Version 2.0 - Février 2022

Convention d'utilisation de Threema avec des personnes externes à l'administration fédérale

1 But de la convention d'utilisation

La présente convention fixe les conditions d'utilisation de Threema pour la communication d' informations jusqu'au niveau de classification «CONFIDENTIEL» (au sens de l'ordonnance concernant la protection des informations, OPrI) compris et de données sensibles (au sens de la loi fédérale sur la protection des données, LPD) entre les collaborateurs de l'administration fédérale et les personnes externes à la Confédération (personnes externes) dont les appareils ne sont pas gérés par le système de gestion des terminaux mobiles (*Mobile Device Management*, MDM) de l'administration fédérale.

2 Principes d'utilisation

2.1 Utilisation de Threema et maintien du secret

S'il est nécessaire d'échanger des informations jusqu'au niveau de classification «CONFIDENTIEL» compris entre des collaborateurs de l'administration fédérale et des personnes externes, et si aucun des autres moyens de communication autorisés (Secure Messaging ou SecureCenter) n'est disponible, l'utilisation de Threema pour passer des appels avec ou sans vidéo et pour échanger messages est autorisée dans le respect de la présente convention d'utilisation. Les personnes externes s'engagent à garder secrètes les informations échangées au moyen de Threema.

Les utilisateurs DOIVENT avoir signé une convention d'utilisation lorsque Threema est utilisé pour la communication entre des collaborateurs de l'administration fédérale et des personnes externes. La signature de la convention d'utilisation est également requise pour la communication entre des collaborateurs de l'administration fédérale et des militaires de milice de l'armée au moyen de Threema.

L'objectif de la convention d'utilisation est de permettre l'échange d'informations classifiées «CONFIDENTIEL» entre des collaborateurs de l'administration fédérale et des personnes externes qui utilisent des appareils non gérés par le système MDM de la Confédération (fournisseurs, militaires, etc.).
Il est interdit d'envoyer des fichiers classifiés «CONFIDENTIEL» (au sens de l'OPrI) ou des données sensibles (au sens de la LPD) via Threema. Par conséquent, seuls les appels avec ou sans vidéo et l'échange de messages sont autorisés.

L'armée n'étant pas soumise à l'ordonnance sur la transformation numérique et l'informatique

(OTNI; RS *172.010.58*), les échanges entre membres de l'armée ne sont pas concernés par la présente convention d'utilisation. L'armée édicte si besoin ses propres directives d'utilisation.

2.2 Mises à jour du système d'exploitation et des applications

Les appareils intelligents des personnes externes DOIVENT disposer de la dernière version du système d'exploitation. Les applications non sécurisées connues DOIVENT être désinstallées de l'appareil en question. Les mises à jour de Threema DOIVENT être installées dès qu'elles sont disponibles. En cas de suspicion d'infection par un logiciel malveillant, l'utilisation de Threema est interdite.
Les logiciels malveillants se logent parfois dans la mémoire temporaire des appareils. C'est pourquoi il est conseillé aux deux interlocuteurs (interne et externe) d'éteindre puis de redémarrer leur appareil avant l'utilisation de Threema. De cette manière, les potentiels maliciels sont supprimés.

2.3 Sécurité de l'environnement

Les personnes externes DOIVENT s'assurer qu'elles utilisent Threema dans un environnement sûr. Les situations et lieux suivants présentent par exemple des risques potentiels: présence de personnes non autorisées à proximité, lieux publics, chambres d'hôtel, ascenseurs. Afin de prévenir le risque que des tiers non autorisés entendent des informations sensibles, il EST INTERDIT de tenir des conversations portant sur des données classifiées «CONFIDENTIEL» (au sens de l'OPrI) ou des données sensibles (au sens de la LPD) dans l'espace public. L'interdiction s'applique notamment pendant tout voyage, entre autres dans les aéroports en Suisse comme à l'étranger et dans les transports publics (train, bus, tram, avion, taxi, etc.).
S'il est impossible de s'isoler dans un environnement sûr ou s'il existe des doutes quant à la sécurité d'un environnement, la communication doit s'effectuer au moyen de messages écrits (chat). Il faut cependant veiller à ce que personne d'autre ne soit en mesure de lire ceux-ci sur l'écran du téléphone mobile et à ce qu'aucun message n'apparaisse sur l'écran de verrouillage.

2.4 Identification des participants à la communication

Les interlocuteurs DOIVENT pouvoir prouver leur identité l'un à l'autre. Threema offre à cet effet plusieurs moyens pour s'authentifier. Pour les informations jusqu'au niveau de classification «INTERNE» (au sens de l'OPrI) et les données personnelles (au sens de la LPD), l'identifiant Threema de l'interlocuteur suffit. Pour les conversations portant sur des informations classifiées «CONFIDENTIEL», les conditions suivantes DOIVENT être respectées:

a. les deux interlocuteurs se sont déjà mutuellement authentifiés (l'application affiche trois points verts), ce qui signifie que les identifiants Threema ont été échangés par le biais d'une numérisation mutuelle du code QR.

Si cette identification mutuelle est impossible pour des raisons organisationnelles, les conditions suivantes DOIVENT être respectées:

b. les interlocuteurs DOIVENT se connaître personnellement ET
   les interlocuteurs DOIVENT être en mesure de se reconnaître mutuellement en activant la vidéo pour une vérification visuelle ou grâce à un signe de reconnaissance commun.

2.5 Assistants vocaux

Les assistants vocaux et les aides à la saisie tels que SIRI ou Google Assistant DOIVENT être éteints avant d'utiliser Threema. Cette règle s'applique également aux appareils périphériques tels que les montres intelligentes. Il EST INTERDIT d'enregistrer les conversations sur l'appareil. Toutes les fonctions d'enregistrement doivent donc être désactivées.

2.6 Appareils périphériques

Il EST AUTORISÉ d'utiliser des appareils externes tels que des écouteurs, un clavier, une caméra, etc. pour les conversations portant sur des informations classifiées «CONFIDENTIEL» (au sens de l'OPrI) et des données sensibles (au sens de la LPD). Ils DOIVENT toutefois être branchés par câble. Il EST INTERDIT de faire s'afficher des messages push de Threema sur des appareils périphériques (par ex. sur des montres intelligentes). Pendant les échanges portant sur des informations classifiées «CONFIDENTIEL» (au sens de l'OPrI) et des données sensibles (au sens de la LPD), les fonctions Bluetooth et Wi-Fi DOIVENT être désactivées. Il EST INTERDIT de charger les appareils à des bornes de recharge publiques ou commerciales, notamment lorsqu'il s'agit de ports USB inconnus. Seule l'utilisation du chargeur fourni par le fabricant est autorisée.

3 Coûts et compatibilité des versions

Les différentes versions du logiciel Threema sont compatibles entre elles. Les utilisateurs de la version employée au sein de l'administration fédérale peuvent donc communiquer avec ceux de la version Threema téléchargée à titre privé.
Les personnes externes sont responsables du téléchargement, de la mise à jour et des coûts de l'installation de Threema.

4 Respect de la convention d'utilisation

En confirmant la réception de cette convention d'utilisation, la personne externe déclare avoir lu et compris les présentes conditions d'utilisation de Threema et s'engage à respecter la convention d'utilisation lors de ses échanges avec des collaborateurs de l'administration fédérale.