E031 – Directive d'application relative à Microsoft 365

Directive concernant l'informatique de la Confédération

Classification[1]	Aucune
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
Version précédente	2.1
Statut	Approuvé
Date de la décision / date de l'entrée en vigueur	Décision relative à la gouvernance de l'informatique : 16 juin 2025 Entrée en vigueur : 16 juin 2025
Édictée par / base légale	Le délégué à la transformation numérique et à la gouvernance de l'informatique (délégué TNI) en vertu de l'art. 40 de l'ordonnance du 2 avril 2025 sur les services numériques et la transformation numérique dans l'administration fédérale (ordonnance sur la numérisation, ONum), RS 172.019.1
Langues	Allemand (original) et français (traduction)

[1] En ce qui concerne les classifications INTERNE et CONFIDENTIEL, voir *l'art. 13 de la loi du 18 décembre 2020 sur la sécurité de l'information (RS 128)*

[2] À propos de la forme de l'acte et du caractère contraignant, voir *Office fédéral de la justice, Guide de législation, 4e édition 2019 (état 2023)*

[3] Voir la plate-forme d'information TNI

[4] Domaines de planification figurant dans la *stratégie Administration fédérale numérique du 12 décembre 2023 (SB000)*

Table des matières

1 Dispositions générales 3

1.1 Objet 3
1.2 Champ d'application 3
1.3 Définitions 3

2 Directive d'application relative à Microsoft 365 5

2.1 Responsabilités 5
2.2 Traitement des données 5
2.3 Conditions générales d'utilisation 6

3 Dispositions finales 7

3.1 Mise en œuvre 7
3.2 Vérification 7
3.3 Entrée en vigueur 7

Annexes 8

A. Utilisation des *services M365* 8
B. Vue d'ensemble de la terminologie 11
C. Modifications par rapport à la version précédente 12
D. Signification des mots-clés pour le degré du caractère contraignant 12
E. Références 12
F. Abréviations 13

1 Dispositions générales

1.1 Objet

[1] La présente directive régit l'utilisation de la *plateforme Microsoft 365* en tant que partie intégrante du service standard Bureautique (SS Bureautique).

[2] Les fournisseurs de prestations et les bénéficiaires de prestations (c'est-à-dire les utilisateurs) doivent respecter la présente directive afin de pouvoir utiliser les services Microsoft 365 et les services sur lesquels ils reposent ou qui les étendent[5]. Le respect de la présente directive garantit l'utilisation légale de la plate-forme M365 et la protection des données de l'administration fédérale.

[3] La présente directive régit les principes de traitement des données sur la *plateforme Microsoft 365*. Elle complète les directives existantes de la Confédération et des départements ainsi que des prescriptions supplémentaires des unités administratives concernant l'utilisation de l'informatique. Sa mise en œuvre dépend de la participation et de la responsabilité individuelle de tous les collaborateurs de l'administration fédérale.

1.2 Champ d'application

[1] **Directive du secteur Transformation numérique et gouvernance de l'informatique (secteur TNI)**

basée sur l'art. 40 de l'ordonnance du 2 avril 2025 sur les services numériques et la transformation numérique dans l'administration fédérale (ordonnance sur la numérisation, ONum), RS 172.019.1

[2] La présente directive est contraignante pour les utilisateurs des *services M365* du SS Bureautique.

[3] Le degré du caractère contraignant[6] des dispositions du chap. 2 de la présente directive est indiqué au moyen des mots-clés définis à l'annexe D.

1.3 Définitions

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

a. *plateforme Microsoft 365 :* les services en nuage public de Microsoft 365 fournis par le SS Bureautique ; la plateforme est intégrée à l'environnement de bureautique de l'administration fédérale, en faisant ainsi partie ;

b. *Microsoft 365 (M365) :* un ensemble d'applications et de fonctionnalités en nuage public pour la bureautique, comme Teams, SharePoint Online et OneDrive for Business, des instruments de gestion et de sécurité ainsi que les *Microsoft 365 Apps for Enterprise*, installées localement sur le poste de travail ;

c. *portefeuille M365 de la Confédération :* le portefeuille qui définit les services en nuage public Microsoft 365 validés par le SS Bureautique ;

---

[5] Par ex. centre d'appel, poste d'opérateur téléphonique, appel téléphonique de groupe et Teams Apps

