Peut-on encore, en Suisse, recourir à des services cloud offerts par Microsoft ?

Philipp Fischer et Sébastien Pittet, le 16 août 2022

Dans une prise de position publiée le 13 juin 2022, le Préposé fédéral à la protection des données et à la transparence a estimé que le recours aux services cloud M365 de Microsoft serait susceptible de violer la Loi fédérale sur la protection des données, quand bien même le projet de la Caisse nationale suisse d'assurance en cas d'accidents (SUVA) envisage que les données soient hébergées en Suisse et que le cocontractant du responsable du traitement soit une entité européenne du Groupe Microsoft.

1. Contenu de la prise de position du PFPDT

Le 13 juin 2022, le Préposé fédéral à la protection des données et à la transparence (PFPDT) a publié une prise de position relative à un projet de la Caisse nationale suisse d'assurance en cas d'accidents (SUVA) impliquant le recours aux services *cloud* M365 de Microsoft, notamment les services *Outlook* et *Teams*. Le PFPDT a également publié la réponse de la SUVA à sa prise de position, une démarche exemplaire en termes de transparence.

Le projet implique un stockage des données personnelles sur une infrastructure *cloud* basée en Suisse. Le cocontractant (sous-traitant dans la perspective des règles de protection des données) de la SUVA est l'entité irlandaise du Groupe Microsoft (Microsoft Ireland Operations Ltd).

La SUVA a identifié dans son analyse du projet le risque d'accès aux données hébergées sur le *cloud* par les autorités américaines en vertu du US CLOUD Act (sur le US CLOUD Act, cf. not. swissprivacy.law/101). Après avoir procédé à une analyse des risques, la SUVA estime qu'un accès aux données par les autorités américaines dans ce contexte est très improbable (« *höchst unwahrscheinlich* ») et considère donc que le recours aux services M365 est licite au regard de la LPD.

Dans sa prise de position, le PFPDT estime tout d'abord que l'existence d'un risque de divulgation de données personnelles aux États-Unis eu égard au US CLOUD Act déclenche automatiquement l'application des dispositions de la LPD en matière de communication transfronta-

lière de données (art. 6 LPD / art. 16 ss nLPD), nonobstant le caractère « suisse » du projet (responsable du traitement en Suisse et stockage de données en Suisse sur les serveurs du sous-traitant). Pour rappel, suite à la décision Schrems II de juillet 2020, le PFPDT a estimé, dans un communiqué du 8 septembre 2020, qu'un transfert de données vers les États-Unis (État ne garantissant pas un niveau de protection adéquat dans une perspective suisse) ne pouvait plus se fonder sur le *Swiss-US Privacy Shield* (sur ce point, cf. not. swissprivacy.law/17). D'autres mesures de protection, comme des clauses contractuelles types de protection des données, doivent donc être mises en œuvre, tout en tenant compte de la pratique du PFPDT en la matière (cf. le « *Swiss finish* » en cas de recours aux Clauses-Modèles de l'Union européenne ; sur ce point, cf. not. le communiqué du PFPDT, commenté *in* swissprivacy.law/91).

Ensuite, le PFPDT maintient sa position en vertu de laquelle, en cas d'existence d'un risque résiduel d'accès par les autorités d'un État ne garantissant pas un niveau de protection adéquat, aucune donnée personnelle ne peut être communiquée à l'importateur des données (nonobstant la mise en place des clauses contractuelles types). En effet, dans son Guide pour l'examen de la licéité de la communication transfrontière de données, publié en juin 2021, le PFPDT avait déjà estimé que, en cas de communication transfrontalière, les mesures de protection prises par le responsable du traitement doivent réduire à zéro le risque d'accès aux données personnelles par une autorité étrangère, faute de quoi le transfert est jugé incompatible avec la LPD. C'est pourquoi, en cas de persistance d'un risque (même faible) après l'analyse (typiquement formalisée sous la forme d'un *Transfer Impact Assessment*), aucune donnée personnelle ne pourrait, selon le PFPDT, être communiquée à l'importateur situé dans un État ne garantissant pas un niveau de protection adéquat.

