Die Justiz des Landes
Nordrhein-Westfalen

Handlungsanweisungen bei Dienstreisen ins Ausland

Titel:	**Handlungsanweisungen bei Dienstreisen ins Ausland**		
Zielgruppe:	Alle Bediensteten der Justiz		
Version:	0.3	Datum:	02.11.2022
Status:	**final**	Seite:	1 von 5
Klassifikation:	Justiz-Intern	Verantwortlich:	Ministerium der Justiz

1 Einführung

1.1 Zweck des Dokumentes

Das vorliegende Dokument enthält Handlungsanweisungen, die aus Sicht der Informationssicherheit bei Dienstreisen ins Ausland zu beachten sind. Diese Anweisungen finden auch bei privaten Reisen ins Ausland Anwendung, falls während der Reise dienstlich bereitgestellte IT-Geräte[1] verwendet werden. Sie ergänzen die Bestimmungen in § 9 der Dienstanweisung zum Datenschutz und zur Informationssicherheit (DA DI). Diese gilt insgesamt auch für Auslandsreisen unter Mitnahme dienstlicher Hardware oder Daten.

Die hier beschriebenen Handlungsanweisungen beruhen im Wesentlichen auf den Ausführungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu Auslandsreisen[2].

1.2 Rolle des Informationssicherheitsbeauftragen (ISB)

Der/die bei der zuständigen Mittelbehörde ansässige Informationssicherheitsbeauftragte (ISB) bzw. die Zentralstelle für Informationssicherheit im Justizvollzug unterstützt die Behörde und die/den Reisende/n dabei, die Belange der Informationssicherheit während der Reise zu wahren.

Die Behördenleitung hat den/die ISB unverzüglich nach Eingang einer Anzeige oder eines Antrags auf Erteilung einer Ausnahmegenehmigung nach § 9 DA DI zu informieren.

Der/die ISB empfiehlt einzelne Maßnahmen anhand der speziellen Gegebenheiten im Reiseland und der Umstände der Reise. Bei regelmäßigen Dienstreisen in Länder, in denen nach dem Schengener Abkommen[3] Grenzkontrollen grundsätzlich nicht erfolgen (sog. Schengen-Staaten), kann die Behörde gesonderte Vereinbarungen mit dem/der ISB treffen. In diesen Vereinbarungen kann erleichternd geregelt werden, dass der/die ISB hierzu in allgemeiner Weise beteiligt wird, so dass seine/ihre Einbeziehung nicht vor jeder einzelnen Reise erfolgen muss.

[1] IT-Geräte sind im Sinne der Definition aus § 1 Abs. 2 und § 7 Abs. 1 DA DI insbesondere PC, mobile Geräte (Smartphones, Tablets o.ä.) und Speichermedien.

[2] Informationssicherheit auf Auslandsreisen (IT-Grundschutzkompendium – Edition 2019, Baustein CON.7, BSI)

[3] https://www.auswaertiges-amt.de/de/newsroom/buergerservice-faq-kontakt/faq/17-schengenstaaten/606502

2 Allgemeine Regelungen

Grundsätzlich sind durch die/den Reisende/n unabhängig vom Reiseland folgende Regelungen zu beachten:

- Nutzung öffentlicher WLAN-Verbindungen nur über VPN-Verbindungen
- Zugang in das Landesverwaltungsnetz nur über die ausgehändigten IT-Geräte
- Keine private Nutzung dienstlicher IT-Geräte
- Keine Weiterleitung dienstlicher Informationen auf private IT-Geräte
- Kein Einsatz privater oder ungetesteter IT-geräte zur Verarbeitung dienstlicher Daten
- Nutzung der IT-Geräte nur durch die dazu befugten Beschäftigten
- Verwendung eines persönlichen Benutzerkennwortes
- Schutz der IT-Geräte vor unberechtigter Einsichtnahme oder Veränderung, insbesondere Sperrung der Geräte bei Nichtbenutzung
- Ausschließlicher Zugriff auf die für die übertragene Aufgabe notwendigen Informationen und Programme
- Sofortige Meldung von Verlust oder Veränderung der IT-Geräte an die Behörde
- Bei Zwang zur Offenlegung der IT-Geräte oder sofern diese in Fremdbesitz waren (Einreisekontrolle), sind diese auszuschalten und der/die ISB zu informieren
- Deaktivierung aller Funkverbindungen (Bluetooth, WLAN, mobiles Datennetz etc.), solange diese nicht konkret benötigt werden
- Aufladen der Geräte ausschließlich mit persönlich mitgeführten Netzteilen. Das Aufladen an einem USB-Port ist ausdrücklich untersagt.

