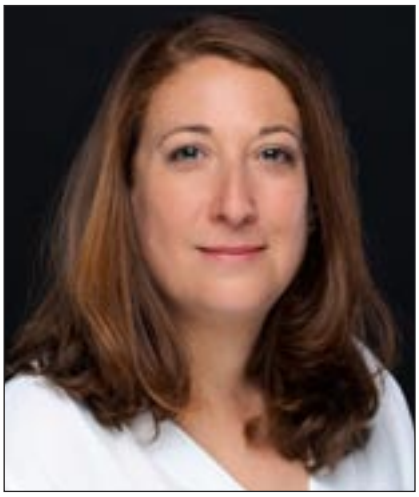
COMMENT ANTICIPER ET GÉRER LES SUJETS RELATIFS À LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CADRE D'UNE OPÉRATION M&A ?

par Guillaume Briant, Associé, Private Equity et M&A, et Laetitia Ghebali, Counsel, Regulatory et données personnelles

STEPHENSON HARWOOD

Guillaume Briant



Laetitia Ghebali

Les opérations M&A sont par essence des opérations stratégiques qui présentent des enjeux importants. Dans une économie de plus en plus digitalisée, où de nombreuses opérations portent sur des sociétés « techs » et où même les entreprises opérant dans des secteurs industriels plus classiques développent une stratégie digitale, les sujets relatifs à la protection des données personnelles doivent être clairement identifiés et appréhendés.

La question de la prise en compte de la protection des données personnelles lors des opérations M&A constitue par ailleurs une préoccupation majeure des autorités européennes de protection des données personnelles comme l'a rappelé l'*European Data Protection Board* (« EDPB ») à l'occasion du rachat de Fitbit par Google en 2020, cette dernière indiquant qu'elle «*examinera les conséquences potentielles de cette concentration sur le plan de la protection des données à caractère personnel dans l'Espace économique européen* »[1].

En effet, au cours d'un processus d'acquisition, de nombreuses données, y compris des données à caractère personnel, sont généralement échangées entre l'entreprise cible, le ou les vendeurs et le ou les acheteur(s) potentiel(s).

[1] EDPB (europa.eu)

Le non respect du règlement général sur la protection des données[2] (« RGPD ») par l'entreprise cible peut également avoir un impact financier important pour l'acquéreur. Ainsi, de lourdes sanctions pécuniaires[3], pouvant s'élever jusqu'à 4% du chiffre d'affaires annuel mondial, peuvent être infligées dans l'hypothèse où les activités de traitement des données de l'entreprise cible ne seraient pas conformes au RGPD. A l'instar de la pratique en matière d'infractions au droit de la concurrence, ces manquements au RGPD sont susceptibles d'être imputés à l'acquéreur dans certaines circonstances. Les acheteurs pourraient ainsi s'exposer à des risques importants tant financiers que réputationnels en cas de manquement au RGPD.

Par conséquent, dans le contexte d'une transaction M&A, les entreprises doivent veiller à tenir compte des exigences posées par le RGPD tant s'agissant du processus d'acquisition proprement dit que lors de l'évaluation qu'elles feront de l'entreprise cible. Le présent article a ainsi pour objet de présenter certaines des bonnes pratiques développées ces dernières années afin de prendre en compte les enjeux liés au RGPD lors des opérations M&A.

1. Comment s'assurer que le processus même de mise en œuvre d'une transaction M&A par les entreprises parties à cette opération soit conforme au RGPD ?

Dans le cadre d'une transaction M&A, les acheteurs potentiels et leurs conseils sont généralement susceptibles d'avoir accès à des données à caractère personnel concernant les salariés ou parfois les clients et les fournisseurs, en particulier dans le cadre des audits de *due diligence*.

Par conséquent, les parties en présence doivent prendre des mesures pour protéger de manière adéquate les données à caractère personnel qu'elles traitent afin de se conformer aux principes de base du RGPD dans le cadre de la transaction.

