www.jusletter.ch

Marine Largant / Philipp Fischer

Health Data Hub

L'éventualité d'un transfert de données liées à la santé vers les Etats-Unis dans le cadre d'une demande d'accès par les autorités américaines constitue-t-elle une atteinte grave et manifestement illégale au droit à la vie privée et à la protection des données des personnes concernées ?

Cet article présente un résumé de l'ordonnance du 13 octobre 2020 du Conseil d'Etat français statuant en référé, qui analyse les risques que présente un traitement de données personnelles relatives à la santé au sein d'un « Health Data Hub », hébergé par Microsoft dans l'Union Européenne. Il analyse également la pertinence du raisonnement de l'ordonnance du Conseil d'Etat pour les entreprises suisses transférant des données au sein d'un cloud et évoque les principaux enjeux du US Cloud Act.

Catégories d'articles : Contributions
Domaines juridiques : Droit de la santé ; Protection des données ; Droit international

Proposition de citation : Marine Largant / Philipp Fischer, Health Data Hub, in : Jusletter 7 juin 2021

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Table des matières

[1] Nous présentons en premier lieu un résumé de l'ordonnance du Conseil d'Etat (I), avant d'évoquer les principaux enjeux du US Cloud Act (II). Nous terminerons en examinant dans quelle mesure le raisonnement présenté dans cette ordonnance peut revêtir de l'importance pour un responsable de traitement situé en Suisse (III).

I. Résumé de la décision

[2] Dans la mouvance de l'arrêt Schrems II de la CJUE[1] qui a invalidé le EU-US Privacy Shield, plusieurs associations et collectifs dans le domaine de la santé ont saisi le juge des référés du Conseil d'Etat français (la plus haute juridiction administrative française) en demandant la suspension du traitement de données personnelles liées à la santé dans le cadre de la lutte contre l'épidémie de COVID-19 sur une plateforme de données de santé (« Health Data Hub »). Le Health Data Hub est géré par un groupement d'intérêt public[2] (« GIP ») institué par le code français de la santé publique et est hébergé par la filiale irlandaise de Microsoft Corporation (« Microsoft Ireland »).

[3] Les demandeurs invoquent à l'appui de leur requête qu'un tel traitement constituerait une atteinte grave aux droits des personnes concernées eu égard au possible accès aux données par les autorités américaines dans le cadre de mesures de surveillance dont peuvent faire l'objet les sociétés européennes qui font partie d'un groupe américain, en vertu du champ d'application extraterritorial de la réglementation américaine dans ce domaine (voir les enjeux du US Cloud Act dans la partie B. ci-dessous).

[4] Ce Health Data Hub contient notamment des données déclaratives de symptômes issues de l'application mobile française StopCovid (maintenant appelée TousAntiCovid) et des résultats d'examens effectués par des laboratoires, toutes les données hébergées et traitées dans le Heath Data Hub étant pseudonymisées.

[5] De manière préliminaire, il convient de noter que le juge des référés du Conseil d'Etat ne peut statuer que sur les mesures de sauvegarde provisoires nécessaires en cas d'atteinte grave et manifestement illégale à une liberté fondamentale par une autorité publique et ne juge dès lors pas de l'affaire au fond.

---

1 Arrêt de la CJUE C-311/18 Data Protection Commissioner/Maximillian Schrems et Facebook Ireland du 16 juillet 2020.

2 En vertu du droit français, le groupement d'intérêt public (« GIP ») permet à des partenaires publics et privés de mettre en commun des moyens pour la mise en œuvre de missions d'intérêt général.

[6] Dans son ordonnance, le Conseil d'Etat analyse l'état de fait sous l'angle du risque de transfert des données personnelles vers les Etats-Unis à la lumière (1) du cadre contractuel agréé par les parties et (2) des mesures de surveillance à disposition des autorités américaines, lesquelles feraient fi des protections contractuelles agréées par les parties.[3]

1. Le risque de transfert vers les Etats-Unis à la lumière du cadre contractuel agréé

[7] Le Conseil d'Etat relève que, dans le cas d'espèce, les garanties suivantes sont prévues par la loi ou mises en place contractuellement :[4]