Dans la prise de position évoquée ici, le PFPDT affiche un grand scepticisme quant à l'approche fondée sur les risques (*risk-based approach*, *risikobasierter Ansatz*) qui a été prônée par la SUVA, le PFPDT arguant qu'une telle approche ne trouve pas d'ancrage dans la LPD. De plus, face à l'argument de la SUVA selon lequel les données concernées par le projet seraient de peu d'intérêt pour les autorités américaines, le PFPDT estime que ce critère ne devrait pas rentrer en compte dans l'analyse de la licéité d'une communication transfrontalière de données.

2. Observations

Même si la SUVA est qualifiée d'organe fédéral au sens de la LPD (art. 3 let. h LPD / art. 5 let. i nLPD), les obligations en matière de communications transfrontalières de données (telles

qu'interprétées par le PFPDT dans cette prise de position) s'appliquent aux responsables du traitement privés, qui liront donc ce document avec beaucoup d'intérêt.

2.1 Une analyse fondée sur les risques est-elle admissible en matière de communication transfrontalière de données ?

Selon nous, il convient de bien distinguer deux étapes dans l'analyse de la licéité d'une communication de données à l'étranger : (i) l'existence même d'une communication effective de données sur une base transfrontalière et (ii), si une communication a lieu (ou est très probable), la licéité de celle-ci. Comme mentionné ci-dessus, le PFPDT estime que l'existence d'un risque d'accès par les autorités américaines entraîne déjà une communication transfrontalière de données (étape 1) et qu'une approche fondée sur les risques n'est pas pertinente pour analyser la licéité d'une communication (étape 2).

À notre sens, contrairement à la position défendue par le PFPDT, le recours à des services *cloud* hébergés sur des serveurs situés en Suisse d'un sous-traitant européen ne donne pas automatiquement lieu à une communication de données personnelles aux États-Unis, mais seulement une communication de données personnelles vers l'Irlande (dans ce sens : Sylvain Métille, L'utilisation de Microsoft 365, illégale en Suisse ?; voir également l'ordonnance du 13 octobre 2020 du Conseil d'État français statuant en référé dans le cas *Health Data Hub*, résumée *in* Jusletter du 7 juin 2021), voire vers les États d'autres sous-traitants de Microsoft (un volet qui n'est pas abordé dans la prise de position commentée ici).

Pour déterminer *l'existence-même d'une communication transfrontalière* de données (en particulier lorsque les données sont stockées en Suisse), le responsable du traitement doit considérer, lors de cette première étape, les risques d'un accès par les autorités étrangères. Ainsi, l'évaluation des risques n'est pas effectuée pour analyser la licéité d'une communication transfrontalière dans un pays non adéquat (étape 2), mais plutôt en amont pour déterminer l'existence même d'une communication transfrontalière vers un État non adéquat et donc la nécessité (ou non) de mettre en œuvre les mesures de l'art. 6 LPD (étape 1).

Si le résultat de cette évaluation des risques démontre un risque très faible que des autorités étrangères d'un État non adéquat puissent accéder aux données (stockées en Suisse), alors le responsable du traitement devrait, selon nous, arriver à la conclusion (et documenter) qu'il n'y a pas de communication transfrontalière vers un État non adéquat et donc que l'art. 6 al. 2 LPD n'est pas applicable. La question de la licéité de la communication (étape 2) n'aurait alors pas à être analysée.

Au contraire, si l'analyse de risque conclut à un risque non-négligeable d'accès aux données par les autorités étrangères, une communication transfrontalière devrait être retenue (étape 1) et le responsable du traitement devrait respecter les obligations qui découlent de l'art. 6 LPD pour s'assurer de la licéité de la communication (étape 2). Dans cette dernière situation, si les données sont communiquées dans un État ne garantissant pas un niveau de protection adéquat, le responsable du traitement doit pouvoir se prévaloir d'une exception de l'art. 6 al. 2 LPD ou alors renoncer à communiquer les données à l'étranger.

