Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Le délégué à la transformation numérique et à la gouvernance de l'informatique

E021 – Directive d'application pour la synchronisation des smartphones et des tablettes

Directive concernant l'informatique de la Confédération

Classification[1] :	non classifié
Caractère contraignant[2] :	directive
Type de directive[3] :	(E) directive d'application
Domaine de planification[4] :	prestations informatiques de base pour l'ensemble de l'administration fédérale
Version :	2.2
Remplace la version :	2.1
Statut (présente version) :	approuvé
Date de la décision / date d'entrée en vigueur :	décision : 15 novembre 2022 / entrée en vigueur : 3 janvier 2023
Édictée par / base légale :	le délégué à la transformation numérique et à la gouvernance de l'informatique (délégué TNI) en vertu de l'art. 17, al. 1, let. e, de l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI, RS 172.010.58)
Langues :	allemand (original), français (traduction) et anglais (traduction)
Annexe :	aucune

[1] À propos des échelons de classification INTERNE et CONFIDENTIEL, voir l'*ordonnance du 4 juillet 2007 concernant la protection des informations de la Confédération (ordonnance concernant la protection des informations, OPrI) (état le 1er janvier 2021)*, RS 510.411

[2] Concernant la forme de l'acte et le caractère contraignant, voir *Office fédéral de la justice, Guide de législation, 4e édition mise à jour, 2019*

[3] Conformément à la plate-forme d'information TNI de la ChF

[4] Domaines de planification selon la *Stratégie informatique de la Confédération 2020-2023 du 3 avril 2020 (SB000)*

Table des matières

1 Dispositions générales

1.1 Objet

Les appareils mobiles des collaborateurs de l'administration fédérale doivent être configurés, gérés et exploités conformément aux prescriptions organisationnelles et techniques de la Confédération. Un *système de gestion de la sécurité et des appareils* est nécessaire pour la mise en œuvre de cette stratégie. La présente *directive d'application pour la synchronisation des smartphones et des tablettes [E021]* réglemente l'utilisation des applications informatiques de la Confédération sur des *appareils intelligents* à partir de réseaux externes grâce à un système d'accès sécurisé au moyen de l'application *Secure Hub* (solution Sandbox).

1.2 Garantie de la protection des données

[1] La protection des données continue d'être garantie à tout moment. L'exploitant du système MDM (système de gestion des terminaux mobiles) ne peut ni consulter les données professionnelles ni les données privées de l'utilisateur.

[2] Les données recueillies dans le cadre de la gestion des appareils intelligents ont été annoncées au *préposé fédéral à la protection des données et à la transparence (PFPDT)*.

1.3 Champ d'application

[1] La présente directive s'adresse à tous les collaborateurs de l'administration fédérale qui accèdent aux ressources informatiques de cette dernière depuis des appareils intelligents fédéraux ou privés.

[2] Le champ d'application de la présente directive est identique à celui qui est défini à l'*art. 2* de l'*ordonnance sur la transformation numérique et l'informatique (OTNI)*.

[3] Le degré du caractère contraignant[5] des dispositions du chapitre 2 de la présente directive est indiqué au moyen des mots-clés définis à l'annexe B.

1.4 Définitions

[1] Dans la présente directive, on entend par :

a. *appareil intelligent :* tout appareil contrôlé et homologué par l'administration fédérale, par exemple un smartphone ou une tablette ;

b. *synchronisation des données :* la communication cryptée entre un appareil intelligent et une zone du réseau de la Confédération au moyen d'un accès sans fil *(over the air,* OTA*)* ;

[5] Degrés du caractère contraignant selon *Request for Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* L'indication des degrés du caractère contraignant selon [RFC 2119] est une pratique répandue dans la normalisation internationale.

