LIAISONS SOCIALES QUOTIDIEN

COUNTRY: France
PAGE(S) :1-3
SURFACE :210 %
FREQUENCY : Daily

CIRCULATION :(18597)
AVE :24,57 K€

► **3 October 2024 - N°19012 - Dossier pratique**

Sort des données personnelles en cas de transfert d'entreprise

Le transfert d'entreprise est une situation courante qui peut concerner toutes les sociétés. En 2023, plus de 10000 ont été enregistrés en France, illustrant l'importance de ce processus pour l'économie. Quelles précautions faut-il prendre avant et après le transfert? Quels sont les risques encourus en cas de manquement aux règles du RGPD (règlement général de protection des données) ?

Dossier réalisé par Élise Dufour, avocat associé, Bignon Lebray Avocats, département Pint, pour Les Cahiers du DRH.

1 Rappels

PRINCIPAUX CAS DE TRANSFERT

Le transfert d'entreprise, tel que défini par le Code du travail *(C. trav., art. L. 1224-1)*, implique le **transfert** des **contrats de travail** en cas de changement d'employeur, à condition que l'**entité économique conserve** son **identité** et que son **activité** soit poursuivie ou reprise. Les principaux cas de transfert d'entreprise comprennent :

– la vente d'entreprise : elle implique le **transfert** de la **propriété** de celle-ci d'un vendeur à un acheteur. Juridiquement, cela entraîne le transfert des actifs, des passifs et des contrats de travail en cours. Le nouvel employeur est tenu de respecter les contrats de travail existants ;

– la fusion d'entreprises : elle consiste en la « **combinaison** » de deux **entreprises en une seule entité** juridique. Cela peut se faire par absorption (une entreprise en absorbe une autre) ou par création d'une nouvelle société issue de la fusion des deux. Cette dernière implique le transfert automatique des contrats de travail à la nouvelle entité, et l'article L. 1224-1 garantit la continuité des droits contractuels des salariés ;

– la transformation d'un fonds de commerce : elle peut intervenir lors de la conversion d'une entreprise individuelle en société. Dans ce cas, tous les actifs et passifs de l'entreprise individuelle, y compris les contrats de travail, sont transférés à la nouvelle société. Cette opération requiert souvent des formalités juridiques spécifiques pour assurer le transfert de tous les éléments de l'entreprise ;

– la succession d'entreprise : lorsqu'une entreprise est transférée à la suite du **décès** de l'exploitant (dans le cas d'une entreprise individuelle) ou par héritage, les héritiers ou le nouveau propriétaire doivent continuer à en assurer la gestion. Les contrats de travail sont maintenus sous les mêmes conditions qu'auparavant, assurant ainsi la continuité de l'emploi pour les salariés ;

– l'incorporation d'entreprise : elle implique la **création** d'une **nouvelle entité juridique** pour exploiter l'entreprise. Les actifs, passifs et contrats de travail de l'entreprise initiale sont transférés à la nouvelle société.

EXIGENCE INDUITE PAR LE RGPD

Le transfert d'entreprise est un **processus complexe** nécessitant une attention particulière aux droits des salariés pour garantir la continuité de l'emploi et des conditions de travail. Il implique la **transmission** des **données personnelles** des **collaborateurs** et des **clients**, dont la gestion est cruciale dans un environnement de plus en plus digitalisé.

Ce transfert met en lumière **différentes problématiques** qu'il convient d'analyser pour se conformer au cadre légal de la protection des données, en particulier le 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 (RGPD).