- Les données transférées dans le Health Data Hub sont pseudonymisées, puis chiffrées ;[5]
- Le GIP ne peut collecter (et donc le Health Data Hub ne peut contenir) que des données nécessaires à la poursuite d'une finalité d'intérêt public en lien avec l'épidémie de COVID-19 ;
- Les serveurs de Microsoft Ireland dédiés au Health Data Hub sont localisés dans l'UE (dans un premier temps aux Pays-Bas et par la suite en France) ;
- Microsoft s'engage contractuellement (engagement prévu dans un avenant au contrat) à ne pas traiter (y compris par le biais d'accès distants) les données hébergées en dehors de la zone géographique définie par le contrat (soit au sein de l'UE), sans l'approbation préalable du GIP ;
- Le GIP s'est engagé à l'égard de l'autorité française en matière de protection des données, la Commission nationale de l'informatique et des libertés (« CNIL »), à refuser tout transfert de données en dehors de la zone géographique définie contractuellement ; cet engagement est renforcé par un arrêté du Ministre de la santé interdisant le transfert en dehors de l'UE des données contenues dans le Health Data Hub.

[8] Sur la base des mesures énoncées ci-dessus, le Conseil d'Etat considère que les données personnelles relatives à la santé ne peuvent pas être transférées vers les Etats-Unis sur la base du contrat entre le GIP et Microsoft Ireland.

---

3 Conseil d'Etat, ordonnance N°444937 du 13 octobre 2020 (https ://www.conseil-etat.fr/actualites/actualites/health-data-hub-et-protection-de-donnees-personnelles-des-precautions-doivent-etre-prises-dans-l-attente-d-une-solution-perenne) (tous les sites web ont été consultés pour la dernière fois le 1er juin 2021).

4 Notamment par le code de la santé publique et l'arrêté du ministre de la santé du 10 juillet 2020, pris en application de ce dernier, instituant un GIP et prévoyant le traitement de données que celui-ci est autorisé à conduire.

5 Ceci nous renvoie à la notion de donnée personnelle au sens relatif ou absolu. En vertu de la définition « concrète » ou « relative » de la notion de données personnelles, ne sont considérées comme données personnelles que les informations qui permettent l'identification d'une personne physique, cette identification devant être possible en prenant en considération l'ensemble des moyens que le responsable de traitement, le destinataire ou un tiers est raisonnablement susceptible d'utiliser pour identifier la personne (cd. 26 RGPD). *A contrario* une appréciation « abstraite » ou « absolue » de la notion de données personnelles considère qu'en présence d'une possibilité théorique d'identification, l'information doit être considérée comme une donnée personnelle (Arrêt de la CJUE C-582/14 du 19 octobre 2016, §25 ; Philippe Meier/Nicolas Tschumy, L'adresse IP : une donnée personnelle ? Ou quand la CJUE rejoint le TF !, in : Jusletter 23 janvier 2017). Pour de plus amples développements sur l'appréciation de la notion de données personnelles en vertu de la notion relative ou absolue selon le droit européen et le droit suisse, nous vous renvoyons à l'article suivant : Célian Hirsch/Emilie Jacot-Guillarmod, Les données bancaires pseudonymisées – Du secret bancaire à la protection des données, in : RSDA 2/2020, p. 160ss.

[9] Le Conseil d'Etat requiert toutefois que le contrat avec Microsoft Ireland soit complété par un avenant précisant :

1. que Microsoft Ireland ne divulguera pas les données traitées aux pouvoirs publics, sauf si elle y est tenue *par le droit de l'UE ou celui de l'Etat Membre auquel elle est soumise* (nous mettons en évidence l'ajout ordonné) ;
2. que l'avenant interdisant à Microsoft Ireland de traiter les données du Health Data Hub en dehors de la zone géographique prévue par le contrat soit étendu à l'ensemble des services fournis par Microsoft Ireland et susceptibles d'être utilisés pour le traitement de données relatives à la santé (engagement jusqu'alors limité aux services « Azure »).

2. Le risque de transfert vers les Etats-Unis dans le cadre de mesures de surveillance à disposition des autorités américaines

[10] Les demandeurs font valoir que Microsoft Ireland et sa société mère Microsoft Corporation peuvent faire l'objet de demandes d'accès des autorités américaines dans le cadre de programmes de surveillance, quand bien même les données sont hébergées exclusivement dans l'UE. En effet, les engagements contractuels pris par Microsoft Ireland ne permettent pas de faire échec à ces mesures de surveillance étatiques.

