



Travel OpSec Checklist

Before the trip, at the border, after your return · belongs to Chapter 19 · Destination: _____ · Date: _____

Device: ☐ Everyday device ☐ Travel device ☐ Travel profile on the everyday device

Decisions are made at home, not at the counter. Border crossings are no place for improvisation. Whether you hand over a password or not, you decide before the trip with a clear head, not under pressure. At the counter you only carry out what is on this sheet. A powered-off device is in its most secure state: all keys are gone, nothing is decrypted. The sheet names no menu paths, because interfaces age. It may be found, so it holds only check marks and short notes.

1 · BEFORE THE TRIP

Item	OK	Note
Complete backup exists. In case the device is confiscated and not returned. Backup and device never travel together, the backup drive stays home.		
Travel device or travel profile set up. Only the apps needed on the trip, no private data, no access to contacts, photos or professional communications from the main profile.		
Logged out of cloud accounts you do not need on the trip. As long as you are logged in, cached cloud content can be extracted too. Unneeded apps with sensitive data uninstalled or logged out.		
Biometrics disabled, travel with PIN or password only. If you want to keep the fingerprint, use the two-factor variant: after the scan the PIN is required as well, the finger alone is not enough.		
Auto reboot set to a short interval. Adjustable between 10 minutes and 72 hours. After the reboot, no keys remain in working memory.		Interval: _____
USB protection set. When locked, new USB connections are blocked (default). For the border set the USB-C port to "Off": powered on, the device then neither charges nor connects, powered off it still charges.		
Duress password set and consequence understood. Clearly different from the normal code, safely memorized, written down nowhere. It wipes the device immediately and irreversibly, including eSIMs.		
SIM strategy decided. Your own SIM stays home, a local SIM at the destination or an eSIM for the destination country not linked to your main identity. A foreign SIM does not make the device anonymous, the network recognizes the device identifier (Chapter 6).		Option: _____
Decision on handing over the password made. Refusal can have consequences, up to confiscation or denial of entry. This decision is made now, not at the counter.		

2 · AT THE BORDER

Item	OK	Note
Device powered off completely before entering the checkpoint zone. If you are in the travel profile: "End session", then the profile's keys are out of working memory.		
Main profile not unlocked since the last reboot. What was never unlocked has no keys in working memory.		
No unlocked device handed over. What leaves your hand unlocked can be opened.		
Stay polite, do not lie, do not obstruct the search. These are obligations that can be enforced. Everything else was decided beforehand.		

3 · AFTER THE TRIP

Item	OK	Note
Device treated as compromised after confiscation and return. Forensic analysis or manipulation can happen in a short time.		
Not used further until you are in a secure environment.		
Passwords changed from a different device.		
In case of doubt: GrapheneOS reinstalled and restored from backup.		
Travel profile deleted when no longer needed.		

4 · WHAT GRAPHENEOS DOES FOR YOU AT THE BORDER

Feature	Effect
Duress password	Second code at the unlock screen. Wipes the device immediately and completely, including eSIMs, without a reboot and with no way to interrupt it.
Auto reboot	After the set locked period the device reboots. Afterwards no keys remain in working memory, forensics meets encrypted storage.
USB protection	When locked, the data lines of the USB-C port are disabled at the hardware level, not just in software. On "Off" charging is blocked too.
End session	Logs out a secondary profile and removes its keys from working memory. The data is preserved, the profile is locked. A simple user switch would leave the keys in memory.
Memory zeroing	Freed memory is overwritten with zeros, after locking residual PINs and passwords are cleared immediately. Disk keys remain until reboot or end of session, hence the auto reboot.
PIN scrambling	The numeric keypad is rearranged with each unlock attempt. Smudge marks, cameras and shoulder surfers do not reveal the PIN.

⚠ **Not legal advice.** The legal landscape changes and differs by country. When in doubt, consult legal counsel. ⚠ **Biometrics can be compelled without your cooperation, a password only with it.** The consequences of refusal depend on the country. ⚠ **The duress password wipes irreversibly, including eSIMs.** No undo, no recovery. Only set it if a working backup exists.