GRAND CONSEIL **QUE 2220-A**
de la République et canton de Genève

Date de dépôt : 20 août 2025

Réponse du Conseil d'Etat

à la question écrite urgente de Pierre Nicollier : L'intégrité numérique des collaborateurs de l'Etat est-elle garantie ?

En date du 20 juin 2025, le Grand Conseil a renvoyé au Conseil d'Etat une question écrite urgente qui a la teneur suivante :

Le Temps a révélé que l'Etat de Genève a discrètement opté pour un déploiement élargi de la suite Microsoft 365 au sein de son administration. Cette décision soulève plusieurs questions importantes concernant l'usage, la sécurité et la gouvernance des données des collaborateurs.

Dans ce contexte, mes questions sont les suivantes :

- ***Quelles applications et fonctionnalités de Microsoft 365 sont et seront activement déployées dans l'administration cantonale ?***
- ***Où sont localisées les données et comment est-ce garanti ?***
- ***L'intégrité numérique des utilisateurs est-elle garantie et quelles mesures techniques ou organisationnelles ont été mises en place pour la garantir ?***
- ***Qui au sein de Microsoft a accès aux données des utilisateurs et avec quel cadre juridique se fait cet accès encadré ?***
- ***Par quel mécanisme de contrôle et de vérification ces mesures sont-elles surveillées et auditables ?***

Que le Conseil d'Etat soit vivement remercié par avance des réponses qu'il apportera aux présentes questions.

RÉPONSE DU CONSEIL D'ÉTAT

– ***Quelles applications et fonctionnalités de Microsoft 365 sont et seront activement déployées dans l'administration cantonale ?***

A l'exception de 2 tests menés sur Microsoft Planner et Power Automate Desktop, l'usage de Microsoft 365 est actuellement limité aux seules fonctionnalités indispensables à la gestion des identités et des droits d'accès. Cela concerne exclusivement des données d'identification de base – nom, prénom, adresse e-mail professionnelle – utilisées pour attribuer et gérer les licences logicielles. Aucun service collaboratif (comme OneDrive, Teams ou SharePoint Online) n'est activé, et aucune donnée métier, confidentielle ou sensible n'est traitée dans le cloud. Ce choix architectural permet une maîtrise complète des flux de données et s'inscrit dans un cadre juridique et technique strictement encadré.

En janvier 2025, l'Etat de Genève a souhaité s'assurer de la conformité légale de cet usage de Microsoft 365 en sollicitant un avis de droit indépendant. Cet avis porte spécifiquement sur le traitement des données d'annuaire (nom, prénom, adresse e-mail professionnelle) dans le contexte légal actuel. Il confirme que ces données, considérées comme non sensibles, peuvent être utilisées dans ce cadre, à condition que les garanties contractuelles et techniques prévues soient respectées. Cette démarche traduit la volonté de l'administration cantonale d'agir avec prudence, transparence et dans le respect du cadre légal.

A noter qu'il est envisagé dans les prochaines années, un déploiement progressif et encadré des fonctionnalités les plus pertinentes pour l'Etat de la suite Microsoft 365, en fonction de l'évolution des conditions techniques, organisationnelles, juridiques et de maturité numérique. Cela pourrait inclure des services tels que OneDrive, Teams, SharePoint Online, ou encore les outils de cybersécurité avancée. Chaque activation sera précédée d'une évaluation rigoureuse des impacts, des risques et des garanties à mettre en place, notamment en matière de souveraineté des données et de protection de la vie privée.

Cette approche permet à l'administration cantonale de répondre à des besoins croissants de collaboration, de gestion unifiée des environnements numériques et de sécurité renforcée, tout en respectant les principes fondamentaux de proportionnalité, de maîtrise des risques et de conformité légale. Microsoft a d'ailleurs récemment annoncé la mise en place de solutions souveraines renforcées pour l'Europe, garantissant un traitement des données – y compris les métadonnées – exclusivement dans l'Union européenne, sous contrôle local. L'office cantonal des systèmes

d'information et du numérique (OCSIN) en suit attentivement la concrétisation et l'intégrera dans ses évaluations futures pour renforcer encore la maîtrise des données dans le cadre du déploiement progressif de Microsoft 365.

En parallèle, l'OCSIN poursuit une veille sur les alternatives possibles, notamment open source ou souveraines, dans la perspective d'un éventuel désengagement partiel ou total. L'horizon cible de 2032 a été fixé pour rendre disponibles des solutions alternatives viables, fonctionnelles et interopérables.