[6] 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.

d. *services M365 :* les services utilisés conformément au *portefeuille M365 de la Confédération* ;
il s'agit notamment des services suivants :

   1) *Microsoft 365 Apps for Enterprise (ou M365 Apps) :* applications bureautiques installées localement sur le poste de travail (Teams, Outlook, Word, Excel, PowerPoint, OneNote, Access, etc.) ;

   2) *Microsoft 365 :* applications bureautiques en nuage qui peuvent être utilisées avec un navigateur, telles que Teams, Outlook Web Access, Word Online, Excel Online et PowerPoint Online ;

   3) *Exchange Online :* solution utilisée pour les services liés aux courriers électroniques ; cette solution permet d'accéder aux courriers électroniques, au calendrier, aux contacts et aux tâches ;

   4) *Teams :* application de collaboration en nuage ; elle intègre dans un espace de travail centralisé le chat individuel, le chat en groupe, la vidéoconférence, l'audioconférence, le partage de documents et de calendriers ainsi que le statut de joignabilité des collaborateurs ;

   5) *SharePoint Online :* plateforme de collaboration en nuage ; elle permet à l'administration fédérale de partager le stockage, l'utilisation et la gestion de contenus et d'applications ;

   6) *OneDrive for Business :* service de stockage personnel en nuage pour les données personnelles et privées conformément à la définition figurant dans la directive d'application [E026] ; les données professionnelles devraient, dans toute la mesure du possible, être conservées dans les espaces de stockage partagés ou dans les systèmes prévus à cet effet ;

   7) *Viva Engage (anciennement Yammer) :* réseau social utilisé dans le contexte de l'entreprise ; grâce à l'orientation professionnelle, le partage et l'édition de documents, l'échange de connaissances ainsi que la collaboration et la communication au sein de l'entreprise et entre les entreprises sont mis au premier plan ; au sein de la Confédération, ce réseau social est surtout utilisé pour les « communautés de pratique » ;

e. *Account Modern :* compte d'utilisateur selon le catalogue de services standard, qui est géré dans l'On-Premises Active Directory et répliqué dans l'Azure Active Directory ; les services M365 ne sont disponibles qu'avec l'*Account Modern* ;

f. *système de poste de travail ou poste de travail :* service composé du service « Poste de travail » [SD105] et du service « Bureau virtuel » [SD119], qui est proposé dans le SS Bureautique conformément au catalogue des services standard [SD100] ; le système de poste de travail est intégré dans les environnements de bureautique de la Confédération et permet d'accéder aux applications spécialisées de cette dernière.

[2] Une vue d'ensemble de la terminologie et du champ d'application est présentée sous forme graphique à l'annexe B.

2 Directive d'application relative à Microsoft 365

2.1 Responsabilités

[1] Le SS Bureautique fournit, de concert avec les fournisseurs de prestations définis, les prestations informatiques de base standardisées et centralisées du poste de travail conformément au catalogue des services standard [SD100].

[2]Il assure la fourniture des *services M365* et garantit la protection informatique de base [Si001].

[3] Les départements et les unités administratives (bénéficiaires de prestations) connaissent les données et les processus opérationnels qu'ils souhaitent traiter avec M365. Ils se sont familiarisés avec les prescriptions en vigueur dans leur domaine. Ils DOIVENT donc déterminer sous leur propre responsabilité le niveau de protection requis pour les données. Ils vérifient si les mesures de protection informatique de base sont suffisantes pour les données dont ils sont responsables. Ils doivent notamment s'assurer qu'aucune donnée non autorisée au sens du chap. 2.2, al. 1, n'est traitée avec M365.

[4] Les documents traités DOIVENT être classés ou munis d'un label correspondant par les utilisateurs ou par des processus automatisés en fonction de leur classification en vertu de la loi sur la sécurité de l'information [LSI] et de la loi fédérale sur la protection des données [LPD].

[5] Les départements et les unités administratives (bénéficiaires de prestations) définissent au besoin des prescriptions et des mesures plus poussées pour leur domaine de responsabilité.

[6]Le SS Bureautique aide les départements et les unités administratives, notamment avec des outils informatiques, des moyens auxiliaires et des offres de formation, pour qu'ils puissent assumer les responsabilités visées à l'al. 3.

