Administrations publiques : et si le vrai danger pour les données des administré(e)s n'était pas le cloud, mais l'inaction numérique ?

Stéphanie Chuffart-Finsterwald, Philipp Fischer, Nathan Philémon Matantu et Claire Tistounet, le 5 mars 2026

La résolution de privatim du 18 novembre 2025 considère que l'externalisation par les organes publics du traitement de données personnelles sensibles ou soumises à une obligation légale de garder le secret dans des solutions *cloud* proposées par des fournisseurs dits internationaux n'est pas admissible dans la plupart des cas. Selon les autrices et auteurs de la présente contribution, la résolution n'est pas suffisamment nuancée, ne repose pas sur le cadre juridique de *lege lata* et ne tient pas compte de l'ensemble des risques en présence.

Résolution de privatim sur l'externalisation du traitement des données dans le cloud du 18 novembre 2025

Remarque : La présente contribution complète et approfondit un éditorial publié le 5 mars 2026 dans le journal Le Temps, accessible ici.

I. Introduction

À l'instar des acteurs du secteur privé, les organes publics se détournent de plus en plus fréquemment des solutions informatiques installées sur site (*on premise*) au profit de solutions fournies à distance grâce au recours à la technologie de l'informatique en nuage (*cloud computing* ou *cloud*). Le *cloud computing* permet notamment aux fournisseurs de proposer l'accès aux logiciels en tant que services (*Software-as-a-Service*, ci-après : « SaaS »).

Avec ces solutions, les données sont hébergées et traitées directement sur l'infrastructure *cloud* du fournisseur de services. Ce dernier assure la disponibilité du logiciel et sa maintenance, met en œuvre les mesures de sécurité requises et fournit un service de support (Jean-Claude Franchitti et al., Introduction to Computer Science, Houston 2024, p. 693 ss ; Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller/Damian George, Utilisation des services de cloud par les avocats, Revue de l'avocat 2019, p. 34).

Ces dernières années, l'administration fédérale (cf. Communiqué de presse de la Chancellerie

fédérale et de l'Office fédéral de l'informatique et de la télécommunication du 18 décembre 2025 ; cf. ég. Office fédéral des assurances sociales (OFAS), Communication eGov n° 054 du 10 mars 2025, disponible ici, qui porte sur l'usage de M365 (la version *cloud* de la suite bureautique de Microsoft) par les organes d'exécution du 1er pilier et des allocations familiales) ainsi que les administrations des cantons d'Argovie (cf. Réponse du Conseil d'État du 17 septembre 2025), de Bâle-Ville (cf. Communiqué du Conseil d'État du 8 avril 2025), de Berne (cf. Communiqué de presse du 30 juin 2023), de Lucerne (cf. Réponse du Conseil d'État du 24 septembre 2024) ou encore de Zurich (cf. Procès-verbal du Conseil d'État du 30 mars 2022), ont migré vers la suite Microsoft 365, générant quelques remous politiques.

Le 24 novembre 2025, privatim, la Conférence des Préposé(e)s suisses à la protection des données (ci-après : « privatim ») a publié une résolution adoptée le 18 novembre 2025 intitulée « Résolution sur l'externalisation du traitement des données dans le cloud » (ci-après : la « Résolution »), dans laquelle elle retient notamment que :

> « […] l'externalisation par les organes publics de données personnelles sensibles ou soumises à une obligation légale de garder le secret dans des solutions SaaS de grands fournisseurs internationaux n'est pas admissible dans la plupart des cas. »

Depuis la publication de la Résolution, Martine Stoffel, Préposée à la protection des données du canton de Fribourg et représentante de privatim (cf. interview du 22 décembre 2025 dans l'émission *Forum* de la RTS), et Dominika Blonski, Préposée à la protection des données et à l'information du canton de Zurich et Vice-présidente de privatim (cf. interview du 25 novembre 2025 par la SRF), ont défendu la position de l'association dans les médias.

Dans son interview du 22 décembre 2025, Madame Stoffel est allée encore plus loin que le contenu de la Résolution, déclarant que les données sur la santé, les opinions religieuses ou les sanctions prises contre des personnes ne doivent pas être externalisées dans des *clouds*, bien que cette position de principe semble ensuite être un peu nuancée en fin d'interview.

