OPÉRATIONS DE M&A ET PROTECTION DES DONNÉES PERSONNELLES : IDENTIFIER ET MINIMISER LES RISQUES

par Hubert Segain, Avocat associé,
et Jean-Baptiste Thomas-Sertillanges, Avocat,
Herbert Smith Freehills Paris LLP

Hubert Segain

Jean-Baptiste Thomas-Sertillanges

Alors que les actifs incorporels représentent aujourd'hui près de 84% de la valeur totale des sociétés du classement Fortune 500, les données à caractère personnel, plus particulièrement, se situent au cœur du business-model de la plupart des entreprises innovantes.

Avec l'adoption au niveau européen de nouvelles règles encadrant les traitements de données à caractère personnel (le « GDPR »), le risque de non-conformité n'a plus rien d'anecdotique : les régulateurs exigent désormais que les entreprises concernées soient en mesure, à tout moment, de pouvoir documenter et démontrer leur niveau de conformité au GDPR, sous peine de lourdes amendes, pouvant aller jusqu'à 4% de leur chiffre d'affaires mondial annuel ou encore 20M € en vertu du nouveau texte.

Pire ! Au-delà des sanctions financières, les tribunaux français n'ont pas hésité dans le passé à annuler une vente de fonds de commerce, au motif de l'illicéité des traitements de données sous-jacents ... et donc de l'objet de la transaction.

Ainsi, dans le cadre d'une opération de M&A, le risque de non-conformité des activités de la cible au GDPR (mais également le risque de non-conformité de l'opération elle-même) doivent être appréhendés au plus tôt, afin de prendre les mesures propres à les minimiser.

1. Assurer la conformité des traitements de données liés à l'opération

Le processus d'audit implique la mise à disposition par le vendeur d'une masse de documents en vue de leur analyse par l'acheteur. Ces documents contiennent généralement des informations de toute nature relatives à des personnes physiques telles que des clients de la cible, ses salariés, ses fournisseurs etc autrement dit, des « données à caractère personnel » au sens de la loi.

Bien que le périmètre de cette divulgation soit en principe limité – par exemple, l'acquéreur n'a pas vocation à ce stade à avoir accès à l'intégralité des bases de données client – le vendeur et la cible seront amenés à sélectionner, compiler, copier, numériser, transférer sur un réseau, stocker sur des serveurs tiers et au final, divulguer à des tiers, des informations pouvant contenir des données à caractère personnel.

En d'autres termes, dans la plupart des cas, ce processus peut constituer en soi un « traitement de données à caractère personnel ». Il en résulte que la cible ou l'acquéreur, en qualité de responsable de traitement, devra s'assurer que celui-ci est réalisé conformément aux obligations mises à sa charge par le GDPR.

Dans ce cadre, deux approches sont envisageables.

La première consiste à procéder à une anonymisation de la masse de documents transmise. Il s'agit d'identifier et d'effacer purement et simplement le nom des personnes physiques au sein des documents transmis, l'objectif étant de neutraliser l'application des textes en matière de protection de données.

Cette approche connait toutefois certaines limites. D'une part, juridiquement, le processus d'anonymisation doit être conforme à l'exigence « d'irréversibilité » fixée par les autorités de protection des données, ce qui en pratique est rarement le cas. D'autre part, techniquement, le processus peut s'avérer particulièrement fastidieux et couteux, lorsque l'objectif est l'anonymisation de contrats numérisés au format image / PDF.

La seconde approche consiste à admettre qu'un traitement de données est en cause et qu'il convient de le mettre en conformité avec la loi « informatique et liberté » – une tâche qui est d'ailleurs loin d'être insurmontable :

- Premièrement, il y a lieu de présumer que les données transférées sont « licites » c'est-à-dire qu'elles ont été collectées et conservées à l'origine en conformité avec la loi, notamment s'agissant des formalités préalables ou de l'information des personnes concernées ;

- D'autre part, la finalité du traitement devrait en soi être considérée comme un « motif légitime » au sens de la loi, puisqu'il s'agit pour le vendeur de disposer à sa discrétion de ses actifs. La conséquence est importante : certaines exceptions aux principes d'information préalable ou de déclaration préalable pourront être applicables.

