Option Finance

N° 1597
lundi 8 au dimanche 14 mars 2021
Pages 48-49
1372 mots - 5 min

Garanties de passif et due diligences à l'heure du RGPD : points d'attention et enjeux

L'arrivée du Règlement européen pour la protection des données personnelles en 2016 constitue un véritable bouleversement pour les entreprises et pour les gouvernances qu'elles doivent mettre en œuvre. En matière de privacy, rien n'existait de manière européenne, voire mondiale, qui permettent de mettre de manière opérationnelle au centre des business models la question de la vie privée et des données personnelles. Pourtant, après, voire même avant les ressources humaines et les finances, les data sont les plus essentielles aux performances des entreprises, quel que soit leur objet et leur taille. En conséquence, toutes les opérations de haut de bilan devraient se focaliser sur la manière dont les questions de protection des données personnelles sont prises en compte. A défaut, c'est une des gouvernances les plus essentielles qui fera l'objet d'une sanction de la part des autorités, des marchés ou des salariés.

Quel que s chiffres clés permettent de rappeler l'importance de la réglementation sur la protection des données personnelles. En France, il y a eu 3 459 signalements auprès de la CNIL depuis le 25 mai 2018, date d'entrée en application du RGPD et, rien qu'en 2020, le montant total des sanctions s'est élevé à 138,9 millions d'euros.

Le 26 novembre 2020, la CNIL a par exemple prononcé une amende de 3,05 millions d'euros à l'encontre de Carrefour France et de Carrefour Banque pour de nombreux manquements au RGPD, en matière de sécurité des traitements, de collecte des données et de transparence vis-à-vis des personnes concernées.

Les sanctions prévues à l'article 83 du RGPG peuvent atteindre 4 % du chiffre d'affaires mondial de la société, et les condamnations prononcées dans les différents pays se rapprochent de plus en plus de ce plafond.

Une non-conformité est souvent révélatrice de mauvaise transparence auprès des personnes concernées et de failles de sécurité profondes dans les systèmes d'information. Outre les sanctions et le préjudice d'image, les coûts de (re)mise en état sont importants et donc extrêmement coûteux, spécialement dans le cadre d'une acquisition de sociétés.

Marriott International en a fait l'amère expérience lors de son acquisition de Starwood Hotels en 2016 pour plus de 12 milliards de dollars. Elle s'est vue sanctionnée d'une amende de 99 millions de livres par l'autorité de contrôle anglaise (ICO), pour une faille découverte deux ans après l'acquisition de la cible portant sur des faits antérieurs à celle-ci.

La digitalisation croissante de l'économie rend les actifs incorporels de plus en plus importants et parmi eux les données sont souvent au centre même de l'activité.

C'est le cas dans tous les domaines, mais peut-être plus particulièrement dans le domaine de la santé (bio et medtech), des fintech et du e-commerce. Les due diligences portant sur les traitements des données sont donc encore plus particulièrement cruciales dans ces secteurs.

1. Que faut-il vérifier et comment se garantir ?

Tout d'abord, un point d'attention relativement périphérique consiste à s'interroger sur le processus de data-room lui-même. Il est important de vérifier dans le règlement de data room et l'accord de confidentialité (le NDA) que les données personnelles partagées ont été collectées conformément au RGPD et ne seront pas partagées en dehors de l'espace économique européen (EEE).

Les données personnelles doivent être réduites à ce qui est strictement nécessaire et une anonymisation des documents doit être envisagée. Une attention particulière doit être portée aux données « sensibles » et aux transferts internationaux.

Rappelons que les sous-traitants, fournisseurs de data-room virtuels, sont soumis à l'article 28 du RGPD et que la clause de sous-traitance doit donc être conforme à celui-ci.

Une vigilance particulière est nécessaire en matière de fourniture d'accès à la data-room, les personnes devant être localisées dans les pays pertinents ayant besoin de recueillir l'information et ne soulevant pas de problème de transferts internationaux en dehors de l'EEE.

En ce qui concerne la revue de la cible elle-même, les principaux points d'attention sont les suivants : – la question de la conformité au RGPD a-t-elle fait l'objet d'un véritable projet interne, de manière transverse et sous la responsabilité d'un pilote, idéalement DPO ?

– quel est le niveau d'exhaustivité de la cartographie des traitements de données, entité par entité, direction par direction ?

