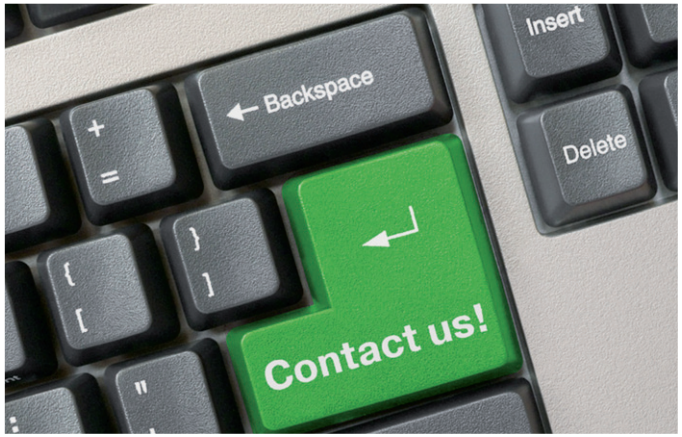
Recommended action

After the trip:

- Check your travel laptops as well as smartphones and storage media for malware
- Evaluate the trip afterwards with regard to any possible conspicuous incidents
- Exchange experience with others
- Contact the German domestic intelligence services in case of any security-related incidents

Do not hesitate to contact us and make an appointment for confidential awareness talks



Your points of contact in economic security

initiative wirtschaftsschutz

Protecting values in a concerted effort

For additional information and your local contacts' communication data, please visit the website.

www.wirtschaftsschutz.info

Imprint

Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states

Pictures: © Parris Cope - Fotolia.com
© Westend61 - Fotolia.com
© Nikolai Sorokin - Fotolia.com

DOI: March 2016

Domestic intelligence service

Federal Republic of Germany
Federal States

Economic Security

Security when travelling abroad

Business trips

Economic Security

Different countries – different customs

Opening up new markets in other countries provides a whole lot of economic opportunities to companies. However, numerous security risks go hand in hand with these opportunities.

When travelling on business, please keep the following in mind:

The legal situation in the host country may significantly differ from that prevailing in Germany. Are you e.g. allowed to import an encrypted USB flash drive into the country of destination, or are there any restrictions on taking pictures?

Foreign intelligence services benefit from a "home advantage" when acting on their own territory. Their acting is often based on extensive executive powers.

Prevention through Dialogue and Information

Examples

- Total monitoring of the Internet and of telecommunications, as well as of postal services
- Blocking of particular Internet sites
- Clandestine and purposeful searches of hotel rooms and baggage
- Manipulation of mobile devices and data carriers
- Creation of compromising situations
- Arbitrary repressive measures by the state
- Prevention of departure by means of bogus traffic accidents
- Blackmailing due to contacts with oppositionists
- Infection of mobile devices through Trojans on other individuals' USB flash drives

Recommended action

Prior to the trip:

- Carry out research regarding the threat and security situation in your country of destination
- Take contact details with you for cases of emergency
- Obtain information on legal regulations
- Observe the principle of data economy and use travel laptops/smartphones without sensitive company data

During the trip:

- Be sceptical about attempts to get into contact and presents
- Be vigilant when dealing with service providers
- Be cautious with political topics
- Do not give sensitive information away; your hotel room and the hotel safe are not secure
- Use – authorised – encryption products
- Reduce confidential communication to the essential minimum
- In cases of suspected data loss or unusual occurrences, please notify your home company immediately.