CLARA-ANN GORDON
LUISA EGLI

PROTECTION DES DONNÉES ET TRANSMISSION D'ENTREPRISE

Les enjeux liés au droit de la protection des données lors de la cession et du rachat de PME

Lors d'une transmission d'entreprise, l'attention se porte d'abord sur l'évaluation, la fiscalité ou le contrat. La protection des données passe souvent au second plan. Or, une telle opération implique le transfert de nombreuses données personnelles. Les fiduciaires sont concernés à double titre: dans leur activité de conseil et lors de la cession de leur propre entreprise.

1. INTRODUCTION

La transmission d'entreprise est un enjeu majeur en Suisse: des milliers de PME changeront de mains au cours des prochaines années pour des raisons d'âge, de considérations familiales ou de nouvelles opportunités stratégiques.

On oublie souvent qu'une transmission d'entreprise implique également le transfert d'un grand nombre de données personnelles. Listes d'effectifs, dossiers clients, registres des actions, toutes ces informations sont remises au repreneur dans le cadre de la transaction. Les exigences en matière de protection des données qui en découlent nécessitent une planification des plus minutieuses.

La transmission d'entreprise place les fiduciaires devant un double défi: conseiller leur clientèle et préparer, le cas échéant, la cession de leur propre entreprise.

2. FONDEMENTS JURIDIQUES

La nouvelle loi sur la protection des données (LPD) est entrée en vigueur en Suisse le 1er septembre 2023. Elle avait été précédée par un débat houleux, marqué par la crainte d'une surcharge administrative disproportionnée pour les PME [1]. Parmi les principales nouveautés de la loi, citons l'abandon de la protection des personnes morales, des devoirs étendus d'information et de renseignement, l'obligation d'annoncer toute infraction à la protection des données de même que des amendes pouvant atteindre CHF 250 000 à l'encontre de dirigeants fautifs [2].

Le Règlement général sur la protection des données (RGPD) de l'Union européenne a un effet uniquement indirect ou extraterritorial pour la Suisse [3]. La LPD révisée s'appuie toutefois largement sur le RGPD de façon à aligner le niveau de protection des données sur celui de l'Europe et à obtenir la décision d'adéquation importante de l'UE [4].

La LPD pose plusieurs principes de traitement qu'il convient d'observer également dans un contexte de transmission d'entreprise:

→ Tout traitement de données personnelles doit être licite et conforme aux principes de la bonne foi (art. 6, al. 1 et 2, LPD).

→ Le principe de limitation de la finalité exige que les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée (art. 6, al. 3, LPD).

→ La proportionnalité exige que seules les données nécessaires à la finalité poursuivie peuvent être traitées (art. 6, al. 2, LPD), ce qui inclut notamment le principe de limitation des données.

→ Les données personnelles doivent être exactes (art. 6, al. 5, LPD) et leur sécurité garantie par des mesures organisationnelles et techniques appropriées (art. 8 LPD) [5].



CLARA-ANN GORDON,
AVOCATE, LL.M., ASSOCIÉE,
BÄR & KARRER



LUISA EGLI, AVOCATE,
LL.M., COLLABORATRICE,
NIEDERER KRAFT FREY

Contrairement au droit européen basé sur un régime d'interdiction assorti d'une réserve d'autorisation, le traitement des données par des personnes privées est en principe autorisé par la LPD. Une atteinte à la personnalité peut notamment résulter d'une violation des principes applicables au traitement des données, par exemple lorsque la personne concernée n'est pas suffisamment informée ou que le traitement des données est fait contre la volonté expresse de la personne (art. 30, al. 2, LPD). Une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant, ou par la loi (art. 31, al. 1, LPD) [6]. Ces motifs justificatifs jouent un rôle prépondérant dans la transmission d'entreprise, dans la mesure où le transfert de données personnelles nécessite habituellement une telle justification dans le cadre d'une due diligence [7].