Les précautions suivantes pourront être mises en œuvre afin de s'assurer que le processus de mise en œuvre de la transaction M&A respecte bien la réglementation relative à la protection des données à caractère personnel :

■ Garantir l'intégrité, la sécurité et la confidentialité des données

Afin de de se conformer au principe de sécurité posé par le RGPD[4], les entreprises parties à une transaction M&A doivent prévoir des mesures techniques et organisationnelles appropriées pour garantir à tout moment la sécurité des données à caractère personnel, et en particulier la confidentialité, l'intégrité et la disponibilité de ces données.

Des mesures contractuelles doivent notamment être adoptées pour préserver l'intégrité et la confidentialité des données à caractère personnel. Il conviendra en particulier de veiller à ce que les *Non Disclosure Agreements* (« NDA ») signés au début de l'opération intègrent des stipulations relatives au RGPD. A cet égard, nous conseillons par exemple d'adapter les NDA signés par les personnes ayant accès aux données de l'entreprise cible aux exigences spécifiques du RGPD. A ce titre, le NDA pourra intégrer une clause relative à la protection des données à caractère personnel qui qualifierait le rôle et les responsabilités de chaque partie au regard du RGPD, anticiperait les éventuels transferts de données vers des pays tiers à l'Union européenne et inclurait des engagements quant au stockage et à la destruction desdites données.

Dans le cas somme toute assez classique où les documents sont partagés via l'utilisation d'une *Data Room,* il conviendra de prendre en considération les exigences du RGPD lors du choix du prestataire auprès duquel la *Data Room* sera hébergée, notamment en s'interrogeant sur le pays dans lequel les données seront stockées ou encore sur les mesures de sécurité mises en place par la plateforme proposées par ce prestataire (contrôle des accès, protection contre le hacking, apposition d'un filigrane ou encore limitation des possibilités de téléchargement et d'impression). Une fois le prestataire choisi, dans le cas où il ne s'agirait pas de l'un des leaders du marché (ces derniers sont généralement plutôt bien outillés pour respecter le RGPD), il conviendra de s'assurer que le contrat conclu avec le prestataire prenne bien en compte les aspects liés au RGPD[5], le prestataire agissant comme sous-traitant au sens de cette réglementation.

■ Anticiper l'information des personnes concernées de la communication de leurs données à caractère personnel à un acheteur potentiel

Conformément au principe de transparence[6], il est nécessaire d'informer préalablement les personnes concernées (salariés et, le cas échéant éventuellement clients et fournisseurs,) de la communication de leurs données à carac-

[2] 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.
[3] Article 83 du RGPD.
[4] Article 32 du RGPD.
[5] Article 28, 3) du RGPD.
[6] Article 12 du RGPD.

tère personnel. Ce devoir d'information, qui se distingue de l'obligation du recueil du consentement pour certains traitements de données à caractère personnel, a pour objectif d'informer les personnes concernées de l'utilisation qui est faite de leurs données personnelles.

Or, l'information préalable des personnes concernées peut s'avérer difficile, voire impossible, dans le contexte d'une transaction M&A compte tenu de la nature confidentielle de ce type d'opérations.

Par conséquent, nous conseillons à l'entreprise dont les données sont traitées d'anticiper, le plus en amont possible, l'hypothèse d'un transfert de données à un acquéreur potentiel à l'occasion d'une opération de M&A. Cette anticipation peut se faire dans les chartes ou déclarations de confidentialité ou dans les contrats de travail. De cette manière, les salariés seront informés que leurs données personnelles pourraient être transmises dans le contexte d'une opération M&A bien avant le début d'une opération stratégique. De manière similaire, dans les cas (certes plus rares) où l'activité de la société cible justifierait que des données personnelles relatives aux clients ou aux fournisseurs soient transmises à un acquéreur potentiel dans le cadre d'une opération M&A, il peut être utile de prévoir dans la documentation contractuelle type (telles que les conditions générales de vente ou d'achat) la faculté de communiquer des données personnelles dans le cas exceptionnel où ces données seraient transmises dans le contexte d'une transaction M&A.