- Par ailleurs, l'approche consistant à identifier et minimiser les risques est précisément celle consacrée par le GDPR, qui invite les entreprises à réaliser des « Privacy Impact Assessement » au cas par cas pour déterminer comment protéger les données dans une situation particulière. À cet égard, l'anonymisation de données sensibles susceptibles d'être transférées au sein de la Data Room permet de minimiser substantiellement les risques de non-conformité.

Dans tous les cas, des démarches raisonnables devront être prises pour encadrer les conditions du transfert de données entre les parties prenantes :

- la définition des informations confidentielles dans le NDA devrait a minima couvrir la notion de données à caractère personnel.

- le recours à des services tiers pour la Data Room suppose de vérifier si le prestataire offre un cadre de protection adéquat, notamment en termes de sécurité IT, en particulier en cas d'hébergement sur des serveurs localisés hors de l'UE, mais également en termes de confidentialité, de disponibilité, d'accessibilité etc. ; à cet égard, les services de type « Cloud », qui impliquent généralement une certaine dissémination des données et peu de visibilité sur leur localisation, sont dans la plupart des cas à proscrire.

- il peut être recommandé de prévoir un contrat de transfert de données entre l'importateur (l'acheteur) et l'exportateur de données (la cible/le vendeur), sur la base de clauses-type de la Commission Européenne, notamment en cas de transfert de données sensibles – étant précisé que, conformément à la doctrine de la CNIL, le simple accès à distance à des données à caractère personnel peut être considéré comme un transfert.

2. Identifier le niveau de risque en fonction de l'opération

Dans le cadre d'une opération de M&A, le niveau de risque auquel est exposé la cible au regard du droit de la protection des données peut s'apprécier en fonction de trois critères.

Premier critère, le type de transaction : le cas d'une simple prise de participation, la cible conserve sa personnalité juridique et la qualité de « responsable de traitement », en charge de la conformité des traitements qu'elle met en œuvre pour les besoins de ses activités. L'opération est donc relativement neutre en termes d'exposition au risque. À l'opposé, dans le cadre d'une cession d'actifs ou de fonds de commerce, l'acquéreur a vocation à devenir responsable de traitement pour l'ensemble des bases de données qui lui seront normalement transférées à l'issue du closing, ce qui soulève plusieurs problématiques : les conditions de licéité du transfert de données à l'issue du closing, la nécessaire mise à jour de la documentation juridique afférant à ces traitements, la compatibilité des politiques et des processus appliqués à l'origine sur ces données avec ceux de l'acquéreur, l'intégration technique de ces données dans les systèmes IT de l'acquéreur etc. Dans cette hypothèse, le risque en termes de données à caractère personnel est naturellement bien plus important.

Deuxième critère, le type d'activité de la cible : L'acheteur doit d'emblée chercher à comprendre l'importance des données à caractère personnel dans le business-model de la cible. En effet, une société exclusivement consacrée à des activités B2B dans le domaine, par exemple de l'industrie, mettra en œuvre - a priori - un nombre limité de

traitement de données de personne physiques. Le niveau de risque sera donc relativement faible. À l'inverse, une société dont les activités s'articulent essentiellement autour de l'analyse des données de personnes physiques, le Big Data, le profilage, la digitalisation, l'analyse de données sensibles telles que des données de santé, ou encore la personnalisation de contenus et services, impliquera un niveau de risque plus élevé.

