

Le Conseil d'Etat refuse de suspendre le partenariat de l'Etat avec Doctolib hébergé par Amazon

Par une ordonnance du 12 mars 2021, le Conseil d'Etat a refusé de suspendre le partenariat établi entre l'Etat et Doctolib dans le cadre de la campagne de vaccination contre le Covid-19.

Les requérants avaient demandé cette suspension en référé, soutenant que les garanties apportées par Amazon Web Services (AWS) pour l'hébergement des données étaient insuffisantes.

Dans le cadre de la campagne de vaccination contre la covid-19, l'Etat français a confié la gestion des rendez-vous de vaccination sur internet à différents prestataires dont la société Doctolib.

Doctolib est une société de droit français qui propose un service de gestion en ligne des consultations pour les professionnels de santé et un service de prise de rendez-vous en ligne pour les patients. Pour les besoins de l'hébergement de ses données, elle a recours aux prestations d'une société de droit luxembourgeois AWS Sarl, filiale de la société de droit américain AWS Inc.

Les requérants ont alors demandé au juge des référés, statuant sur le fondement de l'article L. 521-2 du code de justice administrative^[1], de suspendre le partenariat de l'Etat français avec la société Doctolib au motif qu'il repose sur un hébergement des données de santé auprès d'une société américaine le rendant incompatible avec le règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit règlement général sur la protection des données (RGPD).

Selon le RGPD, les responsables de traitement et les sous-traitants peuvent transférer des données hors de l'Union européenne (UE) et de l'Espace économique européen (EEE) à condition d'assurer un niveau de protection des données suffisant et approprié.

Concrètement, ils doivent encadrer ces transferts en utilisant les différents outils juridiques définis au chapitre V du règlement :

- les transferts hors UE peuvent être fondés sur une décision d'adéquation de la Commission européenne concernant certains pays assurant un niveau de protection adéquat ;
- en l'absence d'une telle décision, les transferts peuvent être fondés sur des garanties appropriées, telles les clauses contractuelles types (CCT) de la Commission européenne, des règles d'entreprise contraignantes (binding corporate rules en anglais), des clauses contractuelles spécifiques.

Or, la Cour de justice de l'Union européenne (CJUE) a rendu le 16 juillet 2020 un arrêt majeur^[2] concernant les transferts de données entre l'UE et les États-Unis dans l'affaire dite « Schrems II ».^[3]

Par cet arrêt, elle a invalidé la décision d'adéquation « Privacy Shield », adoptée en 2016 par la Commission européenne suite à l'invalidation du « Safe Harbor », qui permettait le transfert de données entre l'Union européenne et les opérateurs américains adhérant à ses principes de protection des données sans autre formalité.

C'est dans ce contexte que les requérants ont demandé la suspension du partenariat avec Doctolib, en raison des risques que cette situation comporte au regard du droit au respect de la vie privée, compte tenu de possibles transferts de données vers les États-Unis.

Le juge s'est saisi de la question bien que (i) AWS Sarl soit une société de droit luxembourgeois, (ii) AWS Sarl soit certifiée « hébergeur de données de santé » en application de l'article L. 1111-8 du code de la santé publique, (iii) les données soient hébergées dans des centres de données situés en France et en Allemagne et (iv) le contrat conclu entre la société Doctolib et AWS Sarl ne prévoit pas le transfert de données pour des raisons techniques aux États-Unis. Pour lui, du fait de sa qualité de filiale d'une société de droit américain, la société AWS Sarl peut faire l'objet de demandes d'accès à certaines données de santé par les autorités américaines, dans le cadre de programmes de surveillance. Ce qui justifie de vérifier le niveau de protection assuré lors du traitement des données. C'est une application très extensive du droit européen post-Schrems II.

Pour y répondre, il a dû déterminer concrètement si le niveau de protection assuré lors du traitement des données – en prenant en considération notamment les stipulations contractuelles convenues entre Doctolib et AWS Sarl – était suffisant. Il a conclu que « le niveau de protection des données de prise de rendez-vous dans le cadre de la campagne de vaccination contre la Covid-19 ne peut être regardé comme manifestement insuffisant au regard du risque de violation du règlement général de protection des données » pour les motifs suivants :

- données en cause : « Les données litigieuses comprennent les données d'identification des personnes et les données relatives aux rendez-vous mais pas de données de santé sur les éventuels motifs médicaux d'éligibilité à la vaccination, les personnes intéressées se bornant, au moment de la prise de rendez-vous, à certifier sur l'honneur qu'elles entrent dans la priorité vaccinale, qui est susceptible de

SOULIER BUNCH

concerner des adultes de tous âges sans motif médical particulier » ;

- durée de conservation : *« Ces données sont supprimées au plus tard à l'issue d'un délai de trois mois à compter de la date de rendez-vous, chaque personne concernée ayant créé un compte sur la plateforme pour les besoins de la vaccination pouvant le supprimer directement en ligne » ;*
- gestion des demandes d'accès par les autorités américaines : Doctolib et AWS Sarl ont conclu un addendum complémentaire prévoyant notamment *« la contestation de toute demande générale ou ne respectant pas la réglementation européenne » ;*
- mesure de sécurité : Doctolib a mis *« en place un dispositif de sécurisation des données hébergées par la société AWS par le biais d'une procédure de chiffrement reposant sur un tiers de confiance situé en France afin d'empêcher la lecture des données par des tiers ».*

Pour ces raisons, il a conclu à l'absence d'*« atteinte grave et manifestement illégale au droit au respect de la vie privée et au droit à la protection des données personnelles ».*

[1] Le référé liberté permet de demander au juge de prendre en urgence une mesure nécessaire à la sauvegarde d'une liberté fondamentale si l'administration y porte atteinte de manière grave et illégale.

[2] <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf>

[3] Cf. notre article intitulé [Transfert international de données vers les Etats-Unis - La Cour de justice de l'Union européenne invalide le Privacy Shield](#) publié sur notre Blog en août 2020

Soulier Bunch est un cabinet d'avocats pluridisciplinaire proposant aux différents acteurs du monde industriel, économique et financier une offre de services juridiques complète et intégrée.

Nous assistons nos clients français et étrangers sur l'ensemble des questions juridiques et fiscales susceptibles de se poser à eux tant dans le cadre de leurs activités quotidiennes qu'à l'occasion d'opérations exceptionnelles et de décisions stratégiques.

Chacun de nos clients bénéficie d'un service personnalisé adapté à ses besoins, quels que soient sa taille, sa nationalité et son secteur d'activité.

Pour plus d'informations, visitez soulierbunch.com.

Le présent document est fourni exclusivement à titre informatif et ne saurait constituer ou être interprété comme un acte de conseil juridique. Le destinataire est seul responsable de l'utilisation qui pourrait être faite des informations qu'il contient.