UNIVERSITÉ PARIS I PANTHÉON-SORBONNE

REVUE OFIS

Le Master 2 Opérations et Fiscalité Internationales des Sociétés est fier de vous présenter :

M&A et protection des données : Quelle articulation ?

Dana Badreddine

Étudiante du Master 2 Opérations et Fiscalité Internationales des Sociétés

Edgar Ficatier

Étudiant du Master 2 Opérations et Fiscalité Internationales des Sociétés

Alors que la numérisation de nos sociétés bat de son plein, la question de la protection des données personnelles devient un sujet omniprésent dans les préoccupations des entreprises. Une grande majorité de personnes, morales comme physiques, en collectent et en traitent chaque jour dans le cadre de leur activité. Elles sont une ressource inestimable, moteur d'expansion commerciale, et jouent un rôle fondamental dans la prise de décisions stratégiques. Ainsi depuis 2018, l'entrée en vigueur du RGPD a davantage encadré le sujet et a instauré de nouvelles obligations protectrices de la vie privé et des libertés individuelles des personnes visées.1 Sans surprise, le secteur des fusions-acquisitions n'échappe pas à la réglementation. Bien qu'elles ne soient pas intrinsèquement liées au sujet de la data, les opérations de M&A sont en effet susceptibles d'avoir des conséquences aussi bien pendant la due diligence que post-closing.

Ainsi les enjeux de protection des données laissent une empreinte de plus en plus forte sur le secteur des fusions-acquisitions (I), et il devient essentiel de savoir gérer les nouveaux risques qui peuvent en naitre (II).

I. L'apparition progressive de la protection des données dans les opérations de fusions-acquisitions

A. Définition et contextualisation de la donnée personnelle

La donnée personnelle, cœur du sujet, a reçu sa définition de l'article 4[1] du RGPD. Elle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Le nom, le prénom, l'adresse, le numéro de contrat, ou encore la pointure de chaussure sont des informations dites identifiantes ou faisant référence à une personne. Elles doivent donc être protégées au nom notamment de la protection de la vie privée, de la confidentialité et de la sécurité des individus. Sont dès lors soulevées des préoccupations évidentes en matière de gestion de risques et de conformité.

Ces informations représentent aussi une mine d'or pour les investisseurs et professionnels, qui peuvent adapter leurs décisions d'investissement, leurs stratégies commerciales ainsi que leurs prévisions de rentabilité sur la seule base des préférences de leur clients ou de toute autre partie prenante. La donnée personnelle revêt une typologie aussi variée qu'elle est un facteur de valorisation. Cette typologie varie selon la nature de l'activité, les besoins de l'entreprise et les finalités recherchées.

D'abord viennent les données dites clients, cruciales en ce qu'elles fournissent des informations précises et individualisées

[1] Règlement (UE) 2016/679 du Parlement Européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

permettant de mieux cibler le marché idéal. Par algorithmie et automatisation, elles illustrent les préférences de chacun au travers des historiques d'achats et autres interactions passées avec l'entreprise ou ses partenaires.

Ensuite viennent les données des employés, dites RH, qui ne peuvent – elles – qu'être celles dont l'employeur « a réellement besoin » à un instant T à des fins administratives, organisationnelles ou sociales. Elles sont donc d'accès plus restreint[2]. Par ailleurs, l'importance de ces données varie en fonction des opérations, des besoins en jeu et des finalités recherches, aidant les entreprises à prendre des décisions plus éclairées tout au long du processus.

Enfin viennent les données des partenaires commerciaux, des informations contractuelles détaillées sur les accords et contrats en cours. Elles donnent un historique des transactions passées permettant de matérialiser des volumes de vente, des revenus, des difficultés ou encore des atteintes du marché.

Avant mai 2018, date de l'entrée en vigueur du RGPD, la question de la protection de toutes ces données émergeait et suscitait déjà de nombreuses questions en Europe comme ailleurs. En ce sens, des lois et des réglementations avaient été mises en place en Europe par la Directive sur la protection des données de 1995[3], en France par la Loi Informatique et Libertés de 1978[4], ou encore aux Etats-Unis par la Loi sur la protection de la vie privée en ligne des enfants (COPPA) de 1998 et la Loi sur la protection des renseignements personnels et la sécurité (HIPAA) de 1996.