La Résolution a suscité de nombreuses réactions critiques de la part des praticien(ne)s ainsi que dans les cercles académiques, notamment en raison de son approche peu nuancée et déconnectée du droit en vigueur et de la réalité technologique. Au sein d'un éditorial publié dans le journal *Le Temps*, nous expliquons pourquoi l'approche de privatim nous parait peu opportune (cf. ég. David Vasella, privatim : Resolution zur Auslagerung von

Datenbearbeitungen in die Cloud, 25 novembre 2025, in : datenrecht.ch).

La présente contribution vise à analyser et nuancer la Résolution. Après avoir présenté brièvement privatim (section II *infra*) et résumé le contenu de la Résolution (section III *infra*), il sera lieu de l'apprécier juridiquement (section IV *infra*), avant de conclure (section V *infra*).

II. Considérations générales relatives à privatim

privatim est une association de droit privé au sens des art. 60 ss CC (art. 1.1 des Statuts de privatim ; ci-après : les « Statuts »), dont les membres sont le Préposé fédéral à la protection des données et à la transparence (ci-après, le « PFPDT »), tous les Préposées cantonales et Préposés cantonaux, ainsi que certaines communes (Ville de Berne, Bienne, Köniz, Steffisburg, Thoune, Ville de Zurich, Uster et Winterthur). La Préposée à la protection des données de la Principauté du Lichtenstein a également adhéré à privatim avec un statut d'observatrice (art. 5.4 des Statuts).

Conférence suisse en matière de protection des données, privatim vise à (i) renforcer le respect des exigences de la protection des données, (ii) encourager la collaboration entre les cantons, les communes et la Confédération, (iii) améliorer les compétences des membres, (iv) utiliser plus efficacement les ressources des membres et (v) être un interlocuteur pour les autorités et le public (art. 3.1 des Statuts).

Aux fins d'atteindre ses buts statutaires, privatim a notamment la possibilité de prendre position sur tout projet relatif à la protection des données (art. 4.1 let. c et 18.1 des Statuts). Il convient toutefois de noter que les prises de position et résolutions de privatim ne sont pas nécessairement adoptées à l'unanimité. En effet, les membres de l'assemblée générale ont la possibilité de s'en dissocier en exerçant une option de sortie (art. 18.2 des Statuts). C'est ce que la Préposée du canton de Glaris a fait dans le cadre de la Résolution (cf. section III *infra*).

Les prises de position et les résolutions adoptées par privatim sont des décisions prises par une association de droit privé, bien que celle-ci soit composée d'organes publics. Par conséquent, elles ne sont directement contraignantes que pour ses membres (CR CC I-Hari/Jeanneret, art. 66 N 1 s. et art. 67 N 20). Il est également relevé que privatim n'est pas un organe législatif compétent au niveau cantonal et/ou fédéral.

III. Contenu de la Résolution

Rappelant l'existence d'une « *responsabilité particulière* [des organes publics] *vis-à-vis des*

données de leurs citoyens », privatim a adopté la Résolution, dans laquelle elle exclut par principe l'externalisation des données personnelles sensibles ou soumises à une obligation de garder le secret dans des solutions *cloud* de type SaaS offerts par « *de*[s] *grands fournisseurs internationaux* ».

Cette Résolution repose sur les cinq motifs suivants :

1. Les fournisseurs *cloud* n'offriraient pas de véritable chiffrement de bout en bout les empêchant d'accéder aux données en clair (cf. section IV/B/i *infra*) ;
2. Le fonctionnement des fournisseurs « *opérant à l'échelle mondiale* » serait opaque et empêcherait un contrôle efficace par les autorités suisses qui leur confient des données (cf. section IV/B/ii *infra*) ;
3. Le transfert entraînerait une « *perte de contrôle considérable* » pour l'institution concernée (cf. section IV/B/iii *infra*) ;
4. Le transfert créerait une « *grande insécurité juridique* », en particulier s'agissant des données soumises au secret de fonction (cf. section IV/B/iv *infra*) ; et
5. Ces risques seraient accrus par le *Clarifying Lawful Overseas Use of Data Act* étatsunien (ci-après : le « US CLOUD Act »), qui permet aux autorités américaines d'accéder aux données hébergées par les fournisseurs sans respecter les règles de l'entraide judiciaire (cf. section IV/B/v *infra*).

