

Le traitement de données à caractère personnel à l'épreuve des opérations d'acquisition

Les "data rooms" virtuelles sont de plus en plus utilisées dans le cadre d'opérations d'acquisitions. Elles offrent une grande souplesse géographique en permettant notamment la consultation simultanée de documents par plusieurs personnes situées en des lieux différents. Le gain de temps et d'argent peut ainsi être considérable, surtout dans le cadre de négociations internationales.

Les sociétés soucieuses de garantir la confidentialité de leurs affaires et d'assurer une sécurité de leurs données voudront toutefois limiter l'accès aux seules personnes autorisées et interdire la reproduction des documents consultés. C'est ainsi que plusieurs prestataires se sont spécialisés dans la fourniture de plates-formes informatiques prêtes à l'emploi, permettant un tel usage sécurisé. Cependant, qu'elles soient virtuelles ou non, les "data rooms" sont aussi l'occasion de transmettre aux acheteurs potentiels des informations qui peuvent tomber sous le coup de la loi du 2 août 2002 relative à la protection des données à caractère personnel (la "Loi"). C'est notamment le cas des données relatives à des personnes comme par exemple les fournisseurs, les clients et, plus particulièrement encore, les employés du vendeur.

Ainsi par exemple, il n'est pas rare dans le cadre d'une acquisition de société que le vendeur garantisse que "La société n'a pas d'autres employés (que ce soit à titre temporaire ou permanent, dans le cadre de contrats de travail, de contrats d'intérimaire ou de contrats de service) que ceux listés en annexe du présent contrat". Une telle clause est-elle en accord avec les droits des employés? Le caractère international de l'opération, qui appelle souvent l'utilisation de "data rooms" virtuelles, n'est-il pas justement de nature à rendre ce transfert encore plus difficile au regard de la Loi? En effet, lors d'un transfert de données à caractère personnel, plusieurs principes doivent être respectés, dont certains sont de nature à rendre la transaction envisagée difficile sinon impossible en pratique, particulièrement si la possibilité de transmettre confidentiellement des données à caractère personnel dans le cadre d'une opération d'acquisition n'a pas été anticipée.

Quels sont les principaux principes à respecter?

Principe de licéité et de légitimité

Le traitement de données à caractère personnel ne peut avoir lieu que s'il est licite (c'est-à-dire qu'il respecte l'ensemble des principes et obligations à charge du responsable du traitement) et poursuit un intérêt légitime (il existe

de cinq cas limitativement énumérés par la Loi). Deux cas de légitimité peuvent être applicables aux traitements réalisés dans le cadre d'une acquisition de société: le consentement de la personne concernée ou l'intérêt légitime de la société. Le consentement doit avoir été donné à la suite d'une information claire sur les circonstances du traitement, ce qui signifie que la personne concernée doit avoir été informée du transfert potentiel de ses données dans le cadre d'une acquisition. Or, cela est rarement le cas et en raison de la volonté de ne pas rendre l'opération publique mais aussi parfois en raison du nombre de personnes concernées, on se tourne en principe vers l'intérêt légitime pour justifier le traitement de données à caractère personnel. Cet intérêt légitime sera néanmoins apprécié subjectivement, au regard des risques d'atteintes aux droits et libertés fondamentales des personnes concernées par le traitement. Ainsi, la communication des contrats de travail d'employés dans le but d'assurer la continuité de leur travail pourrait être vue comme justifiable au regard de la condition de l'intérêt légitime.

Un troisième cas de légitimité peut encore intervenir selon les circonstances. En effet, certaines législations particulières, comme la protection des travailleurs dans le cadre du transfert d'entreprise (mieux connue sous l'acronyme TUPE pour "Transfer of Undertaking - Protection of Employment"), prévoient la communication d'informations par le vendeur. Il s'agit là d'une obligation légale qui sera de nature à justifier le traitement, sans toutefois exempter le responsable du traitement des formalités administratives qui lui incombent (voir plus bas). Lors de la mise en œuvre du traitement, le responsable du traitement doit également assurer la sécurité et la confidentialité de celui-ci.

Respect des droits de la personne concernée

Le responsable du traitement doit respecter les droits des personnes concernées (droit à l'information - voir ci-dessous, droit d'accès et de rectification et droit d'opposition).

Principe de transparence

Informations des personnes concernées

Il faut principalement informer les personnes concernées de l'identité du destinataire des données et des buts du traitement. En général, l'information préalable est communiquée lors de la collecte des données auprès des personnes concernées. Très souvent, à ce stade, l'opération d'acquisition n'a pas été anticipée et une nouvelle information est alors nécessaire, ce qui peut en soi poser problème dans le cadre d'une transaction confidentielle que les parties voudraient, dans un premier temps en tout cas, dévoiler à un nombre de personnes le plus limité possible. Parfois même, le prix de l'acquisition pourrait être affecté si les travailleurs sont préalablement informés de la transaction.