Ebenso greifen die gängigen Handlungsempfehlungen zum Selbstschutz und Schutz dienstlicher Informationen auf Dienstreisen:

- Keine Besprechung dienstlicher Angelegenheiten in der Öffentlichkeit
- Kein Arbeiten an öffentlichen Plätzen ohne Ergreifung von geeigneten Schutzmaßnahmen (z.B. Sichtschutzfolie)
- Verwendung neutraler Unterlagen (keine Laufmappen des Ministeriums)
- Information des Beratungstelefons Informationstechnik (BIT)/Dezernat 2 des Zentralen IT-Dienstleisters der Justiz des Landes Nordrhein-Westfalen, wenn der Verdacht auf Schadsoftware oder sonstige verdächtige Vorgänge besteht

Die individuelle Sicherheit kann durch zusätzliche Maßnahmen noch erhöht werden:

- Sichtschutzfolien auf Bildschirmoberflächen
- Sicherheitsschloss für Notebook / Deponierung der Geräte in einem Hotelsafe
- Verschlüsselung wichtiger Datensätze oder Datenträger
- Nach Möglichkeit Aktivierung der Ortungsfunktion der IT-Geräte zur Standortbestimmung im Notfall

Die entsprechenden Maßnahmen empfiehlt der/die ISB anhand der speziellen Gegebenheiten im Reiseland.

3 Reisen in sicherheitstechnisch unbedenkliche Staaten

Reisen in Schengen-Staaten gelten als sicherheitstechnisch unbedenklich. In diese ist eine Mitnahme dienstlicher Geräte und Informationen, sofern diese nicht vertraulich sind, möglich.

Die unter Kapitel 2 aufgeführten Maßnahmen sind dennoch zu befolgen. Dem/der ISB bleibt unbenommen, im Bedarfsfall von diesen Handlungsanweisungen abweichende Maßnahmen zu empfehlen.

4. Reisen in Staaten mit kritischer Sicherheitslage

Für alle Nicht-Schengen-Staaten gelten zusätzliche Anforderungen. Gründe hierfür können eine instabile gesellschaftliche oder politische Lage, eine starke Aktivität des dortigen Geheimdienstes oder spezielle rechtliche Anforderungen darstellen, die in etwa die Durchsuchung oder Beschlagnahmung dienstlicher IT-Geräte erlauben.

Entsprechend muss der ISB einen individuellen, an das Zielland angepassten Maßnahmenkatalog erstellen.

Unmittelbar nach der Reiserückkehr sind die mitgenommenen Geräte durch den Betreuungsverbund zu überprüfen, im Bedarfsfall ist durch diesen eine sichere Löschung der Datenträger vorzunehmen.

Folgende Maßnahmen können je nach Reiseland und –situation sinnvoll sein:

- Verwendung dedizierter Reise-Hardware
- Verschlüsselung der tragbaren IT-Geräte
  Ist dies im Zielland nicht zulässig, sollte auf die Mitnahme grundsätzlich verzichtet werden. Anderenfalls dürfen sich keine dienstlichen Daten auf dem IT-Gerät befinden. Kryptografische Schlüssel sind getrennt vom verschlüsselten Gerät aufbewahren.
- Einschränkung der Zugriffsberechtigungen für die Dauer der Dienstreise
- Verzicht auf Businesskleidung zur Vermeidung von Aufsehen
- Keine direkte Taxiverbindung zur Unterkunft verwenden
- Zurückhaltung in Hotelzimmern, da diese abgehört werden könnten
- Verlangen eines neuen Hotelzimmers nach Ankunft
- Bei größeren Tagungen, Messen, Konferenzen etc. zurückhaltend agieren
- Wachsamkeit bei vermeintlichem „Smalltalk“
- Gespräche eher abbrechen, bevor dienstliche Informationen bekannt werden
- In Ländern, in denen aufgrund rechtlicher Bestimmungen oder technischer Beschränkungen der Einsatz von VPN-Technik nicht möglich ist, muss auf die Einwahl in das Landesverwaltungsnetz verzichtet werden.
- Verwendung neutraler Unterlagen: Akten und Mappen darf man äußerlich nicht ansehen, dass sie dem Land NRW und insbesondere dem Ministerium zugehörig sind. Des Weiteren ist auf Mappen und Akten auf die Beschriftung mit Vertraulichkeitseinstufungen zu verzichten.
- Schutzbedürftige Datenträger und Dokumente sind nach Beendigung der Reise in der Behörde entsprechend sicher zu vernichten.
- Mitnahme der IT nur im Handgepäck
  Besteht der Zwang zur Offenlegung der IT-Geräte oder waren diese in Fremdbesitz (Einreisekontrolle) sind diese auszuschalten und während der gesamten Reise nicht mehr zu nutzen. Der ISB ist zu informieren. Die ausgegebenen Geräte werden nach Abschluss der Reise durch den Betreuungsverbund auf Schadsoftware geprüft. Anschließend werden die Geräte vor einer erneuten Nutzung gelöscht.
- Die Geräte sind nicht unbeaufsichtigt beispielsweise im Hotelzimmer liegen zu lassen, sondern stets mit sich zu führen (Diebstahlsicherung).