clothing

- Think about what you are bringing with you: Is there anything that might be considered suspicious or could be perceived as an attack to UAE's religious and moral values (such as alcohol, books or magazines with political, activist, sexual or religious content, and products containing cannabis, even if you have a prescription for them). Keep in mind that the law broadly prohibits anything that does not adhere to the UAE's values, which leaves room for customs migratory agents to interpret the law and act under their discretion.
- Be aware of current restrictions and prohibited items, such as anything that may be considered a weapon or law enforcement or military equipment (that might include tools and decorative items as well).
- Consider your attire. Clothes with political messages and/or symbolism may draw unwanted attention and lead to social disapproval and questioning.
- Respect local customs and cultural sensitivities when choosing what outfits

to pack. Clothing that might be perceived as immodest (such as transparent fabrics, tight clothing, or attire that exposes your shoulders, cleavage, and legs) may also lead to unwanted attention.

- Bring any necessary medication accompanied with their prescriptions

## 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).

Consider a network with three types of contact within your support network:

### 1. Trusted individuals outside of the UAE

This could be colleagues, friends, or family that are not physically present in the UAE, and who would be aware of your schedule and movements. Having a trusted contact outside of the UAE that you regularly check-in with (once daily) is recommended as they will be better positioned to respond to an incident, take action to limit consequences of an incident, or activate external support from international providers / community, if this cannot be done from the UAE.

Make sure that any check-in arrangements with contacts outside the UAE are clearly understood by both parties, and that external people who know what to do in the event that a check-in is missed and repeated attempts to establish communication with you have failed. Such actions may increase with urgency the longer that communication with you cannot be made.

### 2. Trusted individuals amongst COP 28 attendees

This could be colleagues, friends, or fellow delegates who are attending COP 28, who

you will maintain regular communication with throughout the conference, including before and after activities outside of COP 28 (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.

### 3. 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 provider (+ any of their assistance providers)
- Legal assistance or representation
- Well-being support and accompaniment
- Local medical facilities
- Security risk advisory and support

## Step 7: Prepare Yourself to Face Identity-Based Questions and Address Cultural Sensitivities

- Prepare yourself for questions about who you are and what you do. Consider that you may be at risk by disclosing personal things about yourself that may be acceptable and legal elsewhere. Think about what you will disclose.
- LGBTQIA+ activists should be especially aware of the UAE’s conservative laws and customs. Consider the risks that may occur with explicit expressions of your sexuality or public displays of affection.

## III. Upon Travel

### Information Security

- Switch off all devices before leaving the plane - you'll be relying on your foundational information security strategy until you reach your destination
- Once at your destination turn on your devices and check that your chosen apps and services are functioning as expected.

### Border Control

- Prepare yourself for border control, including possible questioning on your route, countries you have visited before and why, length of your stay, accommodation in the UAE, your job and activities in your home country, money, and personal questions about things like your religion or sexual orientation.
- Be prepared to respond calmly, convincingly, and in a manner that does not create unwanted attention if you are asked personal questions.
- Keep in mind that regardless of having obtained a visa you will only be allowed entry in the UAE at the discretion of the immigration officer.
- Have relevant documents at hand (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 what is requested.

## DURING THE CONFERENCE

### Information Security

- Keep all your devices powered off, locked, and in a secure location as much as possible, especially when charging and when not in use
- Avoid using chargers other than your own and do not plug in other peripherals or storage devices.

- 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.
- If possible, you should use international roaming instead of purchasing or obtaining a local SIM card because the UAE implements SIM card registration that requires identity documents and biometric data. Failure to do this may result in a criminal offence. If not possible to use international roaming, it is probably better to have a phone with a local SIM card than no phone at all. When engaging with any form of social media or traditional media, keep in mind that you are broadcasting information widely. This communication may serve to provide evidence against you of a criminal offence, or the act of expressing the specific information may itself be a criminal offence in the UAE. (See Part 1: Know the Law Section of this Guide).
- It can be a crime to access prohibited websites and receive unlawful content. The UAE has a national firewall in place to block banned online sources. However, they cannot block specific content on social media platforms directly from the owners of those sites.
- While a VPN may be a useful tool to circumvent UAE blocking of banned online sources, the use of a VPN for this purpose is a criminal offence. If evidence of this content is present on your device then this provides additional ammunition for adversaries against you. If you do not use a VPN, you will not be able to access this content during COP 28
- Furthermore, be aware that using a VPN does not guarantee a continuously secure connection. If you ignore security warnings when connecting then you may not establish a safe connection to your VPN provider in the first place. Your connection to a VPN provider

may drop due to errors or interference and your device may ignore this and continue to send and receive data without the VPN. Finally, you may not have configured the VPN to ensure all traffic is sent over the connection leaving some very sensitive data exposed, such as a list of all sites you access, so do not be under the illusion that connecting to illegal sites is “safe.”

## **Personal Safety & Security**

- If possible, avoid being alone. There is greater safety in groups with other trusted COP 28 attendees
- Be mindful of cultural norms and avoid engaging in speech that could be considered offensive or inflammatory.
- Remember the UAE is a Muslim country and Islam prohibits the consumption of alcohol, so the UAE has strict rules on that matter. While it is not completely forbidden (as foreigners might be able to purchase and consume alcohol in specific circumstances), keep in mind that it is prohibited to drink in public places and there are alcohol-free zones.
- Keep your valuables/belongings secure either in front pockets or contained within zipped or buttoned pockets inside your bag (which should always be secured using a zip or clasp).
- If at the hotel, consider using a safe deposit for any valuable items or belongings that you won't need when outside the hotel.
- Exercise situational awareness at all times by staying informed of any developments and paying attention to your surroundings for anything out of the ordinary.
- Familiarize yourself with key locations in any buildings where you will spend time (emergency exits at your hotel, conference venue, restaurants)
- Be aware that attending unofficial events

outside the official Blue Zone, like public gatherings and demonstrations, poses a significantly heightened risk for COP attendees. Public gatherings and demonstrations outside the Blue Zone are highly regulated in the UAE, are illegal without a permit, and law enforcement agents have the authority to use force under certain circumstances should the protest be deemed illegal.

- Carry an ID with photo and your accreditation badges with you at all times.

## **Accommodation security**

- Choose reputable and secure hotels (considering proximity to the venue, ratings, and reviews from former customers, and security measures - like a 24 hour reception desk, access card to the room, 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.
- Uber is licensed in the UAE, but is more expensive than a taxi. If you use Uber, make sure to check the reviews and ratings of the drivers.
- It is illegal to carpool or use ride-share services in the UAE and it is illegal for a driver without a proper license to haul passengers.
- Avoid being by yourself both during official events but especially when outside the Blue Zone. Always try to pair up with a colleague or friend, or to move around in groups.

- Check in with an event buddy or your delegation upon departure, arrival and return.

## **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 have manually cleaned 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.
- When you have returned to your home country, you can bring your devices back to the configuration in place before COP 28; however, you might use the opportunity to limit the information on your devices and accessible from them going forward.

### **Re-assessing “baseline” security risk at home**

- Re-assess 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 hibernation or 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 the 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 suspect you are about to be detained:**

- Disable biometric and other access controls to your information so that actual passwords are required. On some devices, holding the power button for 10 seconds will achieve this in an emergency

**You suffer attacks to your reputation like smear campaigns and defamation**

- 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](#).