– le registre obligatoire des traitements de données est-il conforme à l'article 30 du RGPD et décrit-il suffisamment toutes les mesures juridiques, organisationnelles et techniques permettant de limiter les impacts négatifs pour les personnes concernées ?

– l'ensemble de la documentation formant l'accountability de l'entreprise est-elle conforme et à jour, de sorte que l'entreprise puisse à tout moment justifier de sa conformité auprès de ses salariés, prestataires et clients et auprès de l'autorité de contrôle ?

– l'entreprise est-elle en mesure de gérer les demandes d'exercice de droits ainsi que les éventuelles failles de sécurité ?

– les politiques internes, processus et registres sont-ils digitalisés avec un logiciel métier de pilotage de la conformité RGPD, de manière à être pérennes et de pouvoir maintenir durablement et facilement l'entreprise en conformité avec ses obligations ? Une des premières actions qui pourrait ainsi être prise lors de l'audit serait de vérifier l'existence et la conformité de la documentation : politique de confidentialité des sites web, politique de gestion des cookies et traceurs, politique de sécurité des systèmes d'information (PSSI), recueil des preuves de consentement, registre des analyses d'impact relatives à la protection des données, justificatifs de la conformité des différents logiciels utilisés (notamment en matière de ressources humaines, de surveillance et de géolocalisation), etc.

Les contrats de sous-traitance conclus par la cible doivent également être passés au crible du RGPD. Ces derniers doivent avoir été mis à jour pour garantir le respect, par l'ensemble des sous-traitants, de leurs obligations au titre de l'article 28 du RGPD. S'il s'agit de sous-traitants basés au sein d'un pays tiers à l'Espace économique européen, des garanties supplémentaires doivent avoir été mises en place, telles que la conclusion de clauses contractuelles types.

2. Quelles sont les garanties applicables ?

La conformité au RGPD entre dans le cadre des déclarations et garanties de conformité à la loi et aux diverses réglementations, au même titre que par exemple les déclarations fiscales, sociales ou environnementales.

Elle doit cependant être spécifiquement visée et plus la déclaration sera précise, plus grande sera son efficacité lors de la mise en œuvre de la garantie.

Un mécanisme d'indemnisation spécifique peut être mis en place pour couvrir ce risque plus directement sans l'encadrer dans les clauses habituelles de limitation prévues par les vendeurs (connaissance de l'acquéreur, seuil ou franchise, plafond, etc.).

Les problématiques de (re)mise en état conforme peuvent être particulièrement coûteuses en matière informatique et l'on peut s'inspirer des clauses prévues dans le domaine de l'environnement, lorsqu'une remise en état d'un site pollué est nécessaire. On peut également s'inspirer de ce qui est prévu en matière de garanties dans le cadre des réglementations luttant contre la corruption. Le fonctionnement de la CNIL n'est pas très éloigné de celui de l'AFA (Agence française anticorruption) et les mécanismes des cartographies de risques requises présentent des similitudes.

Dans les deux matières, le préjudice d'image peut être particulièrement important et les dommages indirects

doivent être visés spécifiquement pour pouvoir être indemnisés.

Enfin, le dol et la nullité de la vente peuvent être invoqués comme cela fut le cas dans une jurisprudence antérieure à l'entrée en vigueur du RGPD. La vente d'un fichier client, contenant des données à caractère personnel a été jugée illicite car ledit fichier n'avait pas fait l'objet d'une déclaration obligatoire à la CNIL.

Dès lors, la Cour de cassation a considéré que le fichier non conforme n'était pas dans le commerce et ne pouvait être cédé[1] . Cette solution, rendue sous l'empire de la loi Informatique et Libertés avant l'entrée en vigueur du RGPD, aura vocation à être transposée dans le cadre du régime juridique actuel. Sans respect des lois relatives à la protection des données à caractère personnel, les données clients perdent leur valeur. En conclusion, l'actif incorporel que constituent les données sera un élément de plus en plus central dans les opérations de fusion-acquisition et devra faire l'objet de due diligences approfondies, de déclarations et de garanties détaillées. n ■

par Bernard Tézé, Associé, et Sylvain Staub, Associé, Ds Avocats

---

1. Cass. Com., 25 juin 2013, n° 12-17.037.