■ **Veiller à limiter les données communiquées au strict nécessaire**

En application du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données)[7]. En d'autres termes, l'entreprise cible et/ou le vendeur et les acquéreurs potentiels ne doivent pas traiter plus de données à caractère personnel qu'ils n'en ont besoin dans le contexte de la transaction en question. Cela signifie que seules les données utiles à l'évaluation de l'opération doivent être communiquées aux acheteurs potentiels, et que les données à caractère personnel qui ne sont pas pertinentes dans ce contexte doivent être protégées autant que possible.

Afin de respecter ce principe de minimisation des données, nous recommandons de prêter une attention particulière aux documents qui seront mis à disposition des acquéreurs potentiels afin de s'assurer que ces documents sont bien nécessaires dans le contexte de la transaction.

En pratique, plusieurs mesures peuvent être prévues pour limiter les données communiquées au strict nécessaire. Il peut s'agir, lorsque cela est possible, de pseudonymisation ou d'anonymisation des données à caractère personnel, ou encore de l'agrégation des données relatives au salaire pour éviter l'identification des salariés. Nous conseillons de préférer l'utilisation de modèle de contrats de travail plutôt que des copies signées ou encore d'anonymiser les procès-verbaux de réunions du CSE afin d'expurger de ces documents toute données personnelles qui ne seraient pas strictement nécessaires à l'évaluation de l'entreprise cible.

2. Comment appréhender la question de la conformité de la cible au RGPD, qui est devenue un paramètre essentiel, dans le contexte d'une opération de M&A ?

En cas de manquements au RGPD par l'entreprise cible antérieurement à l'opération de M&A et qui seraient découverts postérieurement à cette dernière, l'acheteur pourrait s'exposer à un risque de sanctions. Compte tenu de l'importance des sanctions qui peuvent être imposées par les autorités de protection des données à caractère personnel[8], il est donc essentiel de réaliser un audit de conformité au RGPD de la cible, et le cas échéant, en fonction des résultats de cet audit, de prévoir des mesures pour atténuer les risques au titre du RGPD.

Nous conseillons donc de prendre des mesures appropriées pour s'assurer de la conformité au RGPD à tous les stades de la transaction M&A, depuis la phase de *Due Diligence* jusqu'à l'intégration de l'entreprise cible.

■ **La phase de *Due Diligence* est essentielle pour évaluer le niveau de conformité de l'entreprise cible au RGPD et les risques associés**

Au cours de cette phase, nous recommandons d'inclure dans le questionnaire de *Due Diligence* des questions couvrant les principales obligations prévues par le RGPD. La liste des demandes doit permettre de faire un examen approfondi des politiques et procédures mises en place par l'entreprise cible en matière de RGPD. Cette liste devrait notamment inclure la communication du registre des traitements, la confirmation de la nomination d'un délégué à la protection des données lorsque cela est requis, la communication des politiques et procédures internes en matière de RGPD, l'indication quant à d'éventuelles plaintes et/ou violation des données, la communication des contrats de sous-traitance

[7] Article 5, 1) c) du RGPD.
[8] Pour rappel, en application du RGPD, les sanctions pécuniaires peuvent s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4% du chiffres d'affaires annuel mondial en cas de manquement au RGPD.

éventuels et déclarations de confidentialité ainsi que celle des analyses d'impact le cas échéant.

Le questionnaire doit être adapté à l'activité de l'entreprise cible, en particulier dans l'hypothèse où l'acquisition fait intervenir des entreprises qui développent des activités impliquant le traitement de données personnelles sensibles (par exemple, des données de santé, biométriques, raciales et religieuses) car leurs activités représentent un risque plus important du point de vue de la protection des données.