[11] La CNIL, appelée à déposer des observations dans le cadre de la procédure de référé, estime qu'il n'est pas possible d'écarter complètement le risque (i) d'une telle demande d'accès des autorités américaines et (ii) d'un accès par Microsoft Ireland aux données sous-jacentes « en clair » (*clear text*) traitées dans le Health Data Hub en dépit du chiffrement et du stockage des clés de chiffrement.

[12] Le Conseil d'Etat relève ce qui suit :

- L'arrêt Schrems II analyse les conditions d'un transfert de données personnelles de l'UE vers les Etats-Unis et non leur traitement par une société de droit américain ou sa filiale sur le territoire de l'UE ;
- Les demandeurs ne font pas valoir une violation du RGPD,[6] mais un *risque* de violation si Microsoft Ireland ne pouvait pas s'opposer à une demande d'accès des autorités américaines ;
- Il existe un intérêt public important au traitement de données relatives à la santé dans le cadre de la lutte contre la pandémie de COVID-19 et les moyens techniques proposés par Microsoft Ireland en lien avec le Health Data Hub sont sans équivalent à ce jour.

[13] Sur la base de ce qui précède, le Conseil d'Etat retient que le traitement de données personnelles liées à la santé dans le Health Data Hub ne constitue pas une atteinte grave et mani-

6 Règlement général sur la protection des données du 27 avril 2016 (RGPD ; (UE) 2016/679).

festement illicite qui nécessiterait la mise en place (par l'autorité) de mesures d'urgence visant à éliminer tout risque, tout en étant proportionnées à l'intérêt public visé par le traitement.[7]

[14] Bien que la portée de cette ordonnance du Conseil d'Etat puisse être limitée au contexte dans lequel elle est rendue – soit (i) les données étaient pseudonymisées et chiffrées, (ii) un intérêt de santé publique important entrait en jeu et (iii) l'affaire était soumise à une procédure de référé qui vise des requêtes urgentes justifiées par une violation particulièrement grave d'une liberté fondamentale – il est tout de même important de noter que la plus haute juridiction administrative française considère que le risque d'un accès par les autorités américaines à des données personnelles traitées dans l'UE par une entité soumise à l'application extraterritoriale du droit américain constitue en quelque sorte un risque hypothétique, ou à tout le moins ne constitue pas une atteinte grave et manifestement illégale aux droits des personnes concernées. Le Conseil d'Etat considère en particulier que l'arrêt Schrems II ne traite pas de l'impact de la législation américaine régissant l'accès à des données par les autorités de surveillance américaines sur les données traitées dans l'UE par les entités européennes de groupes américains.

II. Aperçu des principaux enjeux du US Cloud Act

[15] L'ordonnance du Conseil d'Etat, pas plus que l'arrêt Schrems II, ne traitent directement de l'impact extraterritorial de la législation américaine en matière de droit d'accès des autorités de surveillance. Cet aspect est pourtant essentiel dans la mesure où un possible accès par les autorités américaines à des données personnelles soumises au RGPD ne ressort pas uniquement du transfert direct de celles-ci vers une société américaine, mais peut également résulter d'un transfert indirect lorsque le fournisseur de services basé dans l'UE auquel les données personnelles sont confiées appartient à un groupe de sociétés américain. En effet, alors même qu'il peut paraître sûr de confier des données personnelles à un fournisseur de services dont les serveurs se trouvent au sein de l'UE, avec la garantie contractuelle qu'aucun transfert n'est effectué vers les Etats-Unis, c'est sans compter l'application extraterritoriale de la législation américaine en matière de surveillance. Pour mieux comprendre les risques liés au choix d'un sous-traitant faisant partie d'un groupe de sociétés soumis au droit américain, nous analysons brièvement l'une de ces lois dont l'application dépasse le territoire américain et qui s'applique aux fournisseurs de services *cloud* : le *US Cloud Act*.