Par ailleurs, il convient de ne pas oublier les obligations de garder le secret professionnel, légal ou contractuel ainsi que les dispositions du droit du travail en matière de traitement des données personnelles (art. 328*b* CO) [8].

3. SHARE DEAL OU ASSET DEAL?

La structure de transaction retenue a une incidence sur les questions de protection des données. Il convient dès lors d'examiner brièvement les principales formes de transaction:

→ S'agissant d'un *share deal*, l'acquéreur reprend l'ensemble de l'entreprise en achetant les actions ou les parts sociales de cette société [9]. L'élément déterminant est l'absence de changement de partie contractante: la société cible demeure partie au contrat et les données continuent de lui être exclusivement attribuées [10].

→ Lors d'un *asset deal*, l'acquéreur achète tout ou partie d'une entreprise en reprenant les actifs, les passifs et les rapports contractuels afférents [11], dont font notamment partie les immeubles, les machines, les données clients et les données du personnel ainsi que les droits de la propriété intellectuelle. Contrairement à un *share deal*, cette structure entraîne un changement de partie dans les contrats de travail et les autres contrats. Les données de la société cible sont ainsi transférées à l'acquéreur, avec les bases juridiques qui en régissaient jusqu'alors le traitement. Ce point doit être pris en compte lors de l'évaluation des mesures de protection nécessaires [12].

Il n'est pas rare que la transmission d'une PME se fasse sous la forme d'un *share deal*, dans la mesure où, sur le plan administratif, le transfert des parts sociales est plus simple que celui de l'ensemble de l'entreprise. Généralement, le choix se porte sur l'*asset deal* lorsque certains actifs ou certains passifs doivent être repris [13].

4. QUELLES SONT LES DONNÉES PERSONNELLES TRAITÉES?

Une transaction regroupe diverses procédures relevant de la protection des données, notamment la transmission de données à des tiers tels que des acheteurs potentiels ou leurs conseillers [14]. En règle générale, la société cible communique les données personnelles à l'acheteur potentiel, ce qui doit être qualifié de traitement de données [15]. Sont importantes ici les données du personnel, les données clients, les données fournisseurs, les données de partenaires commerciaux et les données marketing, de même que les données relatives au(x) propriétaire(s) de l'entreprise [16].

5. PROTECTION DES DONNÉES ET PHASES DE TRANSACTION

Chacune des phases de la transaction soulève diverses questions en matière de protection des données, de la préparation à la due diligence en passant par la conclusion du contrat, son exécution et son intégration ou une éventuelle interruption de la transaction.

5.1 Préparation et due diligence. La première phase de la transaction comprend le premier contact et la préparation, la due diligence par le repreneur constituant l'élément décisif [17].

Du point de vue économique, l'objet d'un achat d'entreprise est toujours l'entreprise proprement dite; c'est pour cette raison qu'un acheteur prudent voudra préalablement avoir un tableau complet de sa situation (cf. paragraphe 6) [18]. Les données pertinentes sont habituellement mises à disposition dans un espace de données virtuel à accès restreint [19]. Le vendeur n'est autorisé à divulguer de telles données à l'acheteur qu'aux conditions définies par la LPD en sachant qu'en vertu de la loi, une telle communication dans un espace virtuel de données est considérée comme une transmission entre deux ou plusieurs personnes responsables [20].

Dans la pratique, on assiste à une communication progressive des données de façon à réduire les risques liés à leur protection [21]. Dans ce contexte, il convient de rassembler et d'identifier les documents nécessaires pour la due diligence [22]. Dans la mesure où ils sont régulièrement tenus au courant des données opérationnelles et des relations personnelles des associés, les fiduciaires de PME jouent un rôle essentiel dans l'examen préliminaire et la préparation de l'espace numérique de données. Il convient de veiller à ce que la divulgation des données pendant la due diligence se limite à ce qui est nécessaire et justifié.