– ***Où sont localisées les données et comment est-ce garanti ?***

Les données des services Microsoft utilisés par l'administration cantonale sont hébergées dans des centres de données situés exclusivement dans l'Union européenne. Cette exigence est garantie par un cadre contractuel suisse renforcé, établi par l'ANS (Administration numérique suisse)[1], auquel l'administration cantonale est partie prenante.

Ce contrat intègre un addendum spécifique à la protection des données, conforme au droit cantonal (LIPAD), suisse (LPD) et européen (RGPD), *addendum* qui prévoit notamment la localisation obligatoire des données, la limitation des accès, la traçabilité, le chiffrement et un droit de recours sous juridiction suisse.

– ***L'intégrité numérique des utilisateurs est-elle garantie et quelles mesures techniques ou organisationnelles ont été mises en place pour la garantir ?***

L'administration cantonale, par l'intermédiaire de l'OCSIN, applique une approche rigoureuse pour garantir l'intégrité numérique des utilisateurs, c'est-à-dire la protection de leur identité, de leurs droits numériques fondamentaux et de leurs données personnelles.

Dans le cas des services Microsoft utilisés actuellement, seules des données d'identification de base sont traitées dans le cloud. Aucune donnée sensible, confidentielle ou issue des contenus métiers (documents, messages, fichiers) n'est transférée ou hébergée hors des infrastructures internes de l'administration cantonale.

[1] Le contrat a été initialement conclu entre Microsoft et la Conférence suisse sur l'informatique (CSI). Depuis le 6 septembre 2024, l'ensemble des missions de la CSI a été transféré à l'Administration numérique suisse (ANS).

Comme évoqué dans la réponse apportée à la question précédente, pour encadrer cet usage, l'administration cantonale s'appuie sur un contrat-cadre conclu avec Microsoft par l'ANS, qui intègre des garanties juridiques renforcées : engagement à traiter les données exclusivement dans l'Union européenne, obligation de chiffrement, limitation stricte des accès internes chez Microsoft, traçabilité des opérations, droit d'audit, et clause de juridiction suisse en cas de litige.

Sur le plan organisationnel, l'OCSIN applique une procédure d'éligibilité pour chaque service numérique, fondée sur l'analyse des risques, la classification des données et la validation des usages. Des directives d'utilisation claires sont également diffusées aux utilisateurs pour éviter toute exposition involontaire de données personnelles ou professionnelles.

– ***Qui au sein de Microsoft a accès aux données des utilisateurs et avec quel cadre juridique se fait cet accès encadré ?***

Dans le cadre des services utilisés par l'administration cantonale, seuls des employés autorisés de Microsoft, agissant dans le cadre de fonctions techniques strictement définies (support, sécurité, maintenance), peuvent potentiellement accéder aux données — et cela uniquement dans des cas exceptionnels, encadrés par des procédures internes, des contrôles techniques et des obligations contractuelles.

En pratique, cet accès est limité aux données personnelles non sensibles (nom, prénom, adresse e-mail professionnelle), car aucun contenu métier, ni aucune donnée confidentielle, n'est stocké dans le cloud. Les accès sont enregistrés, contrôlés et audités.

Le cadre juridique qui régit ces accès est celui du contrat ANS (Administration Numérique Suisse), auquel l'administration cantonale adhère.

Ainsi, tout accès éventuel aux données par Microsoft est non seulement techniquement limité, mais également juridiquement encadré, surveillé et opposable par l'administration cantonale en cas de manquement.

– ***Par quel mécanisme de contrôle et de vérification ces mesures sont-elles surveillées et auditables ?***

Les mesures de sécurité et de protection des données mises en œuvre dans le cadre du contrat entre Microsoft et l'ANS (Administration numérique suisse) sont surveillées à travers plusieurs mécanismes concrets. L'OCSIN dispose par défaut d'un accès aux journaux d'activité (logs) via le portail d'administration de Microsoft 365, ce qui permet de suivre et de tracer les

actions réalisées tant par les utilisateurs que par le support de Microsoft. En complément, le contrat prévoit la possibilité pour l'administration cantonale de demander des audits spécifiques, afin de vérifier que les engagements contractuels sont bien respectés, notamment en matière de localisation des données, de sécurité et de conformité. Ces audits peuvent s'appuyer sur les certifications de service et les rapports de conformité mis à disposition par Microsoft, garantissant ainsi une traçabilité et une audibilité continues, encadrées par un dispositif contractuel opposable.

Au bénéfice de ces explications, le Conseil d'Etat vous invite à prendre acte de la présente réponse.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Michèle RIGHETTI-EL ZAYADI	Thierry APOTHÉLOZ