Tribune

RLDA 6655

Les nouvelles règles de protection des données personnelles dans les opérations de fusions acquisitions

Charles DAUTHIER
Avocat associé, Morgan, Lewis & Bockius UK LLP

Laetitia de PELET
Avocat collaborateur, Morgan, Lewis & Bockius UK LLP

Cet article aborde les moyens d'assurer la conformité d'une opération de fusion-acquisition, et de l'audit qui la précède, à la règlementation applicable en matière de protection des données personnelles[1].

Introduction

Voilà plusieurs mois que le monde juridique œuvre pour se mettre en conformité avec le règlement (UE) n° 2016/679 sur la protection des données personnelles (RGPD)[2] et la version modifiée de la loi n° 78-17 (loi Informatique et Libertés)[3].

L'application de ces nouveaux textes impacte largement la vie des affaires, sans que les opérations de fusions-acquisitions y fassent exception.

La protection des données personnelles doit être, aujourd'hui, un nécessaire point d'attention dans le cadre de ces opérations, tant au titre du respect des droits des personnes dont les données sont traitées, qu'au titre de la sécurisation de leur valeur, qui représente aujourd'hui une part substantielle de la valorisation de nombreux acteurs économiques. En effet, les actifs incorporels représentent aujourd'hui près de 84 % de la valeur totale des sociétés du classement Fortune 500[4]. Parmi ces actifs incorporels de valeur figurent notamment les fichiers clients et RH.

Le transfert de propriété de ces fichiers nécessite une attention particulière dans le cadre d'opérations M&A, tant au stade préliminaire de l'audit juridique qu'au stade de la formalisation et de la documentation de l'opération en cause.

La présente étude se propose de donner quelques éléments d'analyse sur ces questions, compte tenu des récentes réformes.

(1) Il n'est pas destiné à constituer un guide sur la conduite d'un audit data privacy, ni une liste exhaustive des points à vérifier à l'occasion d'un tel audit.

(2) Règl. (UE) n° 2016/679, 27 avr. 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, et abrogeant la directive 95/46/CE, entré en vigueur le 25 mai 2018.

(3) L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

(4) Opérations de M&A et protection des données personnelles : identifier et minimiser les risques, H. Segain et J.-B. Thomas-Sertillanges, Fusions & Acquisitions.

I. – L'audit juridique et le RGPD

A. – L'autocontrôle mis en place par le RGPD

Jusqu'au 25 mai 2018, la très grande majorité des traitements de données personnelles devait faire l'objet d'une démarche préalable auprès de la Commission nationale de l'Informatique et des Libertés (CNIL).

La procédure à respecter variait notamment en fonction du type de données traitées et des risques générés par le traitement en cause. Elle pouvait s'avérer relativement simple (déclaration simplifiée ou déclaration normale) ou être plus complexe (demande d'autorisation) dans certaines hypothèses.

Un des grands apports du RGPD et de la loi Informatique et Libertés résulte de la suppression de ces formalités dans la très grande majorité des cas.

L'approche adoptée est maintenant différente : la place du contrôle préalable est significativement réduite et l'autocontrôle est aujourd'hui privilégié.

> *"La Cour de cassation a estimé que, faute d'avoir été déclaré, le fichier client n'était pas dans le commerce et que, par conséquent, sa vente avait un objet illicite".*

Cet autocontrôle implique de respecter trois grands principes posés par la nouvelle réglementation :

- « *Accountability* » : l'obligation, pour les entreprises, de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données[5] ;
- « *Privacy by Default* » : l'obligation de garantir, « *par défaut* », que seules les données nécessaires au regard de chaque finalité spécifique du traitement sont traitées[6] ;
- « *Privacy by Design* » : l'obligation de considérer l'exigence de protection des données personnelles dès la conception des projets, produits ou procédures.[7]

L'affirmation que ces principes sont respectés ne sera naturellement pas suffisante en cas de contrôle : il est nécessaire de constamment documenter le respect de ces principes.

(5) Glossaire de la CNIL consulté le 18 décembre 2018.

(6) Règl. (UE) n° 2016/679, art. 25.2.

(7) Règl. (UE) n° 2016/679, art. 24.1.

Compte tenu du caractère relativement abstrait des trois principes précités, cette documentation peut apparaitre délicate à mettre en œuvre en pratique.

B. – La mise en œuvre pratique

Le RGPD et la loi Informatique et Libertés s'appliquent « […] *aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non-automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers* […] »[8].

Dès lors, la solution de facilité consiste à éviter l'application de la réglementation relative aux données personnelles en anonymisant l'ensemble de la documentation communiquée dans le cadre de l'audit juridique, sous réserve des données qui seraient déjà publiques (par exemple les informations figurant sur le K-bis, comme le nom du mandataire social ou son adresse personnelle)[9].

Cette solution pourra néanmoins apparaitre très fastidieuse à mettre en œuvre, si de nombreux documents sont appelés à être communiqués, dans la mesure où la définition légale des données personnelles est très large.