Au-delà de l'audit juridique à proprement parler, il peut également être utile de faire appel à des prestataires externes spécialisés dans les risques liés à la cybersécurité afin de rechercher d'éventuelles failles informatiques et de s'assurer de l'absence de fuite de données personnelles au cours des dernières années. Ces audits IT devront idéalement être réalisés avant le *signing* (ou, si les circonstances le requièrent, entre le *signing* et le *closing*), en particulier lorsque l'entreprise cible traite des données sensibles au sens du RGPD (comme des données de santé) ou un nombre très important de données personnelles (par exemple dans le cas d'une entreprise de vente au détail en ligne). La question de la répartition entre les parties de la prise en charge du coût de réalisation de ces audits et des mesures de remédiation éventuelles en cas de faille informatique détectée pourra être traitée dans le contrat de cession.

Cette analyse de la conformité de l'entreprise cible au RGPD est importante pour identifier et formuler une stratégie d'atténuation des risques (cf. ci-après). On peut également souligner que cette évaluation au regard de la conformité au RGPD est susceptible de modifier de manière significative la valorisation de l'entreprise cible. Rappelons qu'à l'occasion du rachat de Yahoo par Verizon, la découverte d'attaques informatiques dont avait été victime Yahoo avait conduit à la réduction du prix de vente de l'ordre de 350 millions de dollars[9]. En outre, dans certaines situations exceptionnelles, notamment dans des secteurs où la question de la conformité au RGPD est fondamentale (par exemple dans le secteur de la santé), la découverte à l'issue de l'audit de Due Diligence de violations de données ou de failles informatiques majeures pourrait conduire l'acheteur à renoncer à l'opération avant le *signing* (l'absence de violations des données étant alors une condition du *signing*).

■ **Le contrat de cession devra être adapté afin de tenir compte de l'évaluation du niveau de conformité au RGPD de l'entreprise cible**

Trois types de clauses peuvent être insérées dans le contrat de cession afin de répondre aux préoccupations en matière de protection des données à caractère personnel identifiées au cours de la phase de Due Diligence : les déclarations et garanties, les indemnités spécifiques et les conditions suspensives.

S'agissant des déclarations et garanties, nous considérons que les garanties générales concernant le respect de la loi ne sont pas les plus adaptées pour couvrir les risques liés aux manquements au RGPD. Nous conseillons d'affiner ces garanties afin de refléter la situation de l'entreprise cible et d'ajuster les garanties spécifiquement au respect du RGPD. Cela permettra de mieux protéger l'acheteur contre les risques liés à la protection des données et le vendeur contre les dispositions légales relatives à la protection des données qui ne seraient pas encore envisagées par les autorités compétentes. A cet égard, il pourrait être stipulée une garantie d'absence de litige aux termes de laquelle le vendeur garantit qu'il n'y a pas eu de plainte ni de procédure devant l'autorité de contrôle au cours d'une période déterminée. Pourrait également être envisagée une garantie d'absence de violation de données selon laquelle le vendeur garantit qu'il n'y a pas eu ou qu'il n'a pas connaissance de violation des données personnelles au cours d'une période déterminée (par exemple au cours des trois dernières années) ou encore une garantie selon laquelle le vendeur garantit qu'il a mis en place des procédures conformes aux pratiques de marché en cas de violation de données.

Les parties peuvent par ailleurs chercher à mettre en place une assurance garantie de passif. Dans ce cas, il est important de s'assurer que la protection des données ne figure pas dans la liste des exclusions de la police d'assurance. Il est toutefois important de garder à l'esprit que l'assurance de représentation et de garantie, selon le plafond retenu, peut s'avérer insuffisante pour couvrir les amendes pouvant être prononcées en cas de manquements grave au RGPD.

En outre, si un risque au regard de la conformité au RGPD est identifié au cours de la phase de *Due Diligence*, une indemnité spécifique peut remédier à la situation. L'objectif de cette indemnité, comme toute indemnité prévue dans le cadre d'un contrat de cession, est de transférer le risque de la non-conformité détectée, qui est connu, à la partie qui indemnise (le vendeur). Par exemple, si une violation de données personnelles s'est produite avant la clôture de l'opération M&A ou qu'une procédure administrative a engagée et est toujours en cours, les parties à l'opération peuvent convenir que le vendeur remboursera l'acquéreur ou l'investisseur pour toute perte découlant de la violation de données.