2 Analyse *ex-ante* de l'entreprise : audit

Lors de la transmission d'une entreprise, le respect de la législation sur la protection

LIAISONS SOCIALES QUOTIDIEN
COUNTRY:France
PAGE(S) :1-3
SURFACE :210 %
FREQUENCY :Daily
CIRCULATION :(18597)
AVE :24,57 K€
► 3 October 2024 - N°19012 - Dossier pratique

des données personnelles, notamment le règlement général sur la protection des données (RGPD), revêt une importance capitale.
Pour le **cessionnaire**, effectuer un **audit préalable** des **données** des **salariés** n'est **pas seulement** une **obligation légale**, **mais** également une **mesure stratégique** essentielle. Cet audit permet de déterminer si toutes les données transmises sont traitées de manière conforme, protégeant ainsi les droits des salariés et évitant de potentielles sanctions. En outre, il offre à ce dernier une compréhension claire des pratiques de gestion des données en place, ce qui est fondamental pour diriger l'entreprise acquise en toute sérénité et pour instaurer une relation de confiance avec les employés.
Un **audit rigoureux** et bien mené constitue donc un **pilier fondamental** dans le processus de transmission, permettant au cessionnaire de se prémunir contre les risques juridiques et opérationnels liés à la protection des données personnelles.
Sont déclinés ci-après les points d'attention sur lesquels doit porter l'audit.

INFORMATIONS ET DOCUMENTATION

Des questions essentielles devront être posées au cédant (le vendeur), et il conviendra de lui **demander** l'**accès** à certains **documents**.
La première d'entre elles est celle du **nombre** de **salariés**, les entreprises dépassant un certain seuil étant tenues à certaines obligations réglementaires ayant des impacts RGPD et nécessitant la réalisation d'analyses.
Par ailleurs, le fait de savoir **si** un **délégué à la protection des données** (DPO) (DPO est le vocable le plus couramment utilisé même si, en France, il serait plus juste de dire DPD) a été **nommé** et, si oui, s'il est **interne ou externe**, paraît également pertinent.
Une autre question utile pourrait être de savoir si des **contentieux** sont **en cours** avec des salariés ou d'anciens salariés au titre du traitement des données.
Enfin, savoir si une **faille** de **sécurité impliquant** les **données** de **salarié**(s) a eu lieu lors des 24 derniers mois semble également utile.
S'agissant de l'accès à des documents, il conviendra de demander s'il existe :
– un **registre des traitements** pour la partie RH ;
– la **liste et** la **copie des politiques et procédures**, et notamment celle en termes de gestion des droits d'accès, des durées de conservation, des habilitations, ainsi que l'existence de politique de confidentialité pour les salariés et de charte informatique.

NATURE DES DONNÉES

Une fois ce « mapping » général effectué, il conviendra de **vérifier** plus en détail la nature des **données traitées** et s'assurer que certaines d'entre elles ne le sont pas par l'employeur cessionnaire. La nature des données est en effet un enjeu primordial, **car certaines** sont **interdites** (cartes d'identité ou passeport et copie de carte vitale ou copie de permis de conduire).
En plus de cela, le RGPD impose une **protection drastique** de celles dites « sensibles ». Ainsi, sauf exceptions limitées, l'employeur n'a pas à collecter des données sur la santé ou sur la vie intime d'un salarié, sur son origine ethnique, sur ses convictions religieuses, politiques, syndicales, philosophiques.

SÉCURISATION DES INFRASTRUCTURES

La sécurité des données parait enfin l'autre enjeu majeur sur lequel le responsable de traitement doit s'attarder et **s'interroger**, en ce qu'il **s'agit** d'un **élément essentiel** de la **protection** des données personnelles.
Elle **s'impose à tout responsable** de **traitement** et **sous-traitant** à travers le RGPD *(RGPD, art. 32)*. En principe, chaque traitement doit faire l'objet d'un ensemble de mesures de sécurité décidées en fonction du contexte, à savoir « des précautions utiles, au regard de la nature des données et des risques présentés par le traitement » selon la loi Informatique et libertés *(L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés, art. 121)*. Le RGPD précise que la protection des données personnelles nécessite de prendre les « **mesures techniques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté au risque » pour les droits et libertés des personnes physiques, notamment leur vie privée.
Dans le cadre de traitement de données RH au sein d'une entreprise, il conviendrait de sensibiliser et authentifier les utilisateurs, gérer les habilitations, tracer les accès tout en gérant les incidents, ou encore de sécuriser le réseau, les postes de travail... La Cnil a d'ailleurs pu sanctionner Amazon d'une amende de 32 millions d'euros sur ce motif, en considérant que l'accès au logiciel de vidéosurveillance n'était pas suffisamment sécurisé, puisque le mot de passe d'accès n'était pas d'une robustesse suffisante et que le compte d'accès était partagé entre plusieurs utilisateurs *(Cnil, délib. de la formation restreinte n° SAN-2023-021, 27 déc. 2023)*.

