Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des InnernEDI
Bundesamt für SozialversicherungBSV
Etat-major de direction DS - IT Management ITM

Communication eGov n° 054 du 10.03.2025

A adresser à : Organes d'exécution du 1er pilier/AFam

Concerne : Nouvelles exigences relatives à l'utilisation de Microsoft 365 (M365) au sein des organes d'exécution du 1er pilier/AFam (version 1.0:2025)

Par la présente, l'OFAS précise la communication eGov 053[1] concernant l'utilisation de M365.

Depuis la publication du communiqué eGov 043[2] au début de l'année 2022, plusieurs développements ont eu lieu. Le 15 septembre 2024, le Conseil fédéral a adopté une modification de l'ordonnance sur la protection des données (annexe[3]), dans le cadre du Swiss-U.S. Data Privacy Framework[4] . De plus, les risques liés au «Foreign Lawful Access» (accès aux données par des autorités étrangères, notamment le «CLOUD Act») ont été réévalués.

Situation de départ et principe

Avec M365, Microsoft propose une suite bureautique complète (Word, Excel, PowerPoint, etc.) permettant aux utilisateurs de travailler où qu'ils soient et sur différents appareils. L'application "Teams", qui fait également partie de M365 et qui succède à "Skype for Business", permet une communication audio et vidéo, une messagerie ainsi qu'une gestion, un traitement et un enregistrement de données sur le SharePoint Online. En outre, Exchange Online fournit un service de messagerie électronique basé sur le cloud qui permet la gestion et le stockage des e-mails, des calendriers et des contacts.

Les données de toutes les applications, y compris les boîtes de messagerie gérées dans Exchange Online, sont stockées de manière cryptée dans un cloud public de Microsoft.

Le cryptage des données dans M365 s'effectue à l'aide de clés de Microsoft, de sorte que la société Microsoft peut décrypter les données stockées à la demande des tribunaux américains et être contrainte de divulguer ces données décryptées aux autorités américaines. Ce problème n'existe pas avec les solutions sur site (on-premise), mais l'exploitation on-premise de systèmes tels que la messagerie électronique (Exchange) peut entraîner un risque accru de cyberattaques et des perturbations importantes dans le fonctionnement d'un organisme d'exécution, car il est difficile de trouver des spécialistes possédant le savoir-faire nécessaire pour la maintenance et l'exploitation.

En revanche, dans le cadre des solutions de cloud public, les versions et techniques les plus récentes sont utilisées, avec des mesures de protection contre les cyberattaques intégrées par défaut. De plus, l'exploitation et la configuration des systèmes sont assurées par Microsoft lui-même.

[1] Communication eGov n° 053 du 17.12.2024
[2] Communication eGov n° 043 du 01.01.2022
[3] Complément à l'annexe 1 du DSV : https://www.fedlex.admin.ch/eli/oc/2024/435/fr
[4] Communiqué de presse sur le Swiss-U.S. Data Privacy Framework : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-102054.html

Après avoir pesé le pour et le contre, l'OFAS conclut que les organes d'exécution du 1er pilier/CAF peuvent utiliser M365. Cependant, ils restent responsables de la protection des données et doivent veiller à ce que les données soient uniquement traitées et stockées dans des centres de données en Suisse, et que la documentation ISDS soit régulièrement mise à jour, conforme aux réglementations en matière de protection des données et que des mesures techniques et organisationnelles appropriées soient prises pour protéger les données (par exemple, cryptage). Si les exigences sont plus élevées, par exemple pour les données sensibles, une analyse des besoins de protection, une analyse des risques, un contrôle de la conformité juridique et une analyse d'impact relative à la protection des données personnelles sont indispensables.

Lors de l'utilisation de M365, un tenant (espace de stockage) en Suisse est obligatoire. Celui-ci permet de traiter les données personnelles sur les terminaux gérés sans cryptage supplémentaire. De même, les données peuvent être traitées et enregistrées en ligne avec les applications en ligne de M365 (par exemple Teams, Sharepoint Online, OneDrive for Business ou Exchange Online). Pour ces services, une authentification multi-facteurs (MFA[5]) doit être mise en place, ce qui est désormais le cas par défaut pour tous les services Azure.

Une dépendance aux services cloud de Microsoft, ainsi qu'à d'autres services cloud, comporte des risques. Les organes d'exécution doivent élaborer une stratégie de sortie et documenter les mesures à prendre pour rester opérationnels en cas d'urgence.

L'utilisation de Microsoft Exchange Online est possible dans le cadre des limitations décrites ci-dessus, telles que l'analyse et l'évaluation pour les données personnelles sensibles et l'implémentation de l'authentification multi-facteurs (MFA). Toutefois, pour l'envoi de données sensibles, il est en outre impératif d'utiliser une technologie de cryptage de pointe (par exemple IncaMail ou équivalent).

Les détails des analyses et des évaluations sont disponibles dans la D-SIPD[6], aux annexes 3 et 4.

L'utilisation d'autres services et fournisseurs de cloud sera abordée dans une future communication eGov.

Nous vous remercions de prendre connaissance de ces informations et de mettre en œuvre ces mesures au sein de votre organe d'exécution.

Le secteur ITM

Pour toute autre question, veuillez vous adresser à egov@bsv.admin.ch

[5] Microsoft MFA : https://go.microsoft.com/fwlink/?linkid=2227647&clcid=0x807&culture=de-ch&country=ch
[6] D-SIPD : https://sozialversicherungen.admin.ch/de/d/20253/download

Contexte du CLOUD Act et de la FISA

Les deux lois américaines, le «CLOUD Act[7] » et le «Foreign Intelligence Surveillance Act» (FISA[8]), présentent un risque de violation de la protection des données suisses lorsqu'on utilise des fournisseurs de cloud public, tels que Microsoft. Le problème fondamental actuel réside dans le traitement des données sous-traité à des entreprises qui, du point de vue suisse, sont soumises au droit suisse, mais qui peuvent être contraintes par des tribunaux américains, en vertu du CLOUD Act et du FISA, à divulguer certaines données aux autorités américaines. On peut supposer que des problèmes similaires existent avec la législation d'autres pays (p. ex. la Chine).
En principe, la législation suisse autorise la communication de données dans le cadre d'une enquête pénale (voir par ex. l'art. 50, al. 1, let. d, LAVS). Cependant, en raison du principe de territorialité, les données demandées ne peuvent être transmises qu'à une autorité d'enquête suisse. Si une autorité étrangère souhaite obtenir des renseignements, elle doit en faire la demande via l'entraide judiciaire internationale, conformément aux accords internationaux en vigueur. L'autorité suisse compétente s'adressera alors à l'organe d'exécution et demandera la remise des données, mais tout ça seulement après avoir examiné la demande d'entraide judiciaire. Les demandes d'entraide judiciaire portant sur des infractions qui n'existent pas en droit suisse ne sont pas acceptées.
Le Cloud Act et le FISA permettent aux autorités américaines de contourner ce principe de territorialité par une sorte d'« entraide judiciaire arbitraire », évitant ainsi la procédure d'entraide judiciaire normalement établie.

[7] CLOUD Act : https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf
[8] FISA : Loi sur la surveillance du renseignement extérieur (FISA)