La phase de préparation présente un risque de diffusion de données personnelles à large échelle, soit parce qu'un acheteur sans réelle intention d'acquisition cherche avant tout à obtenir des informations, soit parce que l'entreprise, par négligence ou dans l'espoir d'en tirer un meilleur prix de vente, divulgue davantage de données personnelles que nécessaire. Le risque d'un tel parti pris est que l'acheteur potentiel tente de débaucher la clientèle ou le personnel concerné en cas d'échec des négociations.

Se pose en outre le problème de modification de la finalité étant donné que les données en question ont été recueillies pour une finalité différente et qu'elles sont traitées dans un but détourné de leur finalité dans le cadre de la due diligence. La société cible est en principe tenue d'informer en amont les personnes concernées du changement de finalité et du destinataire. Obtenir leur consentement est toutefois pratiquement impossible, un consentement général accordé à l'avance ne satisfaisant souvent pas aux exigences de consentement libre, révocable et suffisamment spécifique [23].

Tableau 1: **DUE DILIGENCE ET PROTECTION DES DONNÉES**

Niveau	État des lieux
Niveau des données	Notamment une vue d'ensemble de la nature et du volume de données personnelles traitées, des flux de données et de l'environnement informatique
Niveau organisationnel	Responsabilités, délégués à la protection des données et processus en cas de violation de la protection des données et de requêtes de personnes concernées, mesures de sécurité des données, analyses d'impact
Niveau documentaire	Notamment déclarations (externes) de protection des données, règlements (internes) de protection des données, règlements sur la conservation des données, accords de traitement des données conclus *(data processing agreements), data sharing agreements, intragroup data transfer agreements* et clauses contractuelles types européennes

Il convient donc de prendre les mesures suivantes [24]:
→ Les données personnelles doivent être anonymisées, pseudonymisées ou agrégées dans une large mesure; il suffit en règle générale de présenter des modèles de contrats plutôt que des documents individuels détaillés.
→ Le cercle des destinataires doit être limité et l'accès à l'espace numérique de données ou à certaines données particulièrement sensibles strictement restreint à un petit nombre de personnes (*clean room* ou espace ultra-sécurisé).
→ Il est recommandé de conclure des accords de confidentialité (*non disclosure agreements,* NDA) de même que des contrats de traitement et d'échange de données avec les gestionnaires de salles de données et les acheteurs potentiels.
→ Si l'acheteur ou le gestionnaire de salle de données se trouve hors de l'UE, les mesures nécessaires pour la divulgation transfrontalière doivent être prises, par exemple les clauses contractuelles types dans la version entérinée par le Préposé fédéral à la protection des données et à la transparence (PFPDT).
→ Les acheteurs devraient s'engager à détruire les informations en cas d'interruption des négociations.

5.2 Conclusion et exécution de contrat. Dans une deuxième phase, qui comprend la conclusion et l'exécution du contrat d'achat, l'acquéreur doit être considéré formellement de la même manière qu'un tiers jusqu'à l'exécution du contrat. Les données concernant l'entreprise peuvent lui être communiquées sans autre [25]. Là encore, il peut y avoir un risque de violation du principe de finalité ou de violation de la protection des données.

Selon les résultats de la due diligence, le contrat d'acquisition devrait notamment prévoir des garanties et des déclarations du vendeur en matière de protection des données, des clauses d'indemnisation ainsi que les mesures de protection des données à mettre en œuvre avant l'exécution de la transaction [26].

Après l'acquisition, il convient de vérifier que l'utilisation des données reprises demeure compatible avec les finalités pour lesquelles elles ont été collectées, de limiter leur accès aux seules personnes habilitées et, en cas d'incertitude juridique concernant leur nouveau traitement, d'informer les personnes concernées ou de solliciter leur consentement.

5.3 Reprise de fait et intégration. Durant la troisième phase, l'acheteur reprend de fait la société cible. Notons que la LPD ne prévoit aucun privilège explicite dévolu aux groupes; les communications de données au sein d'un groupe de sociétés doivent elles aussi respecter les principes applicables en matière de protection des données [27].