ENJEUX DES VÉRIFICATIONS

Ces vérifications préalables sont indispensables, car c'est le **cessionnaire** qui **assumera** l'ensemble des obligations et **responsabilités** relatives aux traitements de données à caractère personnel.
En effet, les sanctions en cas de non-conformité sont non négligeables. Le RGPD prévoit ainsi une **amende administrative** pouvant s'élever **jusqu'à 20 000 000 €** ou, dans le cas d'une entreprise, jusqu'à **4 %** du **chiffre d'affaires annuel mondial** total de l'exercice précédent *(RGPD, art. 83.5)*. Cette sanction peut, en sus, se doubler d'une action personnelle intentée par la personne lésée par le manquement, qui devra être indemnisée pour son entier préjudice. Outre ces aspects financiers, la réputation et la confiance envers l'entreprise peuvent être gravement affectées dans de telles hypothèses.
L'intérêt économique n'est d'ailleurs pas étranger à cet audit préalable, car s'il produit des résultats non satisfaisants, les charges de remise à niveau viendront baisser la valeur de l'entreprise.

GARANTIE ACTIF/PASSIF NÉCESSAIRE

Pour s'assurer une certaine tranquillité en cas de doute ou d'absence de vérification sur les choix de gestion du dernier responsable de traitement, il conviendrait de négocier avec le cédant une **garantie** de **passif**. En effet, la conduite de l'ancien responsable de traitement peut entraîner des conséquences fâcheuses indécelables au moment de la cession et qui apparaissent dans le temps... Cette clause permet ainsi de quantifier,

LIAISONS SOCIALES QUOTIDIEN
COUNTRY:France
PAGE(S) :1-3
SURFACE :210 %
FREQUENCY :Daily
CIRCULATION :(18597)
AVE :24,57 K€
► 3 October 2024 - N°19012 - Dossier pratique

d'anticiper et d'annihiler tous les risques RGPD auxquels le repreneur est exposé.

CHAÎNE DE RESPONSABILITÉS

Le RGPD dispose que « le **responsable** du **traitement** met en œuvre des **mesures techniques et organisationnelles appropriées** pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement » *(RGPD, art. 24)*. Il ajoute que « ces mesures sont **réexaminées et actualisées** si nécessaire ». En outre, il indique que « tout responsable de traitement ayant participé au traitement est **responsable** du **dommage causé** […] » par ce dernier lorsqu'il constitue une **violation** du **RGPD**. Dès lors, **en cas de reprise** d'un traitement vicié préexistant par un **nouveau responsable**, ce dernier assumera les erreurs de son prédécesseur, ne serait-ce que parce qu'il n'a pas réagi au(x) manquement(s) constaté(s) *(RGPD, art. 82)*.

Dans cette logique de « suivi de la responsabilité » post-transfert, la Cnil italienne « Garante per la protesione dei dati personali » a sanctionné une entreprise cessionnaire à une amende de 1 400 000 € pour absence de consentement des personnes concernées, couplée à une violation du principe de « finalité et de limitation », des violations pourtant perpétrées prétransfert, sous la responsabilité de l'entité cédée *(Ordinanza ingiunzione nei confronti di Douglas Italia S.p.A., 20 ottobre 2022)*.

