

Ich packe meinen Koffer ...

- Vertrauliche oder sensible Unterlagen gehören nicht ins Reisegepäck.
- So wenig technische Geräte mitnehmen wie möglich – damit Sie den Überblick behalten!
- Reise-Laptops nutzen – ausschließlich mit Daten, die sie für die Reise benötigen!
- Geschäftliches von Privatem trennen! Auf private Geräte gehört nichts Geschäftliches – vice versa.

Ausstattung, Verschlüsselung und Datenübertragung

- Monitore stets mit einer Sichtschutzfolie ausstatten: Laptops, Tablets, Smartphones, etc.
- Notebooks vor Reiseantritt immer mit der aktuellsten Version eines Virenschutzprogramms ausstatten! Alle Programm-Updates **vor** Reisebeginn aktualisieren!
- Passwortgeschützte Bildschirmsperre aktivieren (< 1 Minute)!
- Mitgeführte Laptops verschlüsseln, um Daten bei Verlust der Hardware zu schützen!
- Smartphones ebenfalls verschlüsseln, sperren und die Option der Fernlöschung einstellen!

Es gibt Länder, die eine Entschlüsselung bei der Einreisekontrolle verlangen können (z. B. USA) oder wo eine Einfuhr von Verschlüsselungssoftware – auch auf Datenträgern – generell verboten ist (z. B. China, Russland). Bitte erkundigen Sie sich vor der Reise diesbezüglich über die individuellen Einreisebestimmungen des jeweiligen Landes.

- Bluetooth und W-LAN bei Nichtgebrauch abschalten (Einfallsweg von Hackern)!
- W-LAN-Netze nur im Notfall nutzen!
- Wenn immer möglich, Internet und E-Mail über eine VPN-Verbindung nutzen!
- Auf Reisen niemals vertrauliche Details und Unterlagen per E-Mail versenden!
- Grundsätzlich besteht auf Reisen immer die Gefahr, dass eine Korrespondenz (wie auch immer geführt: E-Mail, Firmen-Plattformen, Soziale Netzwerke, Business Netzwerke wie Xing und LinkedIn usw.) von Dritten mitgelesen werden kann.
- Weder auf Reisen noch nach der Rückkehr USB-Sticks oder ähnliche externe Speichermedien nutzen, die Ihnen Dritte/Fremde angeboten haben!
- Achten Sie darauf, dass auf Ihren elektronischen Endgeräten (Smartphone, Tablett, Notebook) im Ausland keine kritischen (anzügliche, pornografische, religiöse, politische) Inhalte in Form von Texten oder Bildern vorhanden sind. Dies kann Ihnen u. U. erhebliche Probleme bereiten und/oder auch zur Konfiszierung der Geräte führen!

Verhalten im öffentlichen Raum

- Keine geschäftlichen Gespräche, ob per Telefon oder persönlich, im öffentlichen Raum führen – selbst vermeintlich Belangloses kann schädigend sein.
- Unterlagen nie offen liegenlassen! Bereits ein Titel kann zu viel offenbaren.
- Unterlagen/Laptops/Taschen etc. nie unbeaufsichtigt zurücklassen! Auch nicht für den kurzen Moment, wenn Sie bspw. für ein persönliches kurzes Gespräch aus dem Raum gebeten werden.
- Nicht mehr benötigte sensible Unterlagen so vernichten, dass Informationen nicht mehr zu erkennen sind, z. B. Herunterspülen als Schnipsel in der Toilette!

Das Hotelzimmer ist kein privater Raum

- Unterlagen und elektronische Geräte nicht unbeaufsichtigt im Hotelzimmer lassen!
- Zimmer-/Hotelsafe an der Rezeption bieten keinen echten Schutz – Angestellte haben die Möglichkeit, mit einem Generalschlüssel oder -code Zugang zu erlangen.
- Vertrauliche und sensible Gespräche nicht im Hotelzimmer führen: weder persönlich Face-to-Face noch über Mobiltelefon/Hoteltelefon. Denn in manchen Ländern werden versteckte Aufzeichnungen von allen Aktivitäten in Hotelzimmern angefertigt.

Nach der Reise

- Elektronischen Endgeräte nach der Reise auf Unversehrtheit/Kompromate hin checken!
- Geschäftsreise hinsichtlich ungewöhnlicher Ansprachversuche anderer Vorfälle rekapitulieren!
- Bei auffälligen Vorkommnissen Vorgesetzten/Sicherheitsabteilung ansprechen.
- Im Verdachtsfall Experten vom Verfassungsschutz hinzuziehen!