BREXIT, RGPD ET LA CHRONOLOGIE DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

Date: 20 Janvier 2021

Alerte française en Droit de la Propriété Intellectuelle et des Nouvelles Technologies

By: Claude-Étienne Armingaud

Le 1er janvier 2021, la période de transition du Brexit (Période de Transition) est enfin arrivée à terme et le Royaume-Uni a officiellement finalisé sa sortie de l'Union européenne (UE). L'accord commercial post Brexit (Accord) négocié à la dernière minute devrait permettre une transition plus douce sur le plan de la protection des données, dans la mesure où le Règlement Général sur la Protection des Données (RGPD)[1] a cessé d'être directement applicable au Royaume-Uni. Il a également été accordé au Royaume-Uni une période de grâce de six mois afin de négocier une décision d'adéquation qui permettrait le libre transfert de données personnelles de l'UE vers le Royaume-Uni.

Si le Comité Européen de la Protection des Données (CEPD) a modifié le 13 janvier 2021 ses Communications sur le Brexit[2] à la suite de l'Accord (Communications), il ne s'est cependant penché que sur:

- La question des transferts de données de l'UE vers le Royaume-Uni;
- La fin du mécanisme dit de « guichet unique » pour le Royaume-Uni; et
- La nécessité pour les entités britanniques qui seraient soumises au RGPD de désigner un représentant conformément à l'article 27 RGPD.

En outre, à part acter la fin du mécanisme de guichet unique et affirmer que « l*e CEPD a entretenu des relations avec l'ICO [Information Comissioner's Office, l'Autorité de Surveillance du Royaume-Uni] au cours des derniers mois afin de permettre une transition en douceur vers cette nouvelle situation en veillant à ce que les autorités de l'EEE suivent une approche partagée et efficace dans le traitement des plaintes existantes et des affaires transfrontalières impliquant l'ICO, tout en minimisant les retards et les éventuels désagréments pour les plaignants concernés* », le CEPD n'a fait aucun commentaires sur la manière dont une telle collaboration pourra se dérouler efficacement pour les entreprises dont l'Autorité de Surveillance chef de file était jusqu'alors l'ICO.

Cela est d'autant plus pertinent pour les violations de données à caractère personnel, qui étaient le fondement des amendes les plus importantes adoptées par l'ICO sous l'égide du RGPD avant le Brexit. Bien que le cadre général soit sensiblement le même entre le RGPD et son équivalent britannique, qui l'a transposé en droit national britannique (UK GDPR), la scission des régimes applicables pourraient obliger les entreprises à se conformer à des engagements réglementaires supplémentaires.

Dans le cadre du RGPD et de sa version britannique, les entreprises sont supposées notifier à leur Autorité de Surveillance compétente toute violation qui créerait des « *risques* » pour les personnes concernées dans les 72

heures à compter de la connaissance d'une telle violation, ainsi que d'informer ces mêmes personnes des risques lorsque ceux-ci sont considérés comme « *élevés* ».

Différents scénarios peuvent se produire, en fonction (i) du moment où la violation de données à caractère personnel s'est produite et (ii) du moment de la notification à une Autorité de Surveillance:

- La violation et la notification ont eu lieu avant la fin de la Période de Transition (Scénario 1);
- La violation s'est produite avant la fin de la Période de Transition, mais la notification a eu lieu dans les 72 heures, postérieurement à la Période de Transition (Scénario 2); ou
- La violation et la notification ont eu lieu postérieurement à la Période de Transition (Scénario 3).

Les trois scénarios peuvent être appliqués à des situations dans lesquelles les entreprises sont désormais soumises à la fois au RGPD et au UK GDPR (par exemple, la violation s'est produite au Royaume-Uni mais le RGPD serait également applicable à la suite de la Période de Transition, ou la violation s'est produite dans l'UE mais le UK GDPR serait également applicable à la suite de la Période de Transition).

Selon les Communications, le Scénario 1 serait le plus simple: une procédure était déjà en cours et notifiée à l'Autorité de Surveillance alors compétente. Il est prévu que l'ICO et ses homologues européens, sous la coordination du CEPD, coopèrent pour traiter, enquêter et, le cas échéant, poursuivre ces affaires. Cependant, les entreprises ne devraient pas avoir besoin d'étapes supplémentaires pour être conformes aux deux régimes.

De même, le Scénario 3 devrait, en théorie, être suffisamment clair. Étant donné que la violation et sa notification se sont produites après la Période de Transition, les entreprises devront évaluer si elles sont exclusivement soumises à l'un des régimes (RGPD ou UK GDPR), ou si les deux régimes sont applicables simultanément. Dans ce dernier cas, et en raison de la fin du mécanisme de guichet unique, les entreprises devront notifier leur violation de données à caractère personnel à la fois à l'ICO et à l'Autorité de Surveillance chef de file compétente dans l'UE.

Idéalement, la question de savoir quelle Autorité de Surveillance de l'UE est compétente en tant que chef de file aurait dû se poser avant la fin de la Période de Transition et un représentant dans l'UE, conformément à l'article 27 RGPD, aurait dû être désigné. L'État membre de l'UE dans lequel ce représentant a été nommé devrait, en tout état de cause, permettre un alignement pour l'Autorité de Surveillance chef de file de l'UE compétente pour les violations de données.

Cependant, des instructions supplémentaires de l'ICO et/ou du CEPD auraient été les bienvenues pour le Scénario 2 - dans lequel la violation s'est produite avant la fin de la Période de Transition, mais la notification a eu lieu dans les 72 heures, postérieurement à la Période de Transition.

Outre les déclarations du CEPD dans ses Communications, l'ICO a elle-aussi affirmé que même si elle « *ne fait plus partie du mécanisme de guichet unique* », elle « *continuerait de coopérer et de collaborer avec les autorités de surveillance européennes, comme nous l'avons fait avant le RGPD et le mécanisme de guichet unique, concernant toute violation du RGPD qui affecte des personnes au Royaume-Uni et dans d'autres États de l'UE et de l'EEE.* ». Cependant, à part fournir des conseils sur la manière dont les notifications devraient être effectuées après la Période de Transition, l'ICO n'a communiqué aucun élément concret concernant la chronologie des violations de données.

Étant donné le court délai imparti pour notifier une violation, un nombre limité d'événements pourrait être impliqué. Cependant, comme ce délai commence à courir à partir du moment où le responsable de traitement a connaissance de la violation, les cas pourraient être plus importants.

En effet, en vertu du RGPD (article 33 du RGPD) et du RGPD britannique (article 67 du UK GDPR), la violation elle-même est l'événement qui déclenche l'exigence de notification. En tant que tel, toute violation survenue avant la fin de la Période de Transition devrait être exclusivement soumise au RGPD, qu'elle ait été découverte avant ou après la fin de la Période de Transition. En conséquence, les entreprises britanniques devraient être en mesure de notifier leurs violations de données à caractère personnel à l'ICO, qui assurerait ensuite la liaison avec ses homologues (et vice versa pour la notification à une Autorité de Surveillance de l'UE), dans le cadre du mécanisme de coopération détaillé pour le Scénario 1.

Cliquezici pour lire la version originale en anglais.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