À suivre privatim, les organes publics qui souhaitent externaliser le traitement de données personnelles sensibles ou soumises à une obligation légale de garder le secret ne pourraient le faire que moyennant le respect des deux conditions cumulatives :

1. Les données sont chiffrées par l'organe public responsable du traitement ; et
2. Le fournisseur du service de *cloud computing* n'a pas accès à la clé de déchiffrement.

Il est intéressant de noter que la Résolution n'a pas fait l'unanimité au sein même de privatim. En effet, la Préposée à la protection des données du canton de Glaris a fait usage de son droit statutaire à l'*opt-out* (option de sortie selon l'art. 18.2 des Statuts), se dissociant ainsi de la Résolution.

IV. Appréciation de la Résolution

A. Contexte général

La Résolution s'inscrit dans le prolongement de l'« Aide-mémoire sur les risques et les

mesures spécifiques à la technologie du Cloud » publié par privatim le 3 février 2022 (ci-après : l'« Aide-mémoire »), dans lequel privatim retient que le *cloud* induit des risques supplémentaires par rapport à la sous-traitance traditionnelle des données (Aide-mémoire, section 1 p. 1 s.) – étant relevé à cet égard que contrairement à la Résolution, l'Aide-mémoire admet que les organes publics peuvent mettre en œuvre différentes mesures afin d'éliminer les risques identifiés, respectivement de les réduire à un niveau acceptable (Aide-mémoire, section 3 p. 7 s.). Cette Résolution reflète également l'approche plutôt conservatrice adoptée précédemment par l'association (cf. not. privatim, Prise de position « Pas de feu vert pour « Microsoft 365 » » du 30 septembre 2022).

Bien qu'il soit indéniable que les données personnelles sensibles ou soumises au secret de fonction doivent bénéficier d'une protection particulière, et que la Résolution attire légitimement l'attention des organes publics sur les risques induits par les solutions *cloud*, elle n'en demeure pas moins critiquable à plusieurs égards.

Tout d'abord, les cinq motifs développés dans la Résolution ne sont pas suffisamment nuancés, ne reflètent que partiellement le droit en vigueur et ne tiennent pas compte des solutions à disposition des organes publics pour réduire les risques induits par l'externalisation à un niveau acceptable (cf. section IV/B *infra*). En outre, la Résolution se focalise sur les potentiels transferts transfrontières des données et occulte les autres risques auxquels sont confrontés les organes publics, particulièrement en matière de sécurité des données (cf. section IV/C *infra*).

B. Critique de la Résolution

Pour les raisons exposées ci-après, les motifs sous-jacents à la Résolution ne sont juridiquement et techniquement pas convaincants :

i. Motif 1 : Une absence de chiffrement de bout en bout dans les solutions de type SaaS

Dans un premier motif, privatim exclut l'externalisation des données personnelles sensibles ou soumises à une obligation légale de garder le secret au motif que la plupart des solutions de type SaaS n'offrirait pas de chiffrement de bout en bout empêchant tout accès aux données en clair.

Cette affirmation ne prend toutefois pas en compte les mécanismes permettant à l'utilisateur de valider préalablement tout accès du prestataire à la clé de déchiffrement. De tels mécanismes permettent à l'utilisateur de contrôler, sur une base *ad hoc*, qui a accès à quelles

données et pour quel motif.

De ce fait, privatim arrive à la conclusion que le recours au *cloud* ne serait envisageable que si les données sensibles ou soumises au secret sont anonymisées ou cryptées avec une clé de déchiffrement exclusivement détenue par l'organe public.

Or, indépendamment du fait que, dans un tel scénario, le droit suisse de la protection des données ne trouverait même pas application faute de données personnelles concrètement accessibles par le prestataire *cloud* (cf. p.ex. art. 2 al. 1 *cum* 5 let. a LPD, art. 2 al. 1 *cum* 4 al. 1 LCPD-BE, art. 3 al. 1 *cum* 4 al. 1 let. a LPrD-FR et art. 3 al. 1 *cum* 4 al. 1 ch. 1 LPrD-VD), cette affirmation ignore le fait que la conservation de la clé de déchiffrement par le fournisseur *cloud* peut en réalité offrir un niveau de sécurité supérieur à une détention exclusivement assumée par l'institution publique (cf. section IV/C *infra*).

