Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF
**National Cybersecurity Centre NCSC**

Version 2.0 - February 2022

# Threema user agreement for individuals from outside the Confederation

## 1 Purpose of the user agreement

This agreement regulates the conditions of use for communication with Threema of data classified up to and including CONFIDENTIAL (in accordance with the IPO) and sensitive personal data (in accordance with the FADP) between employees of the Federal Administration and individuals from outside the Confederation (external parties) whose devices are not integrated into the Mobile Device Management system (MDM) of the Federal Administration.

## 2 Basic principles of use

### 2.1 Use of Threema and confidentiality

If there is a need to exchange information with data classified CONFIDENTIAL between employees of the Federal Administration and external parties and if no other authorised means of communication (Secure Messaging or SecureCenter) are available, then Threema can be used for voice and video calls and text messages with external parties, subject to compliance with this user agreement. External parties are obliged to maintain confidentiality with regard to information exchanged via Threema.
In addition, a user agreement MUST always be signed if Threema is used by members of the Federal Administration with individuals from outside the Confederation. The user agreement is also required when employees of the Federal Administration communicate with conscript members of the Armed Forces via Threema.

The intention of the user agreement is to offer a possibility for individuals within the Confederation to exchange information classified CONFIDENTIAL with individuals outside the Confederation and consequently with devices that are not integrated in the federal MDM (e.g. suppliers, conscript members of the Armed Forces, etc.).
No files classified CONFIDENTIAL (in accordance with the IPO) or sensitive personal data (in accordance with the FADP) may be sent via Threema. For this reason, only conversations with or without video and text messages are permitted via Threema.

The Armed Forces are not subject to the Ordinance on the Coordination of the Digital Transformation and ICT (DTIO; SR 172.010.58), hence internal Armed Forces communication among conscript members is excluded from this user agreement. The Armed Forces issue their own regulations in this regard if required.

## 2.2 Operating system and application updates

External parties' smart devices MUST be kept up to date with the latest operating system version. Known insecure applications MUST be removed from the device concerned. Threema updates MUST be installed immediately. If malware is suspected, Threema must not be used. Since malware can reside in the RAM, among other places, it is recommended that the smart devices of both communication partners (internal and external) be switched off completely and restarted before use. This removes the malware.

## 2.3 Secure environment

External parties MUST ensure that a secure environment is maintained when communicating via Threema. Potential risks include, for example, unauthorised individuals in the vicinity, public spaces, hotel rooms, lifts.
To prevent the risk of eavesdropping by unauthorised third parties, conversations concerning data classified CONFIDENTIAL (in accordance with the IPO) and sensitive personal data (in accordance with the FADP) MUST NOT be made in public. When travelling, this applies in particular to airport buildings in Switzerland and abroad, and on public transport (e.g. train, bus, tram, taxi, plane).
If no safe environment is available or if there are security doubts, the conversation should be conducted by text message (chat). When doing so, it should be ensured that the mobile telephone is not visible to others; this includes notifications on the lock screen.

## 2.4 Identifying participants

The parties MUST be able to mutually prove their identity. Threema offers various possibilities for authentication. For data classified INTERNAL (in accordance with the IPO) and personal data (in accordance with the FADP), only the communication partner's Threema ID is required. For conversation content classified CONFIDENTIAL, the following conditions MUST be met:

a. the parties have already mutually authenticated each other (shown by three green dots), i.e. the Threema IDs have been exchanged between the devices by scanning each other's ID.

If, for organisational reasons, a. is not possible, the following points MUST be fulfilled:

b. The parties MUST know each other personally AND
   The parties MUST mutually identify themselves by video call and visual verification, or a common identification sign.

## 2.5 Voice assistants

Voice assistants and input aids such as Siri and Google Assistant MUST be switched off before using Threema; this also applies to peripheral devices such as smartwatches. Conversations with Threema MAY NOT be recorded on the device, all recording functions must be deactivated.

## 2.6 Peripheral devices

For conversations with data classified CONFIDENTIAL (in accordance with the IPO) and sensitive personal data (in accordance with the FADP), external additional devices such as headphones, keyboards, cameras, etc. MAY be used. However, these MUST be connected

via a cable. Push notifications from Threema MAY NOT be displayed on peripheral devices (e.g. smart watches). During communication with data classified CONFIDENTIAL (in accordance with the IPO) and sensitive personal data (in accordance with the FADP), Bluetooth and Wi-Fi MUST be deactivated. Smart Devices MUST NOT be charged at charging stations provided or made available, commercially or otherwise – in particular via third-party USB ports. Only the manufacturer's original charger is to be used.

# 3 Cost and compatibility of the software

All versions of Threema software are fully compatible with each other. This means that users of the version rolled out in the Federal Administration can communicate seamlessly with users of a privately purchased version of Threema.
External parties are responsible for the procurement, updating and costs of their own versions of Threema.

# 4 Compliance with the user agreement

By confirming receipt of this user agreement, the external party declares that he or she has read and understood these conditions for the use of Threema and undertakes to ensure compliance with this user agreement when communicating with employees of the Federal Administration.