---

7 Le Conseil d'Etat est par ailleurs arrivé à une conclusion similaire dans un arrêt plus récent en lien avec la plateforme Doctolib, dans lequel il considère que le niveau de protection des données apporté par les mesures mises en œuvre (principalement les mêmes que celles analysées dans l'arrêt ici commenté, soit : garanties contractuelles, en particulier une procédure précise en cas de demandes d'accès par une autorité publique, et chiffrement des données) ne pouvait être considéré comme manifestement insuffisant au regard de la nature des données personnelles (lesquelles n'ont pas été considérées comme des données relatives à la santé) et le risque encouru (Ordonnance N°450163 du Conseil d'Etat du 12 mars 2021). Par contre, l'autorité portugaise de protection des données (*Comissão Nacional de Proteção de Dados*, CNPD) a récemment ordonné à l'Institut National de la Statistique de mettre un terme au transfert vers les Etats-Unis de données personnelles collectées dans le cadre d'une opération de recensement (Censos 2021), un tel transfert intervenant par le biais du recours à une société américaine (Cloudflare, Inc.) en charge de la gestion de la plateforme en ligne. L'autorité a ordonné la suspension immédiate (dans les 12 heures) de tout transfert vers les Etats-Unis, ou tout autre Etat ne fournissant pas une protection adéquate, prenant notamment en compte le fait que les données concernées comprenaient des données sensibles en lien avec la santé ou la religion (Décision 533/2021 du 27 avril 2021, disponible au lien suivant : https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_fr).

[16] Le *US Cloud Act* est venu modifier et compléter le *Stored Communications Act* (« SCA ») en prévoyant qu'un fournisseur de services *cloud* soumis au droit américain peut être obligé à produire des données hébergées sur ses serveurs, sans égard à la localisation géographique de ceux-ci et indépendamment du fait que le client du fournisseur dont les données sont requises soit ou non soumis à la législation américaine.[8]

[17] Ceci signifie que lorsque le fournisseur de services *cloud* est soumis à la juridiction des Etats-Unis, les autorités américaines peuvent, sous certaines conditions (voir ci-dessous), demander à celui-ci de produire des données en sa possession ou traitées par ses filiales, y compris lorsque ces filiales sont situées en dehors des Etats-Unis.

[18] Une telle demande d'accès doit :

1. être basée sur une décision d'une autorité (*warrant*, *grand jury subpoena* ou *SCA court order*) ;
2. la juridiction qui émet la décision doit être compétente à l'égard de la société requise ;
3. la société requise doit être en possession, avoir la garde ou bénéficier d'un contrôle sur les données requises.

[19] Lorsque les données requises concernent des personnes qui ne sont pas des ressortissants ou des résidents aux Etats-Unis, le fournisseur de services *cloud* peut s'opposer à une demande d'accès basée sur le US Cloud Act en faisant valoir qu'un tel transfert de données l'obligerait à violer la législation d'un Etat étranger à laquelle il est soumis et avec lequel les Etats-Unis ont conclu un accord bilatéral sur l'accès à des données par un gouvernement étranger. Cette opposition dépend donc du fournisseur de services *cloud*.

[20] Une demande d'accès en vertu du US Cloud Act par les autorités américaines peut prendre différentes formes (*warrant*, *grand jury subpoena* ou *SCA court order*) en fonction des informations recherchées et des entités requérantes, chacune répondant à des critères différents :

- Ainsi, lorsque la demande d'accès est émise par le biais d'un *warrant*, l'autorité requérante doit démontrer (i) que la demande est fondée sur une *probable cause* (c'est-à-dire démontrer qu'une infraction spécifique a été commise – selon une forte probabilité s'il s'agit d'un crime – et que les données requises contiennent des preuves de celle-ci) et (ii) que la demande d'accès rempli le critère de spécificité (c'est-à-dire qu'elle décrit précisément les données requises, lesquelles doivent être pertinentes et importantes dans le cadre de l'enquête pénale). Seule la forme du *warrant* peut permettre à l'autorité requérante de demander l'accès à des données relatives au ***contenu*** de communications des utilisateurs sans que ceux-ci ne soient notifiés d'une telle requête.
- A l'inverse, une *grand jury subpoena* peut être fondée sur la « simple possibilité » qu'une infraction à la loi ait été commise et à la condition que le champ des données requises ne soit pas trop large, rendant la demande déraisonnable ou abusive. Les critères sont donc plus souples, par contre le type de données auquel une telle demande peut prétendre se

8 Caitlin Potratz Metcalf/Peter Church, U.S. CLOUD Act and GDPR – Is the cloud still safe ?, Linklaters (https ://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe).

limite à des informations générales sur les utilisateurs, *à l'exclusion d'informations sur le contenu des communications*.