Il est par ailleurs intéressant de noter que l'Aide-mémoire de 2022 est plus permissif que la Résolution s'agissant du chiffrement des données personnelles sensibles et de la gestion des clés de chiffrement, alors même qu'il a été publié après l'invalidation du *CH-US Privacy Shield* (cf. Communiqué de presse du PFPDT du 8 septembre 2020 ; cf. ég. Philipp Fischer, Schrems II ou la quadrature du cercle, 18 octobre 2020 in : swissprivacy.law/17) et avant l'adoption du *Swiss-U.S. Data Privacy Framework* (ci-après : le « CH-U.S. DPF » ; à cet égard, cf. section IV/B/v *infra*), dans un contexte où le transfert de données personnelles vers les États-Unis n'était donc couvert par aucun accord international. En effet, aux termes de l'Aide-mémoire, le chiffrement de données personnelles sensibles peut être effectué directement chez le fournisseur de services *cloud*, pour autant que cette modalité ne fasse pas peser de risques inacceptables sur les droits fondamentaux des personnes concernées. Par ailleurs, privatim y indique que le fournisseur peut conserver les clés de chiffrement, sous réserve d'engagements contractuels garantissant leur protection contre tout incident de sécurité, leur utilisation exclusivement avec le consentement exprès de l'organe public et la journalisation de tout accès aux données (Aide-mémoire, section 2.3 b p. 5). Dans ce contexte, on peine à comprendre le durcissement opéré dans la Résolution.

ii. Motif 2 : Une transparence insuffisante des « *entreprises opérant à l'échelle mondiale* »

Dans un deuxième motif, privatim exclut l'externalisation des données personnelles sensibles ou soumises à une obligation légale de garder le secret car les « *entreprises opérant à l'échelle mondiale* » (selon les termes utilisés par privatim) n'offriraient pas suffisamment de transparence, ce qui empêcherait les autorités suisses (en leur qualité de « clientes » de ces prestataires) de vérifier le respect des obligations contractuelles en matière de protection

et de sécurité des données, notamment en ce qui concerne la mise en œuvre des mesures techniques et organisationnelles ou le recours à des sous-traitants. Selon privatim, les fournisseurs de services de type SaaS pourraient par ailleurs adapter unilatéralement les conditions contractuelles, ce qui causerait une incertitude inacceptable.

Ces motifs ne convainquent pas non plus.

En premier lieu, le nombre de pays dans lesquels les fournisseurs de services de type SaaS opèrent n'est pas un critère légal en vertu des législations fédérales et cantonales en matière de protection des données personnelles.

Ensuite, privatim sous-entend que tous les fournisseurs actifs à l'étranger n'offriraient pas suffisamment de transparence, ce qui rendrait difficile l'examen de la conformité des activités de traitement avec le cadre légal applicable. Il n'y a pourtant aucun automatisme en la matière. Les fournisseurs de services opérant à l'étranger peuvent être tout à fait transparents, tout comme les fournisseurs de services en Suisse peuvent être parfaitement opaques.

Par ailleurs, cette position ne tient pas compte du fait que les organes fédéraux (comme les autres personnes physiques et morales soumises à la LPD) peuvent communiquer des données personnelles à l'étranger si le Conseil fédéral a constaté, dans l'Annexe 1 OPDo, que la législation de l'État concerné offre un niveau de protection adéquat au sens du droit suisse de la protection des données (art. 16 al. 1 LPD *cum* art. 8 al. 1 OPDo ; sur la réglementation cantonale en matière de communication de données à l'étranger, cf. Sylvain Métille/Marie-Laure Percassi, Les collectivités publiques face à l'externalisation informatique – Analyse sous l'angle de la protection des données personnelles, in : Jusletter du 29 septembre 2025, N 39 s.). Or, suite à la mise en place du CH-U.S. DPF, la Suisse reconnaît que les entreprises américaines certifiées selon le CH-U.S. DPF offrent un niveau de protection adéquat (Annexe 1 OPDo, ch. 44 ; à cet égard, cf. ég. section IV/B/v *infra*).