C'est par ailleurs un processus qu'il est difficile d'automatiser dans la mesure où une donnée pourra être une donnée personnelle dans certains cas mais pas dans d'autres[10].

L'anonymisation n'apparait donc adaptée que dans le cas d'opérations d'audits de taille très réduite.

À défaut d'anonymisation, le RGPD et la loi Informatique et Libertés trouveront pleinement à s'appliquer.

Dans ce cas de figure, conformément au principe de « *privacy by design* » précité, il pourrait être opportun[11] d'évaluer le risque qu'engendrerait le traitement de données personnelles mis en œuvre en raison de l'audit juridique. Cette évaluation du risque devrait, en principe, prendre la

(8) L. n° 78-17, art. 2.

(9) Attention toutefois de bien distinguer « *anonymisation* » et « *pseudonimisation* ». Il sera insuffisant, pour écarter l'application de la loi Informatique et Liberté, de se contenter de remplacer les données personnelles par une clé d'identification. La technique de l'anonymisation des données, quant à elle, détruit toute possibilité pour quiconque de pouvoir identifier à quel individu appartiennent les données personnelles.

(10) À titre d'exemple, la classification d'un salarié pourrait devenir une donnée personnelle permettant son identification dès lors qu'il serait le seul salarié relevant de cette classification.

(11) La réalisation d'un audit ne fait pas partie de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est expressément requise (délibération de la CNIL n° 2018-327, 11 oct. 2018). Cependant, une telle opération peut potentiellement répondre à certains des critères posés par le G29 dans ses lignes directrices WP 248 adoptées le 4 avril 2017. La conformité aux règles applicables en matière de protection des données de l'audit mis en place devra être, en toute hypothèse, documentée.

forme d'une « *analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel* »[12]. La CNIL a d'ailleurs mis à disposition un logiciel libre intitulé PIA afin d'aider les entreprises à formaliser et conduire ces analyses d'impact d'une façon conforme au RGPD et à la loi Informatique et Libertés [13].

La réalisation d'une telle analyse assure également le respect du principe d'« *accountability* » en permettant de documenter la conformité des traitements analysés.

Cependant, la mise en œuvre d'une telle analyse pourra s'avérer extrêmement lourde et inadaptée à la réalité pratique d'un audit compte tenu, notamment, de la confidentialité et du calendrier très serré souvent imposés par l'opération en cause.

Pour assurer la conformité de l'audit à la règlementation applicable en matière de protection des données, il conviendrait, *a minima*, d'informer préalablement à l'audit juridique, toute personne dont les données personnelles seront traitées lors de cet audit. Cette information permet de respecter à la fois les principes de « *privacy by design* » et d'« *accountability* », à condition qu'elle soit fournie par écrit avec preuve de sa remise (envoi par email avec demande d'accusé de réception et de lecture, remise contre décharge, etc.). Il est conseillé – sinon fortement recommandé – d'anticiper cette information et de prévoir, au sein de la (ou des) charte(s) de protection des données applicable à l'entreprise, ces opérations d'audit et de restructuration.

L'information doit notamment porter sur les données personnelles concernées, les destinataires ou encore la finalité poursuivie.

Tenter de contourner la contrainte découlant de l'application des dispositions légales sur la règlementation des données personnelles en ne donnant accès à une data room qu'à des avocats liés par une obligation de secret professionnel serait vain. En effet, le champ d'application de la règlementation ne prévoit pas d'exception propre à ce cas de figure.

Le RGPD et la loi Informatique et Libertés ne sont donc pas sans influence sur les opérations d'audit juridique. Les entreprises doivent en prendre conscience et adapter leur pratique. Le RGPD et la loi Informatique et Libertés doivent également être pris en compte au stade de la formalisation et de la documentation de l'opération de fusion acquisition en cause.

(12) Règl. (UE) n° 2016/679, art. 35 1.

(13) <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>.

II. – Le risque « data privacy » dans les opérations de fusions-acquisitions

Un traitement de données personnelles est défini comme « *toute opération, ou ensemble d'opérations, effectuée(s) à l'aide ou non de procédés automatisés et appliquée(s) à des données ou des ensembles de données à caractère personnel, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction* »[14].

Compte tenu de cette définition très large, une opération de cession d'activité ou d'entreprise et sa préparation impliquent nécessairement un traitement de données personnelles (des salariés, clients et autres interlocuteurs) et sont, par conséquent, soumises au RGPD et à la loi Informatique et Libertés.

Or, outre les sanctions financières, les risques encourus en cas de violation de cette règlementation sont significatifs. En effet, la cession envisagée risque d'être, tout simplement, annulée. Il faut donc mettre en œuvre des dispositifs assurant la conformité de l'opération au RGPD et à la loi Informatique et Libertés. En tout état de cause, le cessionnaire devra effectuer différentes démarches et vérifications.

A. – L'annulation de la cession pour défaut de respect de la règlementation applicable sur la protection des données personnelles

La Cour de cassation a jugé qu'une cession de fichiers pouvait être annulée pour défaut de respect de la règlementation applicable en matière de protection des données personnelles[15].

