FRONT LINE DEFENDERS
THE INTERNATIONAL FOUNDATION FOR THE PROTECTION OF HUMAN RIGHTS DEFENDERS

WWW.FRONTLINEDEFENDERS.ORG

PROTECT ONE EMPOWER A THOUSAND

DIGITAL PROTECTION ADVICE BULLETIN
FOR PARTICIPANTS OF COP-24, KATOWICE, POLAND 3-14/DECEMBER/2018

This Digital Protection Advice Bulletin is intended for all attendees of the 2018 UN climate change conference (COP-24) in Katowice, Poland, who feel their participation in this international event could be curtailed by any adversary, and particularly in light of the the heightened surveillance mandated by Poland's so-called "COP-24 law" (see more here). Specifically, this guide is meant for civil society members and journalists who believe they could be targeted. Implementing the measures recommended in this guide would not eliminate the threats altogether, but should help improve the security of participants' communications and digital information so that, hopefully, they are able to make the most of their participation in the summit.

FRONT LINE DEFENDERS EMERGENCY CONTACT FOR CIVIL SOCIETY MEMBERS:
+353-1-210-0489 Skype: front-line-emergency Secure Contact Form

---

FOR LAPTOPS, TABLETS, SMARTPHONES

To increase the protection of your digital data:

- Only bring to Katowice devices and information that is needed there. Consider bringing fresh (burner) devices. Consider using devices with fresh pre-paid phone number and SIM card bought outside in other EU country then Poland.
- Update all the software, programs and apps you use and have, including operating systems, to their latest versions before arriving in Katowice.
- During your stay in Katowice do not update your devices or install any programs or apps to avoid infecting your devices.
- Protect your devices with strong passwords (see how here and here). Strongly consider implementing two factor authentication on any accounts that support it (see how here or here)
- Encrypt your devices (see how here). In case of particularly sensitive data, consider encrypting it again within the device (see how here).
- Fully power off your device when not in use or if you expecting you may be searched (e.g. when crossing the border, upon entering the COP-24 venue, etc.).

To reduce the risk of being tracked,

- Fully power off your mobile phone when not in use and before going for meetings.

To minimize the risk of surveillance of communications,

- For secure text and calls, use apps such as Signal, Wire or Whatsapp, Jitis Meet instead of the standard cellular network (GSM calls and SMS).
- Always use VPN (for example this) and/or Tor Browser. Prepare and test your VPN before travelling.
- Be cautious of connecting to untrusted wifi networks, they may be spying on your communication or may try to infect your devices.