Les implications d'un Brexit «dur» sur le transfert de données vers le Royaume-Uni

les faits **Le Royaume-Uni deviendra bientôt un pays tiers à l'Union européenne et, à l'instar de la Chine ou de la Russie, tous les transferts de données vers cette destination seront soumis à des exigences renforcées au regard du RGPD. L'occasion de rappeler les règles applicables et les outils existants pour sécuriser le transfert de données vers un pays tiers.**

Le 29 mars prochain, en l'absence d'accord, le Royaume-Uni quittera l'Union sans aucune concession. Ce Brexit « dur » aura des répercussions importantes sur les échanges commerciaux avec les Britanniques, limitant non seulement les flux de marchandises, mais aussi ceux de données. En effet, le RGPD exige des mesures ad hoc en cas de transfert de données hors UE. Car les entreprises courent le risque que leurs données soient utilisées sans limites, au détriment de leur e-réputation. Afin de leur faciliter la tâche, le RGPD prévoit que des « décisions d'adéquation » adoptées par la Commission européenne confèrent aux États une présomption de protection équivalente. Il est alors autorisé de transférer des données vers ces États aux mêmes conditions que s'ils faisaient partie de l'UE. Pour l'heure, treize pays font l'objet d'une décision d'adéquation, dont les États-Unis, le Japon, le Canada ou la Suisse. La question est de savoir si le Royaume-Uni les rejoindra rapidement une fois sorti de l'Union. Tout dépend du sort que connaîtra alors le Data Privacy Act, transposant le RGPD dans la législation nationale. En attendant que la Commission se prononce sur la législation britannique, il ne pourra y être transféré de données sans certaines

Me Pierre-Randolph Dufau
Avocat à la cour
Fondateur de la SELAS PRD avocats

modalités. En effet, lorsque le transfert n'est pas fondé sur une décision d'adéquation, il est autorisé moyennant des garanties appropriées. Plusieurs outils sont cités par le RGPD : contrats, codes de conduite, certifications… Il incombe à la société transmettant les données d'adopter ces mécanismes afin de réduire le risque de violation ultérieure au transfert. Pour une parfaite conformité, il convient d'utiliser des standards approuvés par la Commission et/ou la Cnil, notamment les clauses contractuelles types qui sont à disposition. Il peut être privilégié le recours à un code de conduite approuvé par une autorité compétente, lequel permet d'expliquer plus en détail les enjeux de la protection des données dans un secteur spécifique. Même chose pour les règles d'entreprise contraignantes, qui s'appliquent, elles, au sein d'un groupe (elles sont en vigueur dans une centaine de multinationales actuellement, dont Salesforce et HPE). Mais que les engagements prennent la forme d'une clause contractuelle, d'une annexe, d'un code de conduite ou d'un accord de groupe, elles doivent être lues et signées par les parties pour obtenir une réelle force obligatoire. Il est donc important de s'assurer que les outils sont en place, qu'ils ont été signés, pour qu'ils présentent des garanties suffisantes au transfert hors UE aux yeux de la Cnil. Cela n'implique pas pour autant de se dispenser du consentement de la personne concernée au transfert. Celui-ci n'est licite que si les conditions fondamentales applicables à tous les traitements sont respectées par ailleurs. ■

ce qu'il faut retenir **Les DSI doivent se préparer au Brexit en sécurisant tous les transferts de données qu'ils effectuent vers le Royaume-Uni et en utilisant de préférence les outils mis à disposition sur les sites internet de la Commission européenne et de la Cnil.**

Règlement européen sur le commerce en ligne

Le 19 février dernier, le Conseil de l'Union européenne a entériné, avec le Parlement européen, un projet de règlement visant à encadrer le commerce en ligne. Il promeut une plus grande transparence visant à assurer une concurrence loyale et renforce le droit des consommateurs en instaurant des voies de recours efficaces et simplifiées, notamment pour faciliter la résiliation de leurs contrats.

Mise en conformité justifiant le retrait d'une mise en demeure de la Cnil

Le 17 octobre 2018, des sociétés d'assurance du groupe Malakoff Médéric et Humanis avaient été mises en demeure par la Cnil pour détournement de finalité des données de leurs assurés. Était ainsi mise en cause l'utilisation de données de pensionnaires de retraite à des fins de prospection commerciale. Après un nouveau contrôle, la Cnil a pu constater que les manquements avaient cessé et a donc clôturé le dossier en février dernier.

Google condamné pour utilisation abusive de données personnelles

Par un jugement du 12 février dernier, le TGI de Paris a déclaré abusives 38 clauses des conditions générales et de la politique de confidentialité de Google. Contraint d'accepter ces clauses pour accéder au service du moteur de recherche, en apparence gratuit, l'utilisateur voyait en réalité ses données personnelles commercialisées, notamment à des fins de publicité ciblée, sans jamais y consentir.