[7]Il EST PERMIS de proposer une collaboration aux utilisateurs externes (invités). Dans ce cas, il DOIT s'agir d'un contexte professionnel, et la personne invitante (collaborateur de l'administration fédérale) DOIT s'assurer de l'identité de la personne. Les droits d'accès attribués à la faveur de l'invitation DOIVENT être vérifiés tous les trimestres par la personne invitante et, le cas échéant, retirés à l'utilisateur externe s'ils ne sont plus nécessaires.

2.2 Traitement des données

[1] Avec M365, il EST PERMIS de traiter des informations non classifiées au sens de l'ordonnance sur la sécurité de l'information [OSI] et des données personnelles au sens de la loi fédérale sur la protection des données [LPD].

Le recours aux services M365 est expressément interdit pour les informations qui sont munies d'une classification supérieure au sens de l'OSI ainsi que pour les données personnelles sensibles et les profilages au sens de la LPD, à quelques exceptions près[7]. Ces données doivent être ouvertes et traitées avec la version d'Office installée localement et les outils validés à cet effet[8]. Elles doivent être enregistrées sur les services validés pour

[7] À titre d'exception, MS-Teams peut être utilisé moyennant le recours au chiffrement de bout en bout pour les données personnelles sensibles au sens de la LPD et les informations classifiées INTERNE au sens de l'OSI.

[8] Actuellement, il s'agit notamment des outils de chiffrement SecureCenter et de son successeur CHCrypt.

l'unité administrative concernée, par exemple sur GEVER ou sur des applications spécialisées.

L'utilisation des différents services M365 qui est autorisée actuellement figure à l'annexe A.

[2] Pour autant qu'aucun règlement de traitement des données ou qu'aucune prescription de l'unité administrative considérée ne l'interdise, il EST PERMIS de traiter avec les services M365 les informations couvertes par le secret de fonction[9].

[3] Les départements et/ou les unités administratives DOIVENT EN PRINCIPE fournir à leurs collaborateurs une aide pour la classification des informations ainsi que pour la classification selon la LPD. Comme il n'y a que les unités administratives qui connaissent leurs affaires et leurs contenus, elles ONT LE DROIT de définir des règles organisationnelles spécifiques pour l'utilisation de M365.

[4] Les *services M365* DOIVENT EN PRINCIPE être utilisés à des fins professionnelles conformément à la directive d'application sur le système de poste de travail [E026].

[5] Les utilisateurs ONT LE DROIT de traiter temporairement des informations importantes pour les affaires avec les services M365. Une fois les travaux terminés, ces informations DOIVENT être replacées dans le système de gestion des affaires GEVER correspondant ou dans l'application spécialisée de l'unité administrative[10].

[6] Pour les conversations avec Microsoft Teams qui contiennent des données personnelles sensibles ou des informations classifiées INTERNE ainsi que pour l'enregistrement des communications vocales et/ou vidéo, il FAUT tenir compte de la directive d'application [E017].

[7] Pour chaque conversation sur *Viva Engage*, au moins un modérateur chargé d'intervenir dans les discussions en cas de besoin (par ex. insultes, racisme et discrimination) DOIT être désigné.

[8] Lors des conversations avec Teams, il EST PERMIS d'effectuer des transcriptions. Les participants à la réunion DOIVENT être informés de cela et de la suite du traitement de la transcription. En cas de communication chiffrée avec Teams, la transcription n'est techniquement pas possible.

2.3 Conditions générales d'utilisation

[1] Les services M365 sont exploités en Suisse chaque fois que cela est proposé par Microsoft, et les données sont conservées sur le territoire suisse. Dans les cas où cela n'est pas possible, les services sont exploités dans l'Union européenne (limite de données de l'UE [EU Data Boundary])[11].

---

[9] Conformément aux explications fournies dans l'analyse des bases légales concernant Microsoft 365, le traitement de données couvertes par le secret de fonction est autorisé sur la base des contrats conclus avec Microsoft et de la modification législative apportée à l'art. 320 CP (renvoi : Projet CEBA ->Bases légales).

