Information sheet for business travel to countries outside Europe

This sheet is intended to provide information for business travel to countries outside Europe when carrying one or more data storage media.

Data storage media includes all electronic equipment that can be used in different locations, and which serves as data storage devices, such as laptops, smartphones, PDAs, mobile telephones, MP3 players, CD-ROMs, DVDs, external hard drives, USB sticks, digital cameras etc.

The following restrictions apply when travelling to countries outside Europe, in particular to countries where security is a particularly critical factor, such as China and Russia, as well as the USA.

SEARCH AND EXAMINATION OF MOBILE STORAGE CARRIERS

As of July 16, 2008, two US administrative bodies that are responsible for border protection and import control, and which both report to the Department of Homeland Security, are entitled to conduct searches on the mobile data storage carriers of anybody wishing to enter, leave, or travel through, the USA, without having to provide a specific reason. According to the corresponding guidelines, officials are may retain data or copies of data, for examination.

Encrypting data or data carriers to protect them from potential examination is only of limited use. While it is generally permitted to carry encryption software when entering the USA, US authorities nevertheless have the right to forward the data they impound to other government or private offices for deciphering.

Similar regulations also apply in other countries. For instance, India and Australia have laws obligating owners to decrypt their data.

IMPORT BANS ON ENCRYPTION SOFTWARE

Several countries, such as China, Russia, Kazakhstan, Ukraine and Belarus have import restrictions on encryption software. Encryption software may only be imported if the country in question has issued a corresponding license. Such regulations consequently amount to an import ban on the type of encoding software that is typically used in Western countries.

These restrictions and bans apply even to the simple existence of such software on data carriers. This applies even if the software is not forwarded to third parties.

The sole exception is software that contains an encrypting component as an "ancillary function", such as web browsers (these can create encryption connections to websites) or mobile telephones (these typically encrypt radio-link communication).

Infringements of these import bans entail consequences that can include confiscation of the data carrier, refusal of entry to the country, through to personal confrontation with the authorities.

RECOMMENDATIONS

The following points should be observed before travelling on business to countries outside Europe, particularly to the above-mentioned states.

1. Do not carry private data or private mobile storage carriers with you.
2. Do not take your usual working equipment, but instead have your IT department prepare a newly preconfigured device.
3. Do not install any additional software, particularly encryption software.
4. Only take along data that you absolutely require, and where there are potentially no negative consequences for the MPS if the nature of the data were to become known to foreign government authorities.
5. Confidential and sensitive data should be stored on an MPS server or in a web mail account at your institute, where it can be downloaded in encrypted form via a web browser using HTTPS via the network.
6. Do not leave your mobile equipment unattended. This also applies to hotel rooms and conference rooms. Hotel safes also offer no security in this respect.
7. Report any inspections to your institute management as soon as you return from your business trip.
8. Turn over mobile equipment - regardless of whether any inspections have occurred or not – to your IT department so that the equipment can be examined, and, if required, reconfigured.

If you have any further questions, please consult the Max Planck Society's IT security manager at it-sicherheit@mpg.de, Tel. 089-2108-1317.