[21] Il convient de noter que le client du fournisseur de services *cloud* qui n'est pas soumis au droit américain ne peut pas s'opposer à une demande d'accès formulée par les autorités américaines auprès du fournisseur de services *cloud*. C'est donc à ce dernier de s'opposer, lorsque le droit applicable lui en donne la possibilité, à une demande d'accès des autorités américaines. Microsoft a réagi rapidement à l'arrêt Schrems II en publiant le 19 novembre 2020[9] une modification de ses termes contractuels et en prévoyant un engagement, à sa charge, de contester toute demande d'accès des autorités à des données personnelles provenant de l'UE lorsque la loi le permet.[10]

[22] En considérant l'application très large du US Cloud Act qui permet aux autorités américaines d'accéder à des données de personnes situées dans l'UE (ou en Suisse), hébergées et traitées exclusivement sur des serveurs situés dans l'UE (ou en Suisse), au motif qu'elles sont traitées par une société américaine, ou une filiale d'un groupe américain, on comprend mieux le risque de transfert indirect de données de ressortissants européens (ou suisses) vers les Etats Unis, indépendamment des termes contractuels prévus par les parties. Cependant, il convient de garder à l'esprit qu'il ne s'agit en aucun cas d'un accès libre et automatique par les autorités américaines, mais que celles-ci doivent déposer une demande d'accès motivée par la présomption d'une infraction, que cette demande est revue par une autorité qui statue sur son bien-fondé et, bien entendu, que de telles demandes d'accès ne peuvent être faites qu'à l'égard de sociétés qui ont un lien avec les Etats-Unis (par exemple dont la société mère est aux Etats-Unis, ou qui sont soumises à la législation américaine sur le blanchiment d'argent).[11]

[23] Le seul moyen, pour une société suisse ou européenne qui souhaite transférer des données à un fournisseur de service *cloud* soumis d'une manière ou d'une autre au droit américain, de s'assurer qu'aucune donnée personnelle ne soit transmise ou rendue accessible aux autorités de surveillance américaines est de faire en sorte que ce fournisseur ne soit pas en possession, ait la garde ou bénéficie d'un contrôle sur les données personnelles (ce qui permet de faire obstacle à la troisième condition pour l'octroi d'une demande d'accès). Une telle assurance ne peut passer que par la mise en œuvre de mesures techniques sûres permettant le cryptage ou la pseudonymisation des données personnelles et à condition que la clé de cryptage, respectivement les informations permettant la réidentification de la personne, ne soient pas en possession du fournisseur de services ou toute autre entité soumise au droit américain.[12] De telles mesures ne sont bien entendu pas possibles si le fournisseur de services a besoin des données personnelles « en clair » (*clear text*) pour rendre le service.

---

9 Communication sur le site internet de Microsoft du 19 novembre 2020 (https ://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/).

10 Cette communication dispose notamment : « *We are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so* ». Microsoft va même plus loin en s'engageant à indemniser les personnes concernées dont les données personnelles auraient été transmises aux autorités en violation du RGPD : « *we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR)* ».

11 François Charlet, Non, le CLOUD Act n'est pas ce que vous croyez. Vraiment pas, 23 août 2020 (https ://francoischarlet.ch/2020/cloud-act-pas-ce-que-vous-croyez/).

12 Il s'agit des seules mesures préconisées par le Comité Européen à la Protection des Données dans ses Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 novembre 2020 (disponibles uniquement en anglais à ce jour).

III. Impact de cette décision pour un responsable de traitement localisé en Suisse qui a recours à un cloud

[24] Les développements qui précèdent ont bien entendu un impact sur les sociétés suisses qui souhaitent avoir recours aux services d'une société américaine, ou appartenant à un groupe américain, pour stocker ou traiter des données personnelles dans un *cloud* (soit la majorité des fournisseurs de service *cloud* à ce jour).