B. *La place de la donnée personnelle dans les opérations de fusions-acquisitions*

Dans le cadre des opérations de fusions-acquisitions, la donnée personnelle peut revêtir diverses importances, mais principalement en matière de valorisation. Elle est d'abord l'actif immatériel primordial d'une entreprise à forte empreinte numérique. Elle aide à définir sa part de marché, l'opportunité de son rachat, ou à chiffrer son prix d'acquisition. Inversement, une mauvaise application des règles propres au traitement de la donnée personnelle peut aussi en faire un facteur de diminution du prix d'acquisition. Les lourdes amendes encourues (i.e., 20m€ ou 4% du chiffre d'affaires mondial, par application de l'article 43ter de la Loi Informatique et Liberté du 6 janvier 1978) sont des risques permettant de négocier le prix à la baisse, lorsqu'ils ne sont pas deal breaker (i.e., une raison de rompre les négociations de rachat).

Une percée notable du sujet de la donnée personnelle s'est observée à partir de 2014, lorsque le groupe Facebook (nouvellement Meta) a réalisé la plus grosse acquisition de son histoire en s'accaparant Whatsapp. Les deux entreprises traitent chaque minute un montant colossal de données personnelles, au point où le volume de messages envoyés par Whatsappp

[2] Article 88 du RGPD.

[3] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

approchait déjà à ce moment le volume entier des SMS à travers le monde[5]. En date de l'acquisition, plus de 450 millions d'utilisateurs étaient présents mensuellement sur l'application, pour une moyenne de 32 milliards de messages reçus par jour[6]. Chacun de ces utilisateurs a au moins fait transiter sur les serveurs de l'application son numéro mobile, sa photo de profil et sa localisation sous l'empire des lois sur la protection de ces données.

Pourtant à partir de 2021, post-closing, la Data Protection Commission (i.e., la CNIL irlandaise) a sanctionné l'entreprise nouvellement acquise et son groupe de plusieurs amendes chiffrées successivement à 225m€ (septembre 2021), 390m€ (début janvier 2023) et 5.5m€ (mi-janvier 2023) pour violation des lois sur la protection des données et défaut de transparence dans leur gestion.

Plus que jamais, les opérations de fusions-acquisitions s'ouvrent à de nouvelles préoccupations majeures nées de la numérisation du marché.

II. Gestion des risques inhérents aux données personnelles en due diligence et post-closing

A. Gestion des risques inhérents à la phase de due diligence

Mieux vaut prévenir que guérir. Pour prévenir en matière de fusions-acquisitions, l'acquéreur doit s'atteler à réaliser une due diligence suffisamment robuste. Ce procédé consiste en un véritable audit de la cible, principalement sur les plans financier, juridique et fiscal. Il permet en l'occurrence d'identifier les potentiels risques liés à la data et de les anticiper.

Or pour réaliser une due diligence, le potentiel acquéreur (i.e., bidder) et ses conseils se voient ouvrir une Virtual Data Room (i.e., une base de données en ligne comportant toute la documentation pertinente à l'audit) elle-même remplie de données personnelles. De par cela, leur traitement doit donc déjà être soumis aux protections du RGPD et des autres textes connexes.

La divulgation de ces données doit ainsi être strictement nécessaire à l'opération ainsi qu'aux personnes habilitées et encadrées contractuellement en application des articles 26 et 28 du RGPD.

Ces données doivent aussi être anonymisées en principe. En pratique toutefois, des milliers de documents sont déposés instantanément auprès des conseils du bidder par l'intermédiaire de la VDR. Une même équipe chargée d'une seule typologie de risque (e.g., TVA) peut demander à elle-même plusieurs centaines de documents dont de nombreux sont susceptibles de contenir des données personnelles (e.g., factures, contrats de prestations de services, preuves de transport, etc.). Les calendriers pour les traiter sont eux-mêmes trop serrés, parfois de l'ordre de quelques jours, pour qu'il y ait raisonnablement le temps de tous les anonymiser.

[5] C. Jabura, Facebook Acquisition of WhatsApp, octobre 2021, Kenya Methodist University

[6] FranceInfo, AFP, Pourquoi Facebook rachète la messagerie WhatsApp pour plus de 11 milliards d'euros, 19 février 2014.

En principe également, les personnes dont les données personnelles sont traitées doivent être préalablement informées de leur traitement ainsi que de leur destinataire (articles 13 et 14 du RGPD). Or en pratique là encore, outre le nombre colossal de parties concernées, ce procédé viendrait balayer toute la confidentialité essentielle au déroulé d'une opération de fusion-acquisition.

Une application peu rigoureuse de la réglementation provoque pourtant des risques chiffrables (i.e., amende 20m€ ou 4% du chiffre d'affaires mondial) ainsi que des actions en responsabilité provenant des personnes dont la data a été irrégulièrement traitée. Au pire des cas, elle peut même entrainer l'annulation d'une cession d'actif (Cass. com., 25 juin 2013, n° 12-17037)[7]. D'un autre côté pourtant, une trop grande rigueur provoquerait des difficultés pratiques insurmontables pour les cibles, leurs bidders et leurs conseils respectifs, et porterait une atteinte démesurée au secret des affaires.