Au surplus, le contenu du contrat que l'organe public conclut avec le fournisseur de services *cloud* est l'élément déterminant (ce qui ressort d'ailleurs expressément de l'Aide-mémoire de privatim, sections 2.1 p. 2 s. et 2.7 p. 7). En tant que responsables du traitement, les organes publics doivent définir la finalité et les moyens du traitement des données personnelles (cf. p.ex. art. 5 let. j LPD, art. 4 al. 1 let. h, 19 et 37 LPrD-FR, art. 4 al. 1 ch. 8 LPrD-VD). À ce titre, il leur incombe d'imposer les obligations contractuelles nécessaires aux fournisseurs afin d'assurer le respect du cadre légal applicable, notamment en matière de localisation des données, de sécurité des données (cf. p.ex. art. 8 LPD *cum* art. 1 ss OPDo, art. 20 s. LPrD-FR, art. 37A P-LIPAD-GE, art. 10 LPrD-VD, art. 10 et 30 P-IDG-ZH) ou de sous-traitance (cf. p.ex.

art. 9 LPD *cum* art. 7 OPDo, art. 18 ss et 37 LPrD-FR, art. 36C P-LIPAD-GE, art. 18 LPrD-VD, art. 9 P-IDG-ZH). Il est notamment possible de prévoir contractuellement des droits d'audit permettant à l'organe public de vérifier le respect des obligations par le fournisseur et l'ensemble de sa chaîne de sous-traitance, ainsi que le droit pour l'organe public de résilier unilatéralement le contrat en cas de recours à un sous-traitant qu'il considère comme « inacceptable ».

En tout état, si la modification unilatérale du contrat par le fournisseur constitue un écueil majeur, l'organe public peut soit chercher à exclure contractuellement de telles modifications unilatérales, soit prévoir qu'en cas de modifications unilatérales, l'organe public dispose d'un délai pour résilier le contrat et ainsi activer la mise en œuvre du plan de sortie prévu par le contrat.

Enfin, il convient de relever qu'en pratique, les contrats proposés par les *hyperscalers* contiennent déjà des clauses détaillées en matière de sous-traitance (avec information préalable et possibilités de contrôle), de droits d'audit et de *reporting* (souvent complétés par des certifications et attestations indépendantes), de localisation des données (y compris avec des options de résidence ou de régionalisation), ainsi que de sécurité de l'information. Ces engagements contractuels s'appuient en outre sur des standards de conformité reconnus au niveau international, ce qui facilite la vérification par les organes publics du respect du droit applicable et des instructions de traitement.

iii. Motif 3 : Une « *perte de contrôle considérable* » sur les données

Dans un troisième motif, privatim exclut l'externalisation des données personnelles sensibles ou soumises à une obligation légale de garder le secret car le recours à des solutions *cloud* entraînerait une perte de contrôle considérable sur les données, de sorte que les organes publics ne pourraient pas exclure la probabilité d'une atteinte aux droits fondamentaux des personnes concernées, mais uniquement réduire la gravité des potentielles violations en ne divulguant pas les données personnelles sensibles « *hors de son domaine de contrôle* ».

Cette affirmation non nuancée ne tient ni factuellement, ni juridiquement.

D'une part, cette affirmation repose sur un présupposé contestable, à savoir que les collaborateurs et les infrastructures informatiques des institutions cantonales et communales préserveraient nécessairement mieux les données que ceux des fournisseurs de services *cloud*. Or, comme il sera exposé à la section IV/C *infra*, l'expérience démontre que le risque d'atteinte à la sécurité des données personnelles ne dépend pas exclusivement de la nature de l'organi-

sation, les entités publiques ayant également été victimes de plusieurs incidents de sécurité.