Le document intitulé « Exigences liées aux risques de violation du secret de fonction dans l'administration fédérale » [Si001-Hi03] décrit les recommandations visant à prévenir les violations du secret de fonction, qui peuvent éventuellement être pertinentes dans le cadre de la transmission de données à des tiers lors d'opérations d'assistance. En cas de doute, il est judicieux de faire appel au service juridique de l'unité administrative pour l'évaluation.

[10] Art. 4 de l'ordonnance sur la gestion électronique des affaires dans l'administration fédérale (Ordonnance GEVER, RS 172.010.441)

[11] Informations sur l'endroit où Microsoft 365 stocke les données des clients : https://learn.microsoft.com/fr-fr/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide

[2] Du point de vue du droit des marchés publics ou en raison de préoccupations liées à la sécurité, certains services M365 ne sont pas disponibles. L'étendue des fonctionnalités disponibles est définie dans le *portefeuille M365 de la Confédération*.

[3] Pour l'utilisation des *services M365*, l'unité administrative concernée commande la prestation de marché « Account Modern » conformément au catalogue des services standard.

[4] Les appareils intelligents qui sont exploités via la gestion des appareils mobiles (Mobile Devices Management, MDM) des fournisseurs de services ONT LE DROIT d'utiliser les services M365 sans restriction.
Tous les autres appareils privés ou tiers ONT LE DROIT d'utiliser les services M365 uniquement via le traitement en ligne (Office Online) au moyen d'un navigateur[12].

[5] L'accès intégral aux services M365 (connexion) DOIT se faire par les moyens d'authentification validés (par ex. carte à puce ou autres authentifications à plusieurs facteurs)[13].

[6] Lors de leur première connexion à la *plateforme M365*, les utilisateurs DOIVENT confirmer qu'ils ont pris acte de la présente directive d'application et qu'ils l'observent.

3 Dispositions finales

3.1 Mise en œuvre

[1] En vertu de l'ONum, les départements et la ChF sont responsables de la mise en œuvre de la présente directive dans leurs domaines de compétence respectifs.

3.2 Vérification

[1] Le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI) 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 16 juin 2025.

[2] La version 1.1 reste applicable à la plateforme CEBA Agile jusqu'à la mise hors service de cette dernière.

[12] Voir également le tableau 2 de l'annexe A. Cette mesure est aussi mise en œuvre sur le plan technique par le fournisseur de prestations.

[13] Cette mesure est aussi mise en œuvre sur le plan technique par le fournisseur de prestations.

Annexes

A. Utilisation des *services M365*

Les tableaux ci-dessous indiquent les possibilités d'utilisation des principaux ***services M365*** concernant les aspects liés à l'information et à la protection des données.
Les prescriptions et la restriction applicables à la classification INTERNE selon l'OSI seront réexaminées une fois que les prescriptions de traitement du SE-POS seront disponibles.

vert : autorisé sans restriction jaune : autorisé avec restrictions rouge : non autorisé

Classification LPD	**Classification OSI**	**Applications Office locales (installées sur le SPT)**	**M365 Online (version Office pour le web)**	**Teams**	**SharePoint Online**	**OneDrive for Business**	**Viva Engage**	**Tous les autres** (par ex. Planner et To Do List)
Données personnelles	**Non classifié**	Sans restriction	Sans restriction sur les terminaux gérés (SPT) Uniquement traitement en ligne sur des terminaux non gérés (par ex. PC privé)	Sans restriction	Sans restriction	Sans restriction	Sans restriction	Sans restriction
Données personnelles sensibles				Moyennant le recours au chiffrement de bout en bout (informations complémentaires dans la directive **E017**), des données personnelles sensibles peuvent être échangées pendant la communication vocale et/ou vidéo. Une transcription n'est pas possible. Les échanges par **chat** ne sont pas autorisés.				
	INTERNE	Le traitement sur un SPT est possible sans restriction. Les informations doivent toutefois être stockées dans des systèmes locaux comme GEVER ou dans un espace de stockage ou une application validés par l'unité administrative. Le stockage dans M365 n'est pas autorisé.	Aucun traitement autorisé	Moyennant le recours au chiffrement de bout en bout (informations complémentaires dans la directive **E017**), des informations classifiées INTERNE peuvent être échangées pendant la communication vocale et/ou vidéo. Une transcription n'est pas possible. Les échanges par **chat** ne sont pas autorisés.	Aucun traitement ni stockage autorisés	Aucun stockage autorisé	Aucun traitement ni stockage autorisés	Aucun traitement ni stockage autorisés
Données personnelles sensibles et profilages	**CONFIDENTIEL**	Les documents doivent être protégés par un chiffrement validé[14]. Traitement uniquement dans la zone sécurisée locale de l'environnement de chiffrement Stockage dans GEVER ou dans un espace de stockage ou une application validés par l'unité administrative	Aucun traitement autorisé	Aucun traitement, aucun stockage et aucune communication chat/audio/vidéo autorisés	Aucun traitement ni stockage autorisés	Aucun stockage autorisé	Aucun traitement ni stockage autorisés	Aucun traitement ni stockage autorisés
	SECRET	Non autorisé	Non autorisé	Non autorisé	Non autorisé	Non autorisé	Non autorisé	Non autorisé