En résumé, nous sommes d'avis que l'évaluation des risques devrait intervenir au stade de détermination de l'existence d'une communication (étape 1) et la question de l'admissibilité de la communication à l'étranger (étape 2) devrait être traitée uniquement en cas d'existence d'une communication. À noter toutefois que telle n'est pas la position prise par le PFPDT dans la prise de position analysée ici.

2.2 Une réticence du PFPDT compréhensible ?

À nos yeux, les raisons suivantes pourraient expliquer la prise de position du PFPDT.

La Commission européenne analyse actuellement si la décision d'adéquation de la Suisse peut être maintenue sous l'angle du RGPD (cf. PFPDT, 29e rapport d'activités 2021/2022, p. 11). Le PFPDT cherche probablement à éviter toute prise de position qui pourrait avoir un impact négatif sur ce processus, en tenant compte également du net durcissement de la pratique des autorités européennes de protection des données en matière de transfert de données aux États-Unis. À titre d'exemples, on peut citer les décisions strictes prises dans les affaires *Google Analytics* : la décision de l'autorité autrichienne de protection des données du 22 décembre 2021, la décision de mise en demeure de la CNIL du 10 février 2022 et plus récemment la décision de l'autorité italienne de protection des données du 9 juin 2022. De même, la chambre des marchés publics de Baden-Wüttemberg (Allemagne) a retenu dans une décision qu'un risque d'accès par les autorités américaines doit être analysé comme une communication effective. En effet, une décision négative quant à l'adéquation de la Suisse aurait des conséquences importantes sur l'économie suisse.

Ensuite, le 25 mars 2022, la Commission européenne et le gouvernement fédéral américain ont annoncé avoir conclu un accord de principe sur un nouveau cadre règlementaire régissant les flux de données personnelles et répondant aux préoccupations exprimées par la Cour de justice de l'Union européenne dans l'arrêt Schrems II de juillet 2020 (cf. les communiqués de presse de la Commission européenne ainsi que de la Maison-Blanche). Précisons que cet accord reste pour le moment une simple déclaration d'intention de vouloir mettre en

œuvre des mesures visant à permettre une communication de données, des mesures de sécurité concrètes devront encore être négociées et mises en œuvre dans le cadre réglementaire américain. Dans sa prise de position, le PFPDT fait référence à cette annonce en précisant que, une fois un accord trouvé au niveau transatlantique, la Suisse devrait également négocier une telle règlementation, qui permettrait un transfert de données vers les États-Unis.

2.3 Divergence entre les autorités cantonales et fédérales

Cette prise de position du PFPDT révèle la complexité de la question et les divergences d'opinions entre les différentes autorités de protection des données suisses. En effet, dans une décision du 30 mars 2022, le Conseil d'État du canton de Zurich avait estimé – après avoir consulté notamment le Préposé cantonal zurichois à la protection des données – qu'une approche fondée sur les risques pouvait être appliquée pour analyser la licéité du recours à des services *cloud* de Microsoft par l'administration cantonale zurichoise.

En résumé, le Conseil d'État du canton de Zurich a estimé dans cette décision que, après analyse, le risque que des autorités étrangères accèdent aux données personnelles stockées sur des serveurs *cloud* de Microsoft situés dans l'Union européenne était très faible et que l'administration cantonale pouvait dès lors recourir à des services M365 de Microsoft, pour autant que certaines mesures additionnelles de protection soient prises afin de limiter ce risque (raisonnement similaire à celui proposé par la SUVA dans le cas d'espèce).