D'autre part, comme indiqué dans la section IV/B/ii *supra*, les organes publics restent, en cas de sous-traitance, responsables des traitements concernés et ne peuvent pas s'exonérer de leurs obligations en raison d'une externalisation. Au contraire, et ainsi que rappelé *supra* section IV/B/ii., les organes publics doivent imposer des obligations contractuelles aux fournisseurs de services de type SaaS aux fins d'assurer une externalisation des données conforme au cadre légal applicable, et limiter ainsi le risque d'atteintes aux droits fondamentaux des personnes concernées (sur l'importance des *Data Processing Agreements*, cf. not. Manon Baur, Data Processing Agreement : un outil clé pour encadrer et sécuriser la sous-traitance de données personnelles en pratique, 7 octobre 2025, in : swissprivacy.law/377).

iv. Motif 4 : Une insécurité juridique concernant la notion d'auxiliaire

Dans un quatrième motif, privatim exclut l'externalisation des données personnelles sensibles ou soumises à une obligation légale de garder le secret en indiquant qu'il existerait « *parfois une grande insécurité juridique quant à la mesure dans laquelle elles peuvent être transférées vers des services de cloud computing* ». Remettant en cause tous les principes en la matière, privatim estime qu'il ne serait pas « *possible de faire appel à tout tiers en tant qu'auxiliaire, seulement parce que les dispositions du droit pénal relatives au secret professionnel* [art. 321 CP] *et au secret de fonction* [art. 320 CP] *obligent également les auxiliaires des détenteurs de secrets à garder le silence* ». Cette mention, également présente dans l'Aide-mémoire (cf. section 2.3.c p. 5), ne semble pas prendre en compte la nouvelle teneur de l'art. 320 CP.

En effet, cette conception entre en contradiction nette avec l'évolution récente du cadre légal en la matière. Depuis le 1er janvier 2023, la disposition légale protégeant le secret de fonction (art. 320 CP) a été spécifiquement modifiée afin d'autoriser le transfert d'informations soumises au secret de fonction à des prestataires tiers, y compris lorsque ceux-ci sont localisés à l'étranger, ce que la Conseillère fédérale Karin Keller-Sutter avait, au demeurant, expressément confirmé devant le Parlement (Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 p. 2886 ss ; Conseillère fédérale Karin Keller-Sutter, in : BO 2022 N 353 s. ; cf. ég. Dominika Blonski, Cloud Computing – Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich, in : Astrid Epiney/Sophia Rovelli (édit.), L'intelligence artificielle et protection des données, Zurich/Bâle/Genève 2021, p. 72 ; Métille/Percassi, N 20 ss et 82).

Le Conseil fédéral a retenu cette solution afin d'assurer une cohérence systématique avec le

régime du secret professionnel. En effet, l'art. 321 CP (secret professionnel) réprimait déjà la violation du secret par les auxiliaires des détenteurs du secret. Autrement dit, puisque les auxiliaires des professionnels soumis au secret étaient déjà concernés par l'art. 321 CP, il était logique de prévoir un mécanisme équivalent pour le secret de fonction via la révision de l'art. 320 CP (Message concernant la loi sur la sécurité de l'information du 22 février 2017, FF 2017 p. 2888).

v. Motif 5 : Un risque induit par le US CLOUD Act

Dans un cinquième et ultime motif, privatim exclut l'externalisation des données personnelles sensibles ou soumises à une obligation légale de garder le secret en raison de l'existence du US CLOUD Act, en application duquel les fournisseurs de services étatsuniens pourraient être sommés de communiquer des données personnelles aux autorités étatsuniennes, cela même lorsque les données seraient hébergées en Suisse (pour une présentation du US CLOUD Act, cf. Philipp Fischer/Sébastien Pittet, *US CLOUD Act* – un aperçu, 8 novembre 2021, in : swissprivacy.law/101).

Ce motif s'ancre dans une certaine réalité juridique. Toutefois, à la suite de l'évolution du cadre légal américain, en particulier la limitation des droits d'accès des services de renseignement et la mise en place de mécanismes de recours pour les personnes concernées, la Suisse reconnaît, depuis le 14 août 2024, que les États-Unis offrent un niveau de protection adéquat au sens de l'art. 16 LPD pour les données personnelles traitées par les organisations certifiées conformément au CH-U.S. DPF (Annexe 1 OPDo, ch. 44 ; pour un aperçu du *Swiss-U.S. Data Privacy Framework*, cf. Jeremy Reichlin/Gabriel Kasper/Kirsten Wesiak Schmidt, Data Privacy Framework, 26 août 2024 in swissprivacy.law/313). Cette décision du Conseil fédéral s'appuie notamment sur une évaluation effectuée par l'Office fédéral de la justice (OFJ) (cf. ég. OFJ, Evaluation de l'adéquation – Etats-Unis du 30 avril 2024).

