Factsheet

"Using apps on mobile devices that are used for work purposes in the Federal Administration"

What do I need to know?

The use of ICT federal applications with mobile devices is regulated in application directive no. E021 on smartphone/smart tablet synchronisation.
E021 - Application directive on smartphone/smart tablet synchronisation

This factsheet contains federal recommendations regarding the use of apps on work-related mobile devices and private mobile devices that are used for work purposes. It is aimed at federal employees.

04/2023

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Finance FDF
National Cyber Security Centre NCSC

Less is more when installing apps

Every additional app poses a potential security risk. So any apps that you are no longer using should be deleted. The fewer apps you have, the easier it is to keep track of them, resulting in a lower security risk. Check your installed apps regularly.	**Recommendation** • Only install apps you actually need. • Delete any apps you no longer need.

Keep apps up to date

Apps that are no longer up to date can pose a security risk. Check regularly for updates to apps and install them immediately.	**Recommendation** • Always keep your apps up to date. The best way is to set the apps to update automatically.

Grant permissions

Permission is requested when an app is used for the first time, and sometimes for updates. Many apps access personal data. You can block this via your smartphone settings.	**Recommendation** • Only grant permissions (e.g. access to Contacts) if you absolutely need this function. If in doubt, refuse permission. You can always grant permission later via your settings. • Check which access is allowed for each app.

Social media apps

Social media apps (Instagram, Facebook, TikTok, etc.) may be installed on work-related mobile devices. However, social media apps potentially have very wide-ranging permissions and are well known for harvesting a lot of data, such as contact details.	**Recommendation** • Check whether you really need these apps on your work-related mobile device. • Grant as few permissions as possible to the apps. • In addition, please consult the FOPER guidelines on dealing with social media.

Location services

Location services not only impinge on your privacy, they also use additional battery. Some apps cannot run without access to certain functions such as location services. Manage this access manually while using the app. You can find all the apps that request access to your location under Location Services, and you can control access manually.	**Recommendation** • If you do not need an app's location services, you can disable them completely. Open Settings and then select Privacy and Security.  • Often, the option While Using is enough, rather than Always. 

Confidential communications

The Threema Work app is available to employees with managed mobile devices (MDM) for confidential speech-based communications (telephone, voice messages and chats).	**Recommendation** • For sensitive internal discussions and/or chats, use the Threema Work or Skype for Business apps. • For confidential discussions, use only Threema Work. • Do not conduct any work-related discussions via third-party messaging services, except those named above. **Requirement** E027 – Application directive on encrypted voice communication

Meaning of status symbols

Check the status bar on your screen. If you look at the symbols, you can tell at any given moment whether an app is collecting location data or activating a radio interface. If any activities are running without you having consciously activated them, you should investigate by checking which apps are currently active.

Recommendation

Always keep a watch on the status symbols in you iPhone's status bar.

	An app or website is using your location (location services).
	This symbol means that network activity is taking place which is being used by apps, for example.
	Call forwarding is activated.
	An app is using your device's microphone.
	An app is using either your device's camera, or the camera plus microphone.
09:41	The device is either recording sound or taking a screenshot.

If you suspect anything untoward, contact the service desk of your service provider.

Using mobile devices abroad

A special duty of care applies when using app while travelling abroad. In some countries, the border authorities are allowed to inspect apps. To prevent this, you must uninstall the MDM secure apps (secure emails, secure notes, secure tasks) before entering the country in question. If apps are absolutely necessary (e.g. owing to regulation in the relevant country), they should be run on a separate mobile device.	Recommendation • Take only the devices (and information) that you really need when travelling abroad. • Special travel rules apply for exposed persons with diplomatic status. Especially as regards the disclosure of information. Ask your office or VIP support about the relevant requirements and options. • FDFA travel advice: FDFA travel advice page • NCSC website on foreign travel: NCSC – travelling abroad

Replacing your mobile device

When mobile devices are replaced, a lot of data is stored on those devices.	Recommendation • Make sure that your data is deleted when you replace your device.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Finance FDF
National Cyber Security Centre NCSC