



Reise-OpSec-Checkliste

Vor der Reise, am Grenzübergang, nach der Rückkehr · gehört zu Kapitel 19 · Reise nach: _____ · Datum: _____

Gerät: ☐ Alltagsgerät ☐ Reisegerät ☐ Reiseprofil auf dem Alltagsgerät

Entscheidungen fallen zu Hause, nicht am Schalter. Grenzübergänge sind kein Ort für Improvisation. Ob du ein Passwort herausgibst oder nicht, entscheidest du vor der Reise mit klarem Kopf, nicht unter Druck. Am Schalter wird nur noch ausgeführt, was auf diesem Blatt steht. Ein ausgeschaltetes Gerät ist der sicherste Zustand: alle Schlüssel sind weg, nichts ist entschlüsselt. Das Blatt nennt keine Menüpfade, denn Oberflächen altern. Es darf gefunden werden, deshalb stehen nur Häkchen und Kürzel darauf.

1 · VOR DER REISE

Punkt	OK	Notiz
Vollständiges Backup vorhanden. Für den Fall, dass das Gerät beschlagnahmt oder nicht zurückgegeben wird. Backup und Gerät reisen nie zusammen, das Backup-Medium bleibt zu Hause.		
Reisegerät oder Reiseprofil eingerichtet. Nur die Apps, die unterwegs nötig sind, keine privaten Daten, kein Zugriff auf Kontakte, Fotos oder berufliche Kommunikation aus dem Hauptprofil.		
Cloud-Konten abgemeldet, die du unterwegs nicht brauchst. Solange du eingeloggt bist, lassen sich auch im Cache liegende Cloud-Inhalte auslesen. Nicht benötigte Apps mit sensiblen Daten entfernt oder abgemeldet.		
Biometrie deaktiviert, Reise nur mit PIN oder Passwort. Wer den Fingerabdruck behalten will, nutzt die Zwei-Faktor-Variante: nach dem Scan wird zusätzlich die PIN verlangt, der Finger allein reicht nicht.		
Automatischer Neustart auf ein kurzes Intervall gesetzt. Einstellbar zwischen 10 Minuten und 72 Stunden. Nach dem Neustart liegen keine Schlüssel mehr im Arbeitsspeicher.		Intervall: _____
USB-Schutz gesetzt. Im gesperrten Zustand sind neue USB-Verbindungen blockiert (Standard). Für die Grenze auf „Aus“: das eingeschaltete Gerät lädt dann nicht und baut keine Verbindung auf, ausgeschaltet lädt es weiterhin.		
Notfallpasswort gesetzt und Konsequenz verstanden. Klar verschieden vom normalen Code, sicher im Gedächtnis, nirgends notiert. Es löscht das Gerät sofort und unwiderruflich, samt eSIMs.		
SIM-Strategie entschieden. Eigene SIM bleibt zu Hause, lokale SIM vor Ort oder eSIM für das Zielland ohne Bezug zur Hauptidentität. Eine fremde SIM macht das Gerät nicht anonym, das Netz erkennt die Gerätekennung (Kapitel 6).		Weg: _____
Entscheidung zur Passwort-Herausgabe getroffen. Verweigerung kann Folgen haben, bis zur Beschlagnahme oder Einreiseverweigerung. Diese Entscheidung fällt jetzt, nicht am Schalter.		

2 · AM GRENZÜBERGANG

Punkt	OK	Notiz
Gerät vor dem Betreten der Kontrollzone vollständig ausgeschaltet. Wer im Reiseprofil unterwegs ist: „Sitzung beenden“, dann sind die Schlüssel des Profils aus dem Arbeitsspeicher.		
Hauptprofil seit dem letzten Neustart nicht entsperrt. Was nie entsperrt wurde, hat keine Schlüssel im Arbeitsspeicher.		
Kein entsperrtes Gerät übergeben. Was entsperrt aus der Hand geht, kann geöffnet werden.		
Höflich bleiben, nicht lügen, die Durchsuchung nicht behindern. Das sind Pflichten, die durchgesetzt werden können. Alles andere ist vorher entschieden.		

3 · NACH DER REISE

Punkt	OK	Notiz
Gerät nach Beschlagnahme und Rückgabe als kompromittiert behandelt. Forensische Analyse oder Manipulation kann in kurzer Zeit erfolgen.		
Nicht weiter genutzt, bis du in einer sicheren Umgebung bist.		
Passwörter von einem anderen Gerät aus geändert.		
Im Zweifel: GrapheneOS neu installiert und aus dem Backup wiederhergestellt.		
Reiseprofil gelöscht, wenn es nicht mehr gebraucht wird.		

4 · WAS GRAPHENEOS AN DER GRENZE FÜR DICH TUT

Funktion	Wirkung
Notfallpasswort (Duress)	Zweiter Code am Entsperrbildschirm. Löscht das Gerät sofort und vollständig, samt eSIMs, ohne Neustart und ohne Möglichkeit zum Abbruch.
Automatischer Neustart	Nach der eingestellten Sperrzeit startet das Gerät neu. Danach liegen keine Schlüssel im Arbeitsspeicher, Forensik trifft auf verschlüsselten Speicher.
USB-Schutz	Im gesperrten Zustand werden die Datenleitungen des USB-C-Anschlusses auf Hardware-Ebene deaktiviert, nicht nur die Software. Auf „Aus“ auch das Laden.
Sitzung beenden	Meldet ein sekundäres Profil ab und löscht seine Schlüssel aus dem Arbeitsspeicher. Die Daten bleiben, das Profil ist gesperrt. Beim bloßen Nutzerwechsel blieben die Schlüssel im Speicher.
Arbeitsspeicher-Bereinigung	Freigegebener Speicher wird mit Nullen überschrieben, nach dem Sperren werden Reste von PIN und Passwort sofort gelöscht. Die Datenträgerschlüssel bleiben bis Neustart oder Sitzungsende, deshalb der automatische Neustart.
PIN-Scrambling	Die Zifferntastatur wird bei jedem Entsperrversuch neu angeordnet. Schmauchspuren, Kameras und Schulter-surfer verraten die PIN nicht.

⚠ **Keine Rechtsberatung.** Die Rechtslage ändert sich und ist je Land verschieden. Im Zweifel Rechtsbeistand konsultieren. ⚠ **Biometrie lässt sich ohne dein Zutun erzwingen, ein Passwort nur mit deiner Mitwirkung.** Welche Folgen eine Verweigerung hat, hängt vom Land ab. ⚠ **Das Notfallpasswort löscht unwiderruflich, samt eSIMs.** Kein Rückgängig, keine Wiederherstellung. Nur setzen, wenn ein funktionierendes Backup vorhanden ist.