Au moment de l'adoption de cette décision, le Conseil fédéral avait pleinement conscience des risques induits par le US CLOUD Act (cf. not. Conseillère fédérale Simonetta Sommaruga, in : BO 2018 N 1400 ; Avis du Conseil fédéral fédéral du 26 août 2020 relatif à l'Interpellation Balthasar Glättli 20.3875 « Amélioration de la protection des données dans le contexte du Cloud Act »). Partant, l'ajout des États-Unis à l'Annexe 1 OPDo clôt *de lega lata* le débat relatif à la comptabilité du US CLOUD Act avec le cadre légal suisse (Katharina Martin/Philipp Fischer, Swiss-US Data Privacy Framework : un premier pas vers une approche plus pragmatique ?, 17 janvier 2025, in : swissprivacy.law/332 ; Métille/Percassi, N 81). privatim ne prend pas en compte l'évolution du système législatif et l'analyse effectuée par le Conseil fédéral

du système juridique américain dans le cadre du CH-U.S. DPF.

Il sied à ce titre de rappeler que les *hyperscalers* Microsoft, Google ou encore Amazon, sont certifiés dans le cadre du CH-U.S. DPF (cf. Data Privacy Framework List).

Par ailleurs, et comme indiqué par privatim dans son Aide-mémoire, les organes publics peuvent réduire encore le risque d'accès en vertu du US CLOUD Act par l'adoption de mesures contractuelles telles que l'obligation d'informer immédiatement les organes publics de toute demande de communication des données fondée sur le US CLOUD Act, et l'obligation, à charge du prestataire, d'épuiser toutes les voies de recours pour empêcher cette communication (Aide-mémoire, section 2.2 p. 4).

C. Absence de prise en compte des autres risques

La Résolution focalise son analyse du risque sur la communication de données personnelles à l'étranger. Elle fait fi des autres obligations applicables aux organes publics, notamment celles d'assurer une sécurité adéquate des données personnelles par la mise en place de mesures techniques et organisationnelles appropriées (art. 8 LPD *cum* art. 1 ss OPDo, art. 20 s. LPrD-FR, art. 37A P-LIPAD-GE, art. 10 LPrD-VD, art. 10 et 30 P-IDG-ZH) et de prévenir toute divulgation des données couvertes par le secret de fonction (art. 320 CP).

L'expérience pratique démontre toutefois que les incidents de sécurité aux travers, notamment, de cyberattaques, présentent un risque conséquent pour la protection des droits fondamentaux des personnes concernées.

À notre connaissance, les autorités étatsuniennes n'ont jamais accédé aux données hébergées en Suisse en invoquant le US CLOUD Act. En 2022, privatim écrivait même « […] *qu'un tel scénario est hautement improbable dans la pratique* […] » (privatim, Prise de position « Pas de feu vert pour « Microsoft 365 » du 30 septembre 2022).

En revanche, les risques relatifs à la sécurité des données se sont déjà concrétisés à maintes reprises. La cyberattaque par rançongiciel (*ransomware*) dont a été victime la société suisse Xplain AG, alors fournisseuse de la Confédération (cf. not. Communiqué de presse de l'Office fédéral de la cybersécurité (OFCS) du 8 juin 2023), ainsi que celles subies par les communes de Rolle (cf. Message aux citoyennes et citoyens de la commune de Rolle du 31 août 2021) et de Montreux (cf. Communiqué de presse de la commune de Montreux du 10 octobre 2021) en 2021, de Zollikofen en 2023 (cf. Communiqué de presse de la commune de Zollikofen du 23 novembre 2023) ou encore de Villars-sur-Glâne en 2025 (cf. Page mise en place par la

commune de Villars-sur-Glâne concernant la cyberattaque du 18 juin 2025), en apportent une démonstration éloquente.

Par ailleurs, dans son rapport annuel 2024 (ci-après : le « Rapport OFCS »), l'OFCS recense notamment 62'954 signalements volontaires de cyberincidents, 991'309 analyses de signalements concernant les appareils infectés par des logiciels malveillants (*malware*) et 371 signalements de vulnérabilités par des pirates éthiques (Rapport OFCS, p. 4). Avec l'entrée en vigueur de l'obligation de signaler les cyberattaques à l'OFCS en avril et octobre 2025 (art. 74a ss LSI, cf. ég. Claire Tistounet/Philipp Fischer, La nouvelle obligation d'annonce des cyberattaques, 31 mars 2025, in : swissprivacy.law/345), et compte tenu des développements technologiques récents (notamment en matière d'intelligence artificielle), nous pouvons légitimement attendre une hausse de ces chiffres.