c. *MDM (Mobile Device Management ou gestion des terminaux mobiles) : la* gestion centralisée – par la Confédération – des appareils intelligents fédéraux ou privés à l'aide de la solution Sandbox ;

d. *solution Sandbox :* une application (logiciel) pour la synchronisation des données professionnelles à l'aide d'applications comme *Secure Mail*, *Secure Tasks* et *Secure Notes* ;

e. *nuage public :* une offre en libre accès d'un fournisseur privé qui laisse ses services en ligne ouverts à tout le monde, comme *iCloud*, *Google One* et *OneDrive* ;

f. *OTA-Sync :* l'application de la Confédération qui sert à synchroniser les données professionnelles avec les applications natives du fabricant, comme la messagerie et le calendrier ;

g. *effacement partiel :* la suppression des données professionnelles et des applications internes à la solution Sandbox ; les réglages, les données et les applications en dehors de la solution Sandbox sont conservés ;

h. *effacement total :* la suppression intégrale des données de l'appareil intelligent (y compris les applications et les courriers électroniques) ; l'appareil est réinitialisé ;

i. *authentification biométrique :* une procédure d'authentification autre que la saisie d'un NIP (par ex. *Touch ID* ou *Face ID*) ;

j. *débridage* : la suppression non autorisée des restrictions d'utilisation fixées par le fabricant ;

k. *maliciel :* tout programme ou logiciel malveillant.

2 Directive d'application pour les appareils intelligents utilisés à titre professionnel

2.1 Code de l'appareil, NIP *Secure Hub* et mots de passe

[1] Un code à 6 chiffres DOIT être utilisé pour l'appareil intelligent.

[2] Un NIP *Secure Hub* à 6 chiffres DOIT être utilisé pour la solution Sandbox.

[3] Une authentification biométrique PEUT remplacer le code de l'appareil ou le NIP *Secure Hub*.

[4] Un effacement total DOIT être effectué sur un appareil de la Confédération lorsque son code a été saisi de façon erronée à huit reprises.

[5] Un nouveau NIP *Secure Hub* DOIT être généré lorsque le NIP *Secure Hub* initial a été saisi de façon erronée à huit reprises.

[6] Si l'appareil intelligent n'est pas utilisé pendant plus de trois minutes, l'utilisateur DOIT saisir à nouveau le code de l'appareil.

[7] La gestion des mots de passe PEUT se faire au moyen d'une application installée sur l'appareil intelligent. Un mot de passe maître à la fois autonome et complexe DOIT être utilisé pour l'authentification. Il EST INTERDIT de synchroniser le mot de passe maître avec d'autres appareils.

2.2 Données professionnelles

[1] Il EST INTERDIT d'établir, de lire ou de traiter des informations classifiées CONFIDENTIEL[6] ou SECRET ainsi que des données sensibles ou des profils de la personnalité sur les appareils intelligents.

[2] Pour le traitement et l'enregistrement de données professionnelles des applications de l'*App Store* de la Confédération et de l'*App Store* du fabricant (concerne les développements propres), il est de la responsabilité du mandant ou de l'unité administrative (UA) compétente d'édicter ou de mettre en œuvre les directives de sécurité qui s'imposent. L'utilisateur EST AUTORISÉ à prendre des photos professionnelles avec l'application prévue à cet effet, mais ces photos DOIVENT ensuite être copiées dans la Sandbox et effacées partout ailleurs. Le transfert par câble sur le poste de travail de la Confédération de grandes quantités de données, comme des vidéos, EST AUTORISÉ.

[3] Il EST INTERDIT de sauvegarder des données professionnelles en dehors de l'appareil intelligent (par ex. sur Internet et sur des services en nuage externes). Font exception les services de sauvegarde du fabricant pour les sauvegardes cryptées de données[7].

[4] Il EST AUTORISÉ de lire et de traiter en dehors de la Sandbox des données professionnelles que l'administration fédérale a mises à la disposition des utilisateurs autorisés sur Internet, comme des applications spécialisées de cyberadministration ou la *Collaboration Extranet*.