Concernant les employés, l'idéal serait donc apparemment de prévoir dans le contrat de travail même, par une clause d'information spécifique, l'éventualité d'un transfert de données dans le cadre d'une opération d'acquisition, de fusion ou toute autre opération similaire qui constituerait une opportunité pour l'entreprise. Il est toutefois difficile de rédiger une telle clause à l'avance car assumant que l'information sera suffisamment détaillée pour conférer au traitement un caractère licite et légitime face à une situation concrète. On pourrait également envisager une information dans le règlement intérieur ou via l'intranet de la société, sachant toutefois que la preuve de la communication des informations incombe au responsable du traitement. Quoi qu'il en soit, il ne semble pas nécessaire pour l'employeur d'effectuer une information distincte de celle en principe réalisée dans le cadre du traitement des données nécessaires à la gestion du personnel. La simple mention d'un éventuel transfert de ces données à un acheteur potentiel, dans le cadre d'une information plus générale, semble être suffisante.

Information de la CNPD

Préalablement à la mise en œuvre du traitement, le responsable doit remplir certaines formalités administratives auprès de la Commission pour la Protection des Données.

Selon les cas, il s'agira d'une notification ou une demande d'autorisation. L'autorisation sera par exemple requise lorsqu'un transfert de données est envisagé vers un pays situé hors de l'Union Européenne et n'assurant pas un niveau de protection adéquat. Cela peut se produire dans le cadre d'une transaction internationale, impliquant un acheteur étranger. Des exceptions existent, comme par exemple le transfert à des sociétés établies aux Etats-Unis et ayant adhéré aux principes dits de "Safe Harbor" ou encore pour des transferts ayant lieu dans le cadre de "Corporate Binding Rules", c'est-à-dire de règles contraignantes qui s'appliquent aux sociétés d'un même groupe.

Il existe également des cas d'exemptions à ces formalités administratives, mais aucun ne permet le transfert de données à des tiers ou hors du Grand-duché de Luxembourg, ce qui réduit leur intérêt dans le cadre d'une acquisition. Ainsi, l'employeur devra renoncer à l'exemption prévue par la Loi pour les traitements nécessaires à la gestion des employés. En effet, cette exemption n'est plus applicable lorsque les données sont transférées à des tiers.

Très souvent, les formalités administratives n'ont pas été accomplies au moment de l'entrée en négociation de l'opération d'acquisition, alors même que la Loi insiste sur leur caractère préalable. Lors de la phase de "due diligence", il est en général trop tard. Le processus d'acquisition étant confidentiel, les vendeurs ne peuvent entreprendre les formalités à ce stade, d'autant plus que leur accomplissement demanderait un certain temps, élément qui fait généralement défaut lors d'une acquisition.

Quelles solutions, en pratique, pour le vendeur?

Lorsque les formalités préalables à la communication des données n'ont pas été effectuées, l'employeur peut anonymiser ces données avant de les communiquer à l'acheteur puisque la loi ne s'applique qu'aux seules données à caractère personnel, c'est-à-dire aux données qui concernent une personne identifiable ou susceptible d'être identifiée. Une donnée anonymisée ne saurait donc par nature se rapporter à une personne identifiable. Mais il est important de noter que bien souvent il ne suffit pas de retirer les noms des personnes concernées pour que les données soient anonymes. En effet, une personne peut tout à fait être identifiable, par recoupement, sans que son nom ne soit communiqué. Ainsi, on pourrait, dans le cadre d'une petite équipe par exemple, identifier une personne par son âge, son ancienneté ou son titre. Dans ce cas, il s'agit de données qui devraient également être omises en cas de transfert d'informations en relation avec cette personne, au même titre que son nom et son prénom. Par la suite, si l'acheteur souhaite absolument obtenir le nom de certaines personnes (par exemple parce que leur identité peut avoir un impact sur sa décision), l'information préalable des personnes concernées ainsi que les formalités requises devront être effectuées.

Dans tous les cas, le vendeur limitera utilement la communication d'informations à:

- des données anonymisées uniquement, dans la mesure du possible ;
- ce qu'il est absolument nécessaire de communiquer ;
- l'acheteur interne ou aux acheteurs restant sur la "short list" ;
- la consultation uniquement, sans copie possible.

L'acheteur lui aura aussi tout intérêt à ce que ces principes soient respectés puisqu'en tant que destinataire des données il procédera lui aussi à un traitement de ces données et devra par conséquent respecter également les conditions de la Loi. Les parties ont donc toutes deux intérêt à ce que la communication d'information se fasse dans le cadre d'un accord de confidentialité prévoyant au minimum que les données communiquées ne pourront être transférées à d'autres personnes qu'au sein d'un environnement sécurisé et qu'elles seront détruites une fois devenues inutiles.

A l'issue de l'opération d'acquisition, des données seront transférées à l'acheteur, à moins qu'il ne s'agisse seulement d'un transfert d'actions, auquel cas les données restent en principe au sein de la société achetée dont les actions seules sont transférées (sauf si l'acheteur souhaite néanmoins y avoir accès). A ce titre, l'acheteur devra lui aussi se conformer aux règles applicables en la matière.