Dans cette affaire, un fichier de clients informatisé n'avait pas été déclaré à la CNIL alors qu'il aurait dû l'être sous l'empire de l'ancienne règlementation. La société qui en assurait la tenue l'a cédé à un tiers. Elle a ensuite été assignée en nullité de la vente. Les juges du fond se sont bornés à constater que la loi ne prévoit pas que l'absence d'une telle déclaration à la CNIL est sanctionnée par la nullité. Toutefois, la Cour de cassation a estimé que, faute d'avoir été déclaré, le fichier client n'était pas dans le commerce et que, par conséquent, sa vente avait un objet illicite. Les hauts magistrats ont donc considéré que c'est

(14) Règl. (UE) n° 2016/679, art. 4.

(15) Cass. soc., 25 juin 2013, n° 12-17.037, JCP E 2013, 1422, note J.-B. Seube ; D. 2013. 1867, note Beaussonie ; *ibid.* 1844, point de vue Storrer ; RTD civ. 2013. 595, obs. Barbier ; JCP 2013, n° 930, note Debet ; RDC 2013. 119, note Rochfeld.

à tort que les juges du fond ont refusé de prononcer la nullité de la vente pour objet illicite.

Bien que les obligations de déclaration préalable à la CNIL aient très majoritairement disparu depuis le 25 mai 2018, cette solution nous semble pouvoir être étendue à d'autres situations pour sanctionner la violation par les responsables de traitement de l'une quelconque de leurs obligations. Cette extension est d'autant plus envisageable que (i) les pouvoirs de contrôle et de sanction accrus de la CNIL peuvent laisser craindre une plus grande sévérité des juridictions civiles en matière de protection des données et (ii) le RGPD a accru les obligations des responsables de traitement et a entendu les responsabiliser davantage.

Une doctrine autorisée a ainsi récemment indiqué que « *la conclusion d'un contrat de vente de données personnelles collectées, traitées ou transférées de façon illicite continuera d'encourir la nullité. Tel serait le cas si les données personnelles étaient traitées en l'absence de tout fondement* . »[16] À notre avis, il pourrait en aller de même en cas de non-respect par le cédant de son obligation d'information préalable[17].

Il est donc impératif, pour assurer la validité de la cession, de vérifier la conformité des fichiers cédés à la réglementation applicable sur la protection des données personnelles (éventuelles déclarations ou demandes d'autorisation préalable réalisées auprès de la CNIL, réalisation d'analyses d'impact, information des personnes concernées, obtention des consentements nécessaires, etc.), sauf à prendre le risque de voir l'opération échouer.

B. – Comment procéder pour réduire les risques d'annulation de la cession ?

Vérifier la conformité des fichiers transférés dans le cadre de la cession à la règlementation applicable en matière de protection des données personnelles est un impératif pour réduire le risque d'annulation de la cession. Cela nécessite de mettre différentes pratiques en œuvre.

Tout d'abord, il faudra, bien évidemment, réaliser un audit « *data privacy* » de la cible de l'opération de fusion-acquisition. Il est aujourd'hui impossible de faire l'impasse sur cette matière dans ce type d'opérations et ce, d'autant qu'au-delà de la possible annulation du contrat de cession, il existe un risque, désormais bien connu, d'être condamné à payer de lourdes amendes administratives d'un montant pouvant atteindre 20 millions d'euros ou égal à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

De plus, en cas d'irrégularité constatée, si l'opération en cause est une cession d'actif et qu'elle inclut la cession d'un ou plusieurs fichiers, comme un fichier client, il est conseillé de soumettre la cession à la réalisation d'une ou plusieurs conditions suspensives imposant au vendeur de régulariser la situation et d'assurer la conformité dudit fichier avec la règlementation applicable en matière de protection des données personnelles avant le transfert de propriété.

Enfin, une fois l'opération finalisée, et en cas de changement de responsable de traitement, le nouveau responsable de traitement doit se manifester auprès des personnes dont les données personnelles sont traitées pour respecter l'obligation d'information qui pèse sur lui. Tel est notamment le cas en matière de cession de fonds de commerce.

L'ampleur des changements apportés par la nouvelle règlementation sur la protection des données personnelles est telle qu'une approche consistant à mobiliser les ressources pour être RGPD compatible à un instant T serait vaine. Beaucoup d'acteurs pensent encore aujourd'hui que le thème de la protection des données personnelles est un effet de mode et n'aspirent qu'à se débarrasser du sujet. C'est méconnaître le changement de paradigme du nouveau cadre règlementaire. Au-delà des investissements techniques et juridiques qui doivent nécessairement être faits pour mettre le fonctionnement d'une organisation à jour du RGPD, un vaste chantier d'éducation doit être engagé pour sensibiliser ses collaborateurs. Les acteurs des opérations M&A ne peuvent y échapper. ■

(16) J.-M. Bruguières, V. Fauchoux et A. Quiquerez, Actualité du droit civil du numérique, RLDC 2018/162, n° 6477.

(17) Sur cette obligation d'information, v. ci-dessus, I, B).