2.3 Modifications interdites

[1] Les manipulations de *logiciels d'exploitation et de sécurité* (par ex. débridage) SONT INTERDITES sur les appareils intelligents utilisés à des fins professionnelles.

[2] Lorsque des manipulations se révèlent non conformes aux exigences de l'administration fédérale, le fournisseur de prestations (FP) PEUT désactiver la synchronisation. Si une manipulation est détectée, la synchronisation est immédiatement et automatiquement bloquée, puis interrompue.

2.4 Mise à jour de logiciels

[1] La version du système d'exploitation installée sur l'appareil intelligent DOIT être conforme à celle prescrite par le FP.

[2] La mise à jour logicielle du système d'exploitation DOIT être effectuée après réception de la notification ou de l'autorisation du FP.

[3] Les mises à jour de logiciels DOIVENT être installées par liaison sans fil (OTA).

[4] Si une version non autorisée du système d'exploitation (ancienne ou nouvelle) est utilisée, le FP PEUT bloquer la synchronisation à tout moment.

---

[6] À propos des échelons de classification INTERNE et CONFIDENTIEL, voir la section 2 de l'*ordonnance du 4 juillet 2007 concernant la protection des informations de la Confédération*, RS 510.411

[7] Le programme CEBA permet de mettre en place une offre Microsoft365 (M365) pour les utilisateurs de l'administration fédérale. Les différentes applications M365 pour l'appareil intelligent peuvent être utilisées dans le cadre de l'utilisation du programme CEBA.

2.5 Applications mobiles

[1] Les applications DOIVENT être installées en passant par l'*App Store* de la Confédération ou par l'*App Store* du fournisseur correspondant.

[2] Les différentes applications PEUVENT être bloquées ou interdites par le FP pour des raisons de sécurité.

2.6 Synchronisation locale et sauvegarde

[1] Il EST INTERDIT d'installer des logiciels de synchronisation (par ex. *iTunes*) sur les ordinateurs de l'administration fédérale.

[2] Les appareils intelligents qui synchronisent des données professionnelles avec la solution Sandbox PEUVENT synchroniser des données ou effectuer une sauvegarde de données avec un ordinateur privé.

2.7 Perte ou vol d'un appareil intelligent

[1] En cas de perte ou de vol d'un appareil intelligent, le *Service Desk* compétent DOIT en être informé sans délai. Il doit également être informé si l'appareil est retrouvé.

[2] Après réception de l'information, le *Service Desk* compétent DOIT procéder à un effacement partiel sur les appareils privés et à un effacement total sur les appareils de la Confédération.

2.8 Réparation

[1] La réparation des appareils de la Confédération DOIT se faire conformément au processus de réparation ordinaire. Pour cela, l'utilisateur DOIT prendre contact avec le *Service Desk*. Il DOIT procéder, sur le portail en libre-service MDM, à un effacement total des données de son appareil intelligent avant d'envoyer ce dernier en réparation. Si cela n'est plus possible, il peut, à titre exceptionnel, réinitialiser manuellement l'appareil. Si un effacement total n'est possible ni sur le portail en libre-service ni au moyen d'une réinitialisation manuelle, l'appareil DOIT être détruit (par ex. en suivant le processus d'élimination de l'OFIT).

[2] Dans le cas d'un appareil privé, l'utilisateur DOIT, avant la réparation, faire procéder à un effacement partiel des données en passant par le portail en libre-service MDM ou par le *Service Desk*. Il DOIT se charger de la réparation ou de l'élimination.

[3] Avant la réparation, l'utilisateur DOIT désactiver la fonction « *Localiser mon iPhone/iPad* » (*find my iPphone*) sur les appareils iOS.

2.9 Résiliation des rapports de service

[1] Si l'utilisateur est licencié ou s'il démissionne, il DOIT en informer le responsable de l'intégration compétent. Ce dernier se charge de faire effacer les données de l'appareil intelligent. Les appareils de la Confédération DOIVENT être soumis à un effacement total ou partiel, alors que les appareils privés DOIVENT être soumis à un effacement partiel.