Cette ordonnance n'est pas sans rappeler un arrêt français, certes un peu daté, de la Cour de cassation du 25 juin 2013 qui affirmait, sous le visa de l'article 22 de la loi Informatique et libertés de l'époque, le principe selon lequel un fichier informatisé contenant des données à caractère personnel n'ayant pas fait l'objet d'une déclaration à la Cnil se trouvait « hors du commerce », de sorte que la vente portant sur un tel fichier devenait nulle pour avoir un objet illicite *(Cass. com., 25 juin 2013, nº 12-17.037)*. Si ce risque spécifique n'est plus d'actualité en raison du principe d'Accountability, privilégiant un régime de responsabilisation à celui de la déclaration, il semble toujours avéré qu'un risque non révélé de non-conformité au RGPD puisse annuler une vente. Cette décision souligne l'importance d'une véritable conformité à la réglementation en vigueur.

3 Gestion de la conformité *ex-post*

Après l'acquisition, il est **conseillé** d'**informer** les **salariés** des **changements**, y compris la **nouvelle politique** de **confidentialité**. Toute la **documentation** et le **registre** des traitements doivent être **mis à jour** en conséquence.

Le nouveau responsable de traitement doit également **garantir** la **conformité** des **pratiques** de l'entreprise cédante. Cela inclut le respect des durées de conservation des données, notamment en prévoyant une période de cinq ans à compter du départ du salarié pour conserver les données pertinentes.

Le nouvel employeur se retrouvera alors avec des données à caractère personnel qui n'ont pas été collectées auprès de la personne concernée au sens de l'article 14 du RGPD. Le **responsable** du traitement sera alors tenu de **fournir** à l'intéressé(e) plusieurs **informations** parmi lesquelles :

– l'**identité** et les **coordonnées** du **responsable** et/ou du délégué à la protection ;

– les **finalités** auxquelles sont destinées les données (gestion de la relation client, inscription au programme de fidélité…), ainsi que la base juridique s'y affiliant.

Il est également nécessaire de préciser les **catégories** de **données** concernées (nom, prénom, courriel, adresse, numéro de téléphone…) et les destinataires de ces données.

4 Archivage par le cédant des données transférées

La question de savoir si l'entreprise cédante peut, ou même doit, conserver une sauvegarde des fichiers informatiques n'est à ce jour pas réglée. Ni le RGPD, ni le référentiel RH de la Cnil ne l'envisagent.

ARGUMENTS EN FAVEUR D'UNE RÉPONSE NÉGATIVE

Les partisans d'une réponse négative s'appuient non pas sur un texte formel du RGPD imposant au cédant de ne pas conserver les données relatives à ses anciens salariés, mais sur l'**esprit** de ce **règlement** qui veut que la collecte de données personnelles soit liée à l'accomplissement d'une obligation du responsable de traitement. Pour eux, l'entreprise sortante n'ayant plus à gérer les salariés transférés n'a plus de légitimité à conserver ces données.

ARGUMENTS EN FAVEUR D'UNE RÉPONSE POSITIVE

Les tenants de la thèse contraire invoquent les **obligations** de **conservation** des **archives** qui sont **pénalement sanctionnées**.

Ils soulignent également qu'ils ne sont pas à l'abri d'une **action en justice** intentée **par** un **ancien salarié** en raison de manquements supposés, dont certains peuvent remonter à une époque lointaine, sachant que le délai de prescription de l'action ne débute qu'à la date où le salarié a eu ou aurait dû avoir connaissance des faits fondant sa revendication.

À cet argument, on opposera qu'il est toujours possible de demander au cessionnaire communication des informations nécessaires, mais cela suppose parfois un véritable traçage du dossier d'un salarié qui peut avoir été à nouveau transféré. L'ancien employeur, qui n'aura pas réussi à se procurer les renseignements et pièces lui permettant de se défendre, n'aura d'autre recours que de demander au juge une mesure d'instruction sur la base de l'article 145 du Code de procédure civile.

Un audit rigoureux et bien mené constitue un pilier fondamental dans le processus de transmission, permettant au cessionnaire de se prémunir contre les risques juridiques et opérationnels liés à la protection des données personnelles.