[25] Au même titre que le RGPD, la LPD[13] interdit tout transfert de données personnelles vers un pays non-conforme, à moins que des garanties supplémentaires (dont les principales et plus utilisées sont les Clauses Modèles de la Commission Européennes ou celles publiées par le Préposé fédéral à la protection des données et à la transparence, le « Préposé »)[14] ne soient mises en place. Par ailleurs, le Préposé a repris, en droit suisse, l'analyse de la CJUE dans l'arrêt Schrems II en invalidant le Swiss-US Privacy Shield au motif qu'il n'assurait pas un niveau de protection adéquat pour les personnes concernées en vertu de la LPD, et en jugeant que les Clauses Modèles n'étaient pas suffisantes à garantir cette protection lorsque l'importateur de données n'était pas en mesure de s'y conformer à cause des exigences de divulgation prévues par son droit national.[15]

[26] La nouvelle mouture de la LPD (adoptée le 25 septembre 2020 et dont l'entrée en vigueur est prévue pour 2022/2023) n'apporte pas de véritables changements à cet égard et le Préposé, respectivement les tribunaux suisses, seront très certainement amenés à interpréter la loi suisse à la lumière des arrêts de la CJUE et des lignes directrices du Comité Européen à la Protection des Données, si la Suisse entend conserver la décision d'adéquation de la Commission Européenne dont elle bénéficie encore à ce jour.

[27] En plus des aspects liés à la protection des données évoqués ici, les banques qui souhaitent avoir recours à un fournisseur de service *cloud* devront également prendre en compte les exigences règlementaires et liées au secret bancaire qui sont développées dans un autre article auquel nous renvoyons.[16]

IV. Conclusion

[28] Sur la base des développements qui précèdent, on s'aperçoit que la légalité d'un transfert de données personnelles vers un Etat tiers réputé « non adéquat » (dans la perspective des règles en matière de protection des données) dépend réellement des circonstances factuelles de ce transfert et donc d'une analyse au cas par cas passant par (i) l'examen approfondi du droit, et même de la pratique, du pays de destination (ex : ingérence des autorités de surveillance, droits des personnes concernées et possibilité de mise en oeuvre effective de ceux-ci), (ii) l'identification précise du besoin d'accès du fournisseur aux données transférées pour rendre le service (accès aux données en clair nécessaire ou non) et sur cette base, (iii) la mise en place des mesures de sécurité

13 Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; RS 235.1).

14 Contrat-type pour l'externalisation (*outsourcing*) du traitement de données à l'étranger, disponible sur le site du Préposé fédéral à la protection des données et à la transparence.

15 Prise de position du Préposé du 8 septembre 2020 sur la transmission de données personnelles vers les États Unis et d'autres États n'offrant pas un niveau adéquat de protection des données au sens de l'art. 6, al.1 LPD.

16 Philipp Fischer/Marine Largant, On Cloud Number Nine : un bref survol des enjeux juridiques et règlementaires du cloud banking, 12 novembre 2020 (www.swissprivacy.law/27).

appropriées (ex : anonymisation, pseudonymisation, chiffrement) et (iv) des garanties contractuelles nécessaires avec le fournisseur de services (ex : engagement du fournisseur de s'opposer, dans les limites du droit applicable, à toute demande d'accès des autorités ; obligation d'information du responsable de traitement avant tout transfert de données à des autorités ; obligation préalable d'information par le fournisseur lorsque son droit national ne lui permet pas de remplir ses obligations en vertu du contrat ou des Clauses Modèles).

[29] Il n'y a donc pas de solution *one size fits all* et le recours aux Clauses Modèles en matière de protection des données, qui étaient jusqu'à l'arrêt Schrems II largement utilisées sans analyse plus approfondie du système juridique de l'Etat de destination, devra être complétée par des garanties supplémentaires, techniques, contractuelles et/ou organisationnelles, en fonction du risque qu'il convient de couvrir. Le responsable du traitement pourra même être amené à conclure à l'impossibilité de contracter avec un fournisseur ou à la nécessité de mettre un terme au transfert de données personnelles vers certaines juridictions afin d'assurer la conformité avec les exigences du RGPD et de la LPD.

Me Marine Largant est collaboratrice au sein de l'Etude d'avocats OBERSON ABELS SA. Après une carrière débutée au sein d'une *Big4*, elle est aujourd'hui inscrite au barreau de Genève et spécialisée en droit des sociétés et de la protection des données.

Me Philipp Fischer, LL.M. (Harvard), est associé fondateur de l'Etude d'avocats OBERSON ABELS SA. Il est spécialisé en droit bancaire et financier, ainsi qu'en droit de la protection des données. Il est responsable du module « Protection des données » dans le cadre du *CAS Digital Finance Law* de l'Université de Genève.