[14] Un chiffrement validé est par exemple Secure Center ou CHCrypt.

Tableau 1 : Possibilités d'utilisation des services M365

Possibilités d'utilisation des services M365 sur les terminaux des différentes catégories

Le tableau ci-dessous présente les possibilités d'utilisation concernant les différentes catégories de terminaux. Les services M365 peuvent être utilisés sans restriction sur les terminaux gérés par la Confédération en ce qui concerne les données personnelles et les informations non classifiées. L'accès à M365 depuis des appareils tiers est possible soit via le service VDI mobile, soit via un navigateur (seuls les outils en ligne peuvent être utilisés). L'accès se fait avec le compte de la Confédération et une authentification à plusieurs facteurs qui a été validée. Les opérations qui concernent les données ayant une classification plus élevée font généralement l'objet de restrictions ou ne sont pas autorisées.

		Terminal		
Classification selon LPD	**Classification selon OSI**	**SPT entièrement géré** (client BA) avec l'application Office installée localement et avec OneDrive for Business (y compris VDI mobile)	Terminal **partiellement géré** avec la MDM de la Confédération, comme Smartdevice, avec applications Office Mobile et OneDrive for Business installées localement	**Appareil tiers non géré** (par ex. PC privé, BYOD, smartphone privé sans MDM)
Données personnelles	**Non classifié**	**Utilisable sans restriction**	**Utilisable sans restriction**	Seul le traitement en ligne sur M365 via un navigateur est possible (M365 Office Online) (avec compte de la Confédération et authentification à plusieurs facteurs) Exception : VDI mobile : utilisable sans restriction
Données personnelles sensibles	**Non classifié**	Effectuer des communications vocales et/ou vidéo en utilisant le chiffrement de bout en bout (renvoi à la directive E017) Les échanges par chat ne sont pas autorisés pour les données personnelles sensibles.	Effectuer des communications vocales et/ou vidéo en utilisant le chiffrement de bout en bout (renvoi à la directive E017). Une transcription n'est pas possible. Les échanges par chat ne sont pas autorisés pour les données personnelles sensibles.	Effectuer des communications vocales et/ou vidéo en utilisant le chiffrement de bout en bout (renvoi à l'E017) Les échanges par chat ne sont pas autorisés pour les données personnelles sensibles.
	INTERNE	Le traitement sur un SPT est possible sans restriction. Les informations doivent toutefois être stockées dans des systèmes locaux comme GEVER ou dans un espace de stockage ou une application validés par l'unité administrative. Le stockage dans M365 ou OneDrive for Business n'est pas autorisé.	Effectuer des communications vocales et/ou vidéo en utilisant le chiffrement de bout en bout (renvoi à la directive E017). Une transcription n'est pas possible, et les échanges par chat ne sont pas autorisés. Le traitement sur un smartphone intégré dans la MDM est possible sans restriction. Les informations doivent toutefois être stockées dans des systèmes locaux comme GEVER ou dans un espace de stockage ou une application validés par l'unité administrative. Le stockage dans M365 ou OneDrive for Business n'est pas autorisé.	Aucun traitement, aucun stockage et aucune communication chat/audio/vidéo avec Teams ne sont autorisés. Exception : le traitement sur VDI mobile est possible sans restriction. Les informations doivent toutefois être stockées dans des systèmes locaux comme GEVER ou dans un espace de stockage ou une application validés par l'unité administrative. Le stockage dans M365 ou OneDrive for Business n'est pas autorisé.
Données personnelles sensibles et profilages	**CONFIDENTIEL**	Les documents doivent être protégés par un chiffrement validé.	Aucun traitement, aucun stockage et aucune communication chat/audio/vidéo avec Teams ne sont autorisés.	Aucun traitement, aucun stockage et aucune communication chat/audio/vidéo avec Teams ne sont autorisés. (il n'y a pas d'intégration avec l'outil de chiffrement)