[9] Verizon and Yahoo amend terms of definitive agreement | News Release | Verizon

Enfin, dans le cas de manquements au RGPD qui peuvent être corrigés relativement facilement, ou lorsque les manquements identifiés sont tels que leur correction est indispensable avant le *closing*, il est possible de prévoir des conditions suspensives exigeant du vendeur qu'il remédie à ce manquement avant même la réalisation de l'opération. Ces conditions suspensives peuvent notamment consister dans la nomination d'un délégué à la protection des données[10], la mise en place de procédures de protection des données personnelles ou encore dans l'établissement d'un registre des traitements[10]. Pour éviter tout risque de condamnation pour *Gun Jumping* par une autorité de concurrence, il conviendra de veiller à ce que ces conditions suspensives ne conduisent pas en pratique à une gestion de l'entreprise cible par l'acquéreur ou à une intégration anticipée des entreprises. Par exemple, lorsqu'une condition suspensive prévoit la mise en place de procédures de protection des données personnelles, les procédures internes à l'acquéreur en la matière ne pourront pas être mises en place par l'entreprise cible avant le *closing*. Des procédures conformes aux pratiques de marché pourront être mises en place entre le *signing* et le *closing* au titre des conditions suspensives, à charge ensuite pour l'acquéreur de terminer la mise à niveau des procédures au moment de l'intégration de l'entreprise cible.

■ **Une fois le *closing* passé, et les conditions suspensives réalisées, des précautions devront être prises au moment de l'intégration de l'entreprise cible afin de satisfaire les exigences du RGPD**

Il conviendra notamment de prévoir d'informer les personnes concernées des changements résultant de l'opération. Selon la nature de l'opération (cession d'actions, cession d'actifs ou opération de fusion et d'acquisition), il pourra également être nécessaire d'obtenir le consentement des personnes concernées afin de continuer à traiter leurs données à caractère personnel. Une analyse au cas par cas devra donc être réalisée avant de procéder au transfert des bases de données et de poursuivre les activités de traitement de l'entité cible.

Une mise à jour du registre de traitement devra également être envisagée si l'opération conduit à un changement de responsable de traitement, de délégué à la protection des données ou si de nouveaux destinataires des données sont envisagés.

Enfin, il conviendra de s'assurer que le transfert des bases de données (de clientèle et du personnel) soit sécurisé et respecte bien les éventuelles restrictions prévues par le RGPD en cas de transfert des données à caractère personnel en dehors de l'Union européenne.

Par ailleurs, une attention particulière aux exigences du RGPD devra être portée en cas de mise en place d'un contrat de services transitoires (« TSA »). Si ce contrat implique le traitement de données à caractère personnel (par exemple en cas de fourniture à la société ou branche cédée de services de ressources humaines, de services comptables ou informatiques par le vendeur), les points suivants devront notamment être intégrés dans le TSA : la qualification du rôle respectif des parties au regard du RGPD (sous-traitant, responsable de traitement), les catégories de données personnelles traitées ou encore l'obligation du vendeur d'effacer les données de l'entreprise cible à la fin de la période de transition.

Au regard des lourdes amendes infligées en cas de violation du RGPD, il est donc impératif aujourd'hui que, dans le contexte d'une opération M&A, les entreprises prennent en considération l'ensemble des recommandations qui précèdent s'agissant de la conformité au RGPD.

[10] L'article 37 du RGPD prévoit une obligation de désignation d'un délégué à la protection des données notamment lorsque les activités de base du responsable de traitement exigent un suivi régulier et à grande échelle des personnes concernées.
[11] Conformément à l'article 30 du RGPD, les responsables de traitement sont tenus de tenir un registre des activités de traitement effectuées sous leur responsabilité.