Une fois la transaction divulguée, les déclarations de protection des données existantes envers le personnel, la clientèle et les fournisseurs doivent être respectées. Les contrats de services transitoires *(transition service agreements)* peuvent être garants d'une transition fluide; le cas échéant, il convient d'informer activement le personnel, les clients et les fournisseurs du changement de propriétaire [28].

5.4 Interruption de la transaction. Si la transaction est interrompue, il faut s'assurer que l'acquéreur potentiel retourne ou supprime immédiatement les données mises à disposition dans le cadre de la structure de transaction. Cette obligation doit être inscrite dès le début dans l'accord de confidentialité.

6. MESURES DE VÉRIFICATION

Une due diligence en matière de protection des données commence par un état des lieux à trois niveaux (cf. *tableau*) [29].

Il convient en outre de déterminer dans quelle mesure l'entreprise a respecté la protection des données par le passé ou s'il y a eu des violations de cette protection. Dans ce contexte, il est important de savoir si l'entreprise a fait l'objet de demandes ou d'enquêtes officielles de la part des autorités en lien avec le respect de la protection des données et si des sanctions ont déjà été prononcées à son encontre.

Les risques identifiés doivent être classifiés: on peut remédier a posteriori aux risques maîtrisables (p. ex. absence de contrat ou de déclaration sur la protection des données). Les risques non maîtrisables (p. ex. violation passée de la protection des données) justifient une modification du prix d'achat, une clause d'indemnisation ou une solution d'assurance. En cas de *share deal*, il convient de veiller spécifiquement à ce que la conformité de l'entreprise cible en matière de protection des données fasse partie de l'acquisition; tout défaut caché peut s'avérer être un passif majeur après l'exécution du contrat [30].

7. PARTICULARITÉS DES SOCIÉTÉS FIDUCIAIRES EN TANT QU'OBJET DE RACHAT

Des exigences accrues s'appliquent lorsque la société cédante est une entreprise fiduciaire. Les fiduciaires sont tenues par le secret professionnel et traitent parfois des données clients particulièrement sensibles. La question se pose de savoir si les données clients peuvent être transmises sans le consentement préalable de ces derniers et comment procéder avec les clients actuels qui pourraient s'opposer à la reprise de la société fiduciaire.

Il est recommandé en pratique d'informer en amont la clientèle et de veiller à rédiger avec soin les contrats de transfert entre la fiduciaire cédante et la fiduciaire reprenante.

8. RECOMMANDATIONS PRATIQUES

Quelle que soit la phase de transaction, la protection des données doit toujours être observée:
→ une due diligence en matière de protection des données doit être effectuée,
→ la reprise de passifs/risques antérieurs doit être évitée, et
→ les garanties/assurances de conformité et les clauses d'indemnisation doivent être négociées dans le contrat d'achat.

Les points à observer concrètement par les fiduciaires figurent dans *l'Infobox*.

9. CONCLUSION

Négliger la protection des données lors d'une transmission d'entreprise expose à des risques considérables, susceptibles d'avoir des répercussions directes sur le prix d'achat et la responsabilité des parties. Les fiduciaires sont doublement concernés: lors de l'accompagnement de leurs clients ou en cas de cession potentielle de leur propre entreprise. Une entreprise, qui définit la protection des données comme partie intégrante du processus de transmission, protège l'organisation et les clients de risques évitables et se positionne comme un partenaire compétent dans un environnement transactionnel toujours plus exigeant. ■