Troisième critère, les modes d'organisation internes de la cible : pour des raisons stratégiques ou du seul fait de l'application de la loi, certaines sociétés sont amenées à mettre en œuvre des traitements impliquant une surveillance étroite des activités de leurs collaborateurs ou de leurs clients, des outils d'analyse comportementale des systèmes de détection automatique des fraudes, à l'image par exemple d'une banque et plus généralement des établissements soumis à un contrôle interne renforcé. Dans cette hypothèse, le risque de non-conformité peut être plus élevé. A l'inverse, une société se limitant à mettre en œuvre des traitements « classiques » liés à l'émission des bulletins de salaires, à la mise à disposition d'outils informatiques ou encore à des applications de gestion de carrière sera moins exposée au risque de non-conformité.

En fonction de ces critères, l'acquéreur pourra déterminer si la protection des données est un sujet-clé ou au contraire un sujet mineur dans le cadre de la transaction.

3. Évaluer le niveau de conformité de la cible et obtenir les garanties appropriées

Dans le cadre d'une opération de M&A, un audit complet des traitements de données à caractère personnel n'est pas envisageable. Une telle mission implique un travail sur le long terme, supposant une connaissance approfondie de l'entreprise, un accès exhaustif aux ressources de l'entreprise, une analyse précise des écarts avec le GDPR pour chaque traitement, le tout dans le but de préparer les grandes lignes d'un plan de régularisation.

Au demeurant, le cadre légal reste incertain : d'une part, les autorités de protection des données publient régulièrement des documents d'orientation destinés à clarifier les dispositions parfois complexes du GDPR, et d'autre part, les lois nationales de coordination attendues à l'origine pour 2017 ne sont pas prêtes de voir le jour.

En d'autres termes, le seul objectif réaliste, dans ce contexte est d'obtenir une vision globale du niveau de conformité de la cible, d'évaluer le niveau de risque général et d'obtenir les garanties nécessaires pour minimiser ces risques. Dans ce cadre, les étapes suivantes constitueront des « passages obligés » :

- cartographie des traitements de données, par catégorie (RH, Client etc.) ;
- inventaire des récépissés de formalités préalables réalisées ;
- analyse des notes d'information/politique de vie privée fournies aux personnes concernées, en ce compris le cas échéant, les clauses « protection des données » dans les contrats-clés (contrats d'abonnement, contrats de travail, etc.) ;
- vérification de l'existence de pratiques et politiques de sécurité IT pour protéger les données (gestion des incidents, clauses-type avec les prestataires, historique des incidents de sécurité, plans de sauvegarde, de reprise et/ou continuité, audits, certification, sensibilisation/formation du personnel etc.) ;
- vérification de l'existence de cadres contractuels en place pour les transferts de données hors UE au sein du Groupe et à l'extérieur du Groupe.

Sur la base du rapport d'audit, l'acquéreur pourra tenter d'obtenir les garanties suivantes :

- conformité globale aux lois et règlements applicables en matière de protection de données notamment au regard des exigences relatives aux formalités préalables, à l'information des personnes, à la confidentialité et sécurité des données, aux transferts internationaux de données etc.) ;
- existence de politiques et procédures appropriées pour assurer la conformité des traitements aux lois et de mesures techniques, logiques et organisationnelles destinées à assurer la sécurité et la confidentialité des données ;
- absence d'action ou réclamation, y compris de la part des autorités administratives ou judicaires alléguant une violation des lois applicables ; absence de violation de la sécurité des données ;
- garantie que la réalisation et la négociation de la transaction, ainsi que la livraison ou l'exécution des documents ne constitueront en aucun cas une violation des lois applicables en matière de protection des données.

Naturellement, de telles garanties auront vocation à être limitées : plafond global d'indemnisation, seuil minimal pour le montant des dommages pouvant donner lieu à réparation, date de prescription conventionnelle. De même, la divulgation explicite de certains faits, risques ou manquement dans les documents fournis durant l'audit implique généralement que ces faits soient exclus du champ des garanties et du périmètre de l'indemnisation.

Dans tous les cas, une expertise dans l'identification des risques en matière de protection des données s'avérera indispensable pour éviter les pièges et les « deal-breaker » à toutes les étapes de l'opération.