Il n'y a à ce jour pas de tempérament concret à l'application du RGPD dans la pratique même des fusions- acquisitions, sinon une tolérance implicite des autorités et des parties concernées. Rien n'exclue pour autant qu'un jour, la jurisprudence n'ait à se prononcer sur la position qu'il convient concrètement de prendre. En attendant, une pratique exponentielle des indemnities and warranties (i.e., indemnités et garanties) peut s'observer pour au moins assurer une gestion des risques post-closing.

B. <u>Gestion des risques encourus post-closing</u>

Outre le procédé de due diligence en lui-même et la gestion des accès à la VDR, il est pour premier enjeu des conseils de savoir déterminer les risques inhérents aux données personnelles que fait encourir la détention de l'entreprise-cible. La typologie des risques potentiels est elle aussi particulièrement variée.

Il existe d'abord un risque manifeste de conformité. Le RGPD introduit des conditions au traitement des données que la CNIL reprend dans ses recommandations. Ainsi l'individu dont les données sont traitées doit avoir manifesté librement, spécifiquement et de manière éclairée et univoque son accord à chaque finalité de traitement. Ce traitement doit être licite et loyal, suivant un principe de transparence qui se doit d'être matérialisé par une accessibilité accrue de toute information ou communication relative au traitement des données personnelles. Egalement, les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités de traitement consenties, et conservées pour une durée limitée au strict minimum. La CNIL veille particulièrement à la conformité de ses justiciables, et a déjà infligé 41 millions d'euros en amendes et en liquidations d'astreinte pour la seule année 2023.

Se trouve aussi un risque de sécurité des données personnelles. Celles-ci sont sujettes de manière croissante aux attaques informatiques de type phishing ou brute-force8. Fin janvier, à titre d'illustration, les

[7] La cour de cassation a jugé qu'une cession de fichiers clients pouvait être annulée pour défaut de respect de la réglementation en matière data protection.

entreprises Viamedis et Almerys ont été victimes d'une fuite de données concernant plus de 33 millions de personnes, dont leur état civil, leur date de naissance, leur numéro de sécurité sociale, le nom de leur assureurs santé et les garanties souscrites.9 En matière de fusions-acquisitions, l'acquéreur peut se trouver responsable d'un tel manquement en matière de sécurité des données personnelles, pour des procédés qui ont pourtant été établis par la cible bien avant son acquisition. In Fine, il peut donc se trouver responsable des négligences des cédants.

Enfin peut aussi se trouver un risque réputationnel évident. Les opérateurs Vlamedis et Almerys ont perdu une grande part de leur crédibilité sur le marché des tiers-payants de complémentaires santé, entrainant naturellement un préjudice commercial que les investisseurs verront se matérialiser dans les prochains comptes annuels. Pour ne pas s'en suffire, la CNIL est aussi susceptible d'inscrire un opérateur négligeant sur une liste de Name & Shaming, afin de les associer publiquement à leurs manquements et au montant de l'amende due.

Afin d'y contrebalancer, dès la rédaction du SPA (i.e., Share Purchase Agreement), il est possible de définir le régime de responsabilité des parties pour tout imprévu à survenir post-closing (i.e., après clôture de l'opération). La cible s'engage alors à des déclarations et garanties directement apposées au contrat d'acquisition et éventuellement couvertes par des polices d'assurance (dites Warranty & Indemnity Insurance). La prime de l'assurance, le cas échéant, est généralement déduite du prix d'acquisition de sorte à ce que l'assureur endosse la responsabilité en cas de contingence.

L'ensemble permet aux négociations d'aboutir malgré des difficultés dans la gestion des risques de Data protection au cours de l'opération et après, et finalement de faciliter l'application de la réglementation en vigueur malgré les contraintes du secteur.

CONTACTS

École de Droit, Université Paris I Panthéon-Sorbonne

Adresse : 12 place du Panthéon, 75231 Paris cedex 05
Téléphone : 01 44 07 80 00

Master 2 Opérations et Fiscalité Internationales des Sociétés

Email : m2ofis2024@gmail.com
Linkedin : https://www.linkedin.com/in/m2ofis/

Dana Badreddine

Email : danabadreddine01@gmail.com
Linkedin : Dana Badreddine

Edgar Ficatier

Email : edgar.ficatier@pm.me
Linkedin : Edgar Ficatier