Par ailleurs sur un plan extra-juridique, le Conseil d'État zurichois a également précisé, probablement à juste titre, qu'il n'est aujourd'hui plus envisageable de recourir exclusivement à des services *on premise* (donc non situés sur un *cloud*) et que, pour ne pas se retrouver « technologiquement hors-jeu » (« *technologisch ins Abseits* » selon les termes utilisés par le Conseil d'État zurichois), un recours à des services de type *cloud* est indispensable. Les principaux prestataires de services *cloud* étant basés aux États-Unis (respectivement, présentant des liens avec les États-Unis et entrant par conséquent dans le champ d'application du US CLOUD Act), l'impossibilité de recourir à ces prestataires est économiquement non envisageable.

3. Et maintenant ?

Le lecteur avide d'obtenir une certaine sécurité juridique quant à la licéité du recours à des prestations *cloud* reste sur sa faim après la lecture de la prise de position du PFPDT. Le processus initié par la SUVA a au moins eu le mérite de sensibiliser le PFPDT sur les contraintes auxquelles sont exposés les acteurs économiques suisses.

Selon nous, lors de l'analyse de la licéité d'un projet de type *cloud*, il convient tout d'abord de bien distinguer la situation où (i) les données sont communiquées directement dans un État ne garantissant pas un niveau de protection adéquat (situation qui entraîne une communication transfrontalière) de la situation où (ii) il existe uniquement un risque que les autorités étrangères accèdent aux données, notamment à travers le US CLOUD Act, les données étant néanmoins traitées depuis des États garantissant un niveau de protection adéquat (situation où le *risque* d'une communication transfrontalière doit être analysé). Le projet de Microsoft en vertu duquel les données seront traitées uniquement dans l'Union européenne (« EU Boundary Project » destiné à être lancé en 2023) revêt une grande importance dans ce contexte, étant précisé que le communiqué du 16 décembre 2021 laisse entendre que les données ne seront pas « communiquées » en dehors de l'Union européenne, mais qu'elles pourront être « accessibles » depuis l'extérieur de l'Union européenne.

La mise en place d'une analyse de risques documentée pour déterminer l'existence d'une communication reste une démarche indispensable, même si l'analyse conduite par la SUVA en l'espèce a été critiquée par le PFPDT. Afin de calculer et de pouvoir appréhender le risque, il convient de mener, selon nous, une analyse de risque qui doit en particulier prendre en compte les deux aspects suivants :

- l'existence d'un droit d'accès légal en faveur d'une autorité étrangère (droit d'accès ponctuel), la probabilité que celle-ci le fasse valoir et la probabilité qu'elle arrive à ses fins ;
- l'existence d'un système de surveillance de masse, la probabilité qu'une autorité étrangère utilise ce système pour obtenir un accès aux données et la probabilité qu'elle arrive à ses fins.

Par ailleurs, cette décision met également en lumière la mission de conseil du PFPDT (art. 28 LPD / art. 58 nLPD), étant précisé toutefois que les documents et informations échangés dans ce contexte sont en principe soumis à la LTrans, sauf si l'autorité en a expressément garanti le secret (art. 7 al. 1 let. h LTrans, cf. swissprivacy.law/71 pour un commentaire de cette exception) .

À titre de remarque conclusive, il nous semble important de rappeler que le risque d'accès aux données personnelles par des autorités étrangères (notamment, mais pas uniquement, sur la base du US CLOUD Act) ne constitue pas l'unique prisme par lequel un projet d'externalisation doit être analysé. L'impératif de sécurité des données (à savoir la protection contre les accès non autorisés, y compris à l'interne) et la nécessité de garantir la *business continuity* en cas de défaillance du prestataire représentent des enjeux tout aussi importants,

voire plus cruciaux en termes de risques effectifs à prendre en compte dans le cadre d'un projet impliquant un traitement de données.

Proposition de citation : Philipp FISCHER / Sébastien PITTET, Peut-on encore, en Suisse, recourir à des services cloud offerts par Microsoft ?, 16 août 2022 *in* www.swissprivacy.law/165