Infobox: RECOMMANDATIONS PRATIQUES À L'INTENTION DES FIDUCIAIRES

→ **Anticiper:** la conformité en matière de protection des données ne relève pas exclusivement de la due diligence, mais débute dès que la transmission est décidée.
→ **Respecter la structure de la transaction:** le *share deal* et *l'asset deal* ont des conséquences différentes en termes de protection des données, notamment en ce qui concerne le transfert de données, le changement des rôles et les obligations d'information.
→ **Vérifier l'ensemble de données:** quelles sont les données personnelles disponibles? Où se trouvent-elles? Qui y a accès?
→ **Concevoir un espace de données professionnel:** sécurité, journal des accès, anonymat et principe du besoin de savoir.
→ **Combiner NDA et accords de traitement de données:** les accords de confidentialité devraient être complétés par des accords de traitement et/ou de partage de données.
→ **Se prémunir dans un contrat de vente:** garanties sur la protection des données, mécanismes d'adaptation du prix d'achat en cas de risques non maîtrisables et règlements relatifs à la suppression des données doivent faire partie du contrat.
→ **Tenir compte de l'après-clôture:** vérifier le principe de la finalité lors de l'intégration des données, modifier les déclarations de protection des données, informer la clientèle et le personnel.

Notes: 1) S. Husi-Stämpfli, A.-S. Morand, Protection des données, 2e édition, Zurich/Genève 2024 (ci-après Husi-Stämpfli, Morand, N ...), N 13. **2)** Dans l'ensemble, C.-A. Gordon, T. Lutz, M&A und Datenschutz, in: Diem (éd.), Mergers & Acquisitions XXII, Zurich/Bâle/Genève 2021, p. 141 ss (ci-après Gordon, Lutz, p. ...), p. 147. **3)** Husi-Stämpfli, Morand, N 20. **4)** Husi-Stämpfli, Morand, N 11. **5)** L. Dal Molin, K. Mattle, Datenschutz in M&A-Transaktionen, in: Dal Molin, Wesiak-Schmidt (éd.), Datenschutz im Unternehmen, Zurich/Saint-Gall 2023 (ci-après Dal Molin, Mattle, § 9 N ...), § 9 N 12 **6)** Cf. Husi-Stämpfli, Morand, N 293 ss. **7)** Cf. Gordon, Lutz, p. 149 ss. **8)** Dal Molin, Mattle, § 9 N 14. **9)** R. Tschäni, H.-J. Diem, M. Wolf, M & A Transaktionen nach Schweizer Recht, 2021 (ci-après Tschäni, Diem, Wolf, par. ...), par. 131 ss. **10)** M. Winkler, Datenschutz bei M&A Transaktionen, GesKR 2018, p. 124 ss (ci-après Winkler, p. ...), p. 127. **11)** Tschäni, Diem, Wolf, par. 194 ss. **12)** Winkler, p. 128. **13)** Tschäni, Diem, Wolf, par. 195. **14)** Gordon, Lutz, p. 149. **15)** R. Mathys, O. Triebold, Deals, Daten, Datenschutz, in: Olano (éd.), Jurisprudenz und Musik, Liber amicorum für Felix H. Thomann zum 80. Geburtstag, Zurich 2016, 0, 51 ss (ci-après Mathys, Triebold, p. ...), p. 61 s. **16)** Cf. Gordon, Lutz, p. 149 **17)** Winkler, p. 153 s. **18)** Winkler, p. 125. **19)** Winkler, p. 126. **20)** Cf. Gordon, Lutz, p. 154 s. **21)** Winkler, p. 153 s. **22)** Gordon, Lutz, p. 157. **23)** Cf. Gordon, Lutz, p. 158 ss; Mathys, Triebold, p. 63. **24)** Cf. Dal Molin, Mattle, § 9 N 24 s. et N 35 ss. **25)** Winkler, p. 125, p. 131. **26)** Cf. Dal Molin, Mattle, § 9 N 71 ss. **27)** Winkler, p. 132. **28)** Gordon, Lutz, p. 161. **29)** Cf. Dal Molin, Mattle, § 9 N 56 ss. **30)** Gordon, Lutz, p. 144; Mathys, Triebold, p. 55.