Ces éléments démontrent que la sécurité des données est un enjeu crucial, et que les organes publics, particulièrement les petites communes (mais pas seulement) disposant de ressources limitées, n'ont pas toujours les moyens nécessaires en leur sein pour y faire face. Dans ces circonstances, obliger les organes publics à chiffrer eux-mêmes des données et gérer à l'interne les clés de déchiffrement, ou à défaut à héberger des données sur des serveurs en local, alors qu'ils n'ont peut-être pas les compétences techniques pour ce faire, peut s'avérer contre-productif.

Comme le relève à juste titre l'OFAS dans sa communication n° 054, les solutions sur site entraînent un risque accru de cyberattaques si les organes publics n'emploient pas des spécialistes disposant du savoir-faire nécessaire pour maintenir ces solutions et permettre leur exploitation en toute sécurité (cf. ég. Franchitti et al., p. 695). En revanche, en cas de recours à une solution de type SaaS, le fournisseur, qui a la possibilité de mutualiser les coûts sur un large éventail de clients, maintient la solution à jour et met en œuvre les mesures techniques les plus récentes aux fins de permettre une utilisation sécurisée de la solution (OFAS, Communication eGov n° 054 du 10 mars 2025, disponible ici, p. 1 ; cf. ég. Vasella). De ce fait, il est erroné de sous-entendre que les données sont nécessairement exposées à un risque accru si elles sont traitées dans le *cloud*, ou qu'elles sont nécessairement mieux protégées si elles sont traitées localement (cf. ég. Vasella).

Face à ce constat, les organes publics ne peuvent pas adopter des positions de principe, mais doivent apprécier au cas par cas tous les risques en présence, tout en tenant compte des réalités juridiques, techniques et économiques.

V. Conclusion

L'on peut ainsi regretter que la Résolution ne tienne pas compte du droit en vigueur et se focalise uniquement sur le risque relatif à la communication transfrontalière de données, là où les autorités fédérales compétentes ont su faire preuve d'une approche pragmatique et flexible dans l'appréciation de ces enjeux, notamment à travers l'adoption du CH-U.S. DPF.

On peut dès lors s'interroger sur le moment où les autorités suisses de protection des données adopteront une approche holistique, davantage ancrée dans la réalité technique, juridique et économique des administrations publiques, fondée sur une appréciation globale des risques, et ne se limitant pas aux seuls enjeux liés aux transferts transfrontières de données.

Il va de soi que le développement et la promotion de solutions suisses souveraines offrant un niveau de service, de sécurité et de fiabilité comparable à celui des *hyperscalers* constituent un objectif légitime et pleinement justifié. Cela étant, une interdiction de principe du recours à des prestataires internationaux offrant des solutions d'hébergement en Suisse – en particulier lorsque ceux-ci présentent un lien avec les États-Unis – apparaît contreproductive, en ce qu'elle est susceptible d'accroître les risques pesant sur les données personnelles des citoyen(ne)s, dans un environnement où les cyberattaques, et les incidents de sécurité de manière générale, sont pourtant récurrents. Le recours systématique à des solutions locales ou « maison » ne constitue, à cet égard, nullement une garantie de sécurité supérieure.

Enfin, une interdiction pure et simple, pour certaines catégories de données, des solutions *cloud*, ou de celles offertes en Suisse par des prestataires internationaux, relèverait d'un choix éminemment politique dont la mise en œuvre légitime incomberait au législateur, étant rappelé que l'absence totale de risque demeure illusoire, y compris dans le cadre de solutions entièrement internalisées.

Proposition de citation : Stéphanie Chuffart-Finsterwald / Philipp Fischer / Nathan Philémon Matantu / Claire Tistounet, Administrations publiques : et si le vrai danger pour les données des administré(e)s n'était pas le cloud, mais l'inaction numérique ?, 5 mars 2026 *in* www.swissprivacy.law/398