		Traitement uniquement dans la zone sécurisée locale de l’environnement de chiffrement. Stockage dans GEVER ou dans un espace de stockage ou une application validés par l’unité administrative Les communications audio/vidéo/chat avec Teams ne sont pas autorisées.	(il n’y a pas d’intégration avec l’outil de chiffrement)	

Tableau 2 : Illustration de l’utilisation des services M365 concernant les terminaux

B. Vue d'ensemble de la terminologie

La directive d'application E031 se rapporte à l'utilisation de la plateforme Microsoft 365 matérialisée par le rectangle de couleur figurant dans l'illustration ci-dessous. Il s'agit d'une délimitation schématique entre la plateforme Microsoft 365 et les services bureautiques existants de l'administration fédérale. Le graphique illustre les liens entre les termes utilisés.

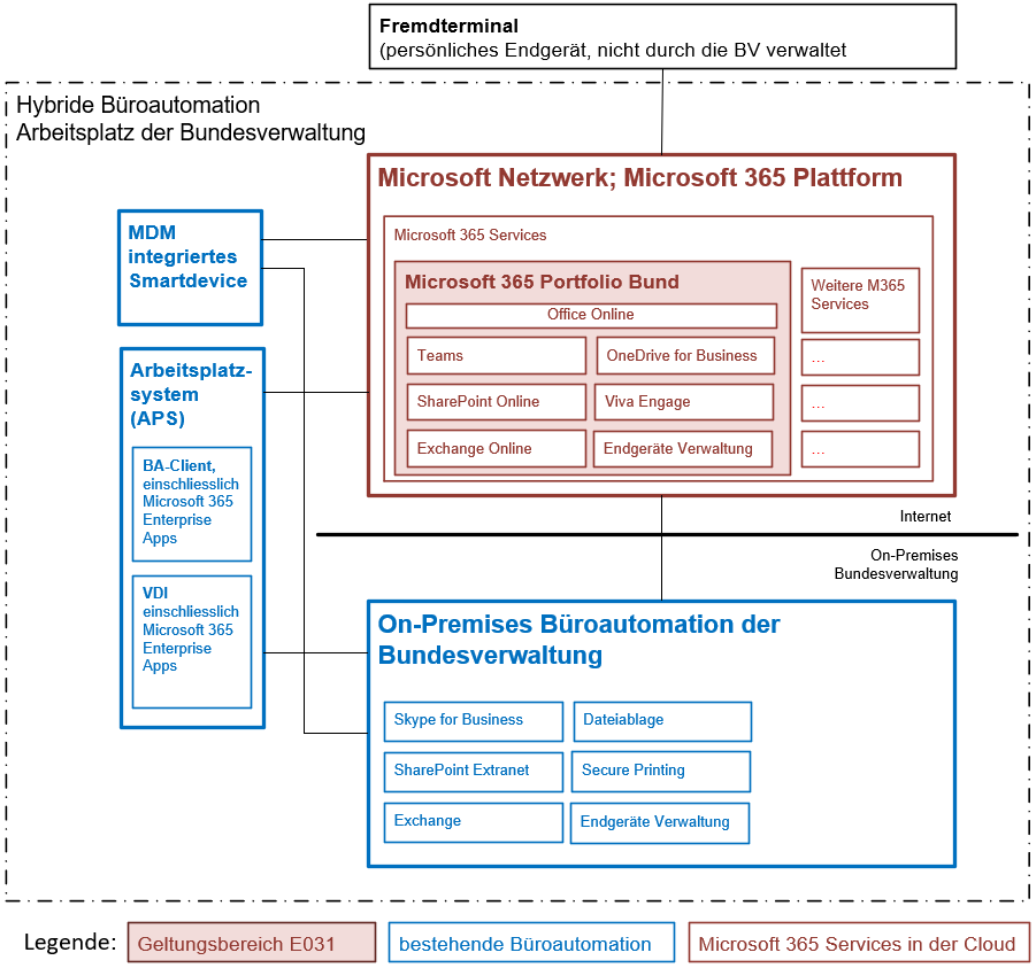

Illustration 1 : vue d'ensemble de la terminologie

C. Modifications par rapport à la version précédente

- Renvoi à la directive d'application [E017] pour les conversations avec Microsoft Teams qui contiennent des données personnelles sensibles au sens de la LPD et des informations classifiées INTERNE au sens de l'OSI et pour les enregistrements de communications vocales et/ou vidéo.
- Adaptation du tableau de l'annexe A (ajout concernant les conversations portant sur des données personnelles sensibles au sens de la LPD moyennant le recours au chiffrement de bout en bout).
- Présentation des responsabilités de la personne invitante vis-à-vis de l'invité.
- OTNI remplacé par ONum

D. Signification des mots-clés pour le degré du caractère contraignant

Le degré du caractère contraignant[15] des différentes dispositions du chap. 2 de la présente directive est indiqué par les mots clés suivants écrits en majuscules :

Mot-clé	**Degré du caractère contraignant**
DOIT	La disposition doit impérativement être respectée (sauf dérogation).
EST INTERDIT	L'option ne peut pas être choisie.
EST PERMIS / A LE DROIT	L'option est autorisée explicitement. L'unité administrative décide si elle veut y recourir. Si la disposition concerne une solution informatique, le fournisseur de la solution doit proposer cette option.
DOIT EN PRINCIPE	En règle générale, cette option doit être choisie. Une unité administrative peut toutefois s'écarter de cette directive sans qu'une dérogation accordée par le secteur TNI ou par l'Office fédéral de 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 disposition concerne une solution informatique, le fournisseur de la solution décide de la proposer ou non.