[2] Avant la restitution de l'appareil, l'utilisateur DOIT désactiver la fonction « *Localiser mon iPhone/iPad* » (*find my iPhone*) sur les appareils iOS.

2.10 Infection par un maliciel

[1] En cas de soupçon de manipulation ou d'infection par un maliciel, le *Service Desk* DOIT en être informé sans délai.

3 Dispositions finales

3.1 Mise en œuvre

[1] En vertu de l’*art. 3 OTNI*, les départements et la Chancellerie fédérale sont responsables de la mise en œuvre de la présente directive dans leurs domaines de compétences respectifs.

3.2 Vérification

[1] Le secteur Transformation numérique et gouvernance de l’informatique (secteur TNI) de la ChF vérifie l’actualité et l’adéquation de la présente directive au plus tard quatre ans après son entrée en vigueur.

3.3 Entrée en vigueur

[1] La présente directive entre en vigueur le 3 janvier 2023.

Annexes

A. Modifications par rapport à la version précédente

- Toutes les formulations faisant référence à l'UPIC ont été modifiées pour qu'elles soient conformes à l'*OTNI*.

- Les dispositions régissant la synchronisation des données professionnelles ont été précisées, et des dispositions concernant aussi bien l'authentification biométrique que l'utilisation d'applications de gestion des mots de passe ont été ajoutées.

B. Signification des mots-clés indiquant le degré du caractère contraignant des dispositions

Le degré du caractère contraignant[8] des différentes dispositions du chapitre 2 de la présente directive est indiqué par les mots clés suivants écrits en majuscules :

Mot-clé	**Degré du caractère contraignant**
DOIT	La directive doit impérativement être respectée (sauf dérogation).
EST INTERDIT	L'option ne peut pas être sélectionnée.
EST AUTORISÉ	L'option est autorisée explicitement. L'UA décide si elle veut y recourir. Si la directive concerne une solution informatique, le fournisseur de la solution doit proposer cette option.
DOIT EN PRINCIPE	En règle générale, l'option doit être sélectionnée. Une UA peut toutefois s'écarter de cette directive sans qu'une dérogation accordée par le secteur TNI ou par le Centre national pour la cybersécurité soit nécessaire, si cette option ne permet plus de garantir la rentabilité ou la sécurité. Une justification écrite est cependant requise.
PEUT	L'option est admise. Si la directive concerne une solution informatique, le fournisseur de cette dernière décide s'il veut proposer cette option.

C. Références

ID	**Référence[9]**

[8] Degrés du caractère contraignant selon *Request for Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* L'indication des degrés du caractère contraignant selon [RFC 2119] est une pratique répandue dans la normalisation internationale.

[9] Les actes législatifs de niveau fédéral sont référencés d'après le Recueil systématique. Pour les directives de la Confédération qui sont référencées, c'est la version en vigueur à la date de la décision portant sur la présente directive qui est indiquée.

SD100	SD100 – Catalogue des services standard (version 2020)
OTNI	ordonnance du 25 novembre 2020 sur la coordination de la transformation numérique et la gouvernance de l'informatique dans l'administration fédérale (ordonnance sur la transformation numérique et l'informatique [OTNI]), RS 172.010.58

D. Abréviations

Sigle	***Signification***
ChF	Chancellerie fédérale
FP	fournisseur de prestations
MDM	gestion des terminaux mobiles (*Mobile Device Management*)
NIP	numéro d'identification personnel (code NIP)
OFIT	Office fédéral de l'informatique et de la télécommunication
OTA	accès sans fil (*over the air*)
secteur TNI	secteur Transformation numérique et gouvernance de l'informatique de la ChF
UA	unité administrative
UPIC	Unité de pilotage informatique de la Confédération