E. Références

ID	**Référence[16]**
CP : art. 320 (secret de fonction)	Il y a secret de fonction lorsqu'il existe une obligation légale de garder le secret et qu'il s'agit de faits qui ne sont ni connus du public ni accessibles à tous et qui ne peuvent être communiqués ni dans l'intérêt public ni dans l'intérêt privé (renvoi à l'art. 320, al. 1, CP).
E026	E026 - Directive d'application sur le système de poste de travail

[15] 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.

[16] Les références aux actes législatifs de la Confédération sont indiquées conformément au Recueil systématique. La date indiquée est alors celle de la version en vigueur au moment de l'entrée en vigueur de la directive.

ID	Référence[16]
LPD	Loi fédérale du 25 septembre 2020 sur la protection des données (LPD) ; RS 235.1
LSI	Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI) ; RS 128
ONum	Ordonnance sur la numérisation ; RS 172.019.1
Ordonnance GEVER	Ordonnance du 3 avril 2019 sur la gestion électronique des affaires dans l'administration fédérale (Ordonnance GEVER) ; RS 172.010.441
OSI	Ordonnance sur la sécurité de l'information dans l'administration fédérale et l'armée (OSI) ; RS 128.1
RFC 2119	Request for Comments: 2119 (PCB14), The Internet Engineering Task Force (IETF)
SB000	SB000 Stratégie informatique de la Confédération 2020-2023
SD100 - Catalogue des services standard	Le catalogue des services informatiques standard répertorie les différentes prestations, variantes et options pouvant être fournies dans le cadre des services standard. Il est avant tout destiné aux responsables de l'intégration des départements et aux fournisseurs de services standard. SD100 - Catalogue des services standard
Si001	Si001 Protection informatique de base dans l'administration fédérale
Si001-Hi3	Si001 - Hi03: Exigences liées au risque de violation du secret de fonction dans l'administration fédérale – version 1.4

F. Abréviations

Abréviation	Signification
BA	Büroautomation (bureautique)
CEBA	Cloud Enabling Büroautomation (programme de bureautique dématérialisée)
ChF	Chancellerie fédérale
GEVER	gestion des affaires
LPD	Loi fédérale sur la protection des données
LSI	loi sur la sécurité de l'information
MDM	Mobile Device Management (gestion des appareils mobiles)
OSI	ordonnance sur la sécurité de l'information
RFC	Request for Comments
SS Bureautique	service standard Bureautique
TNI	Secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale