WilhelmGilliéron
AVOCATS

Auteur: Sandra Gerber | Le : 26 janvier 2020

Protection des données de l'employé – la période de l'engagement

Après la phase de recrutement qui a été traitée dans un précédent article, l'auteur soussignée s'intéresse maintenant à la protection des données de l'employé pendant la phase d'engagement.

Comme cela a été expliqué dans un précédent article intitulé « Protection des données de l'employé, la phase de recrutement », la protection des données est un sujet d'actualité, avec l'entrée en vigueur du Règlement Européen général sur la protection des données (RGPD) du 27 avril 2016 et le projet de modification de la Loi fédérale sur la protection des données (LPD) du 19 juin 1992. Ce sujet d'actualité touche notamment les employeurs.

Comme expliqué également dans le précédent article, le siège de la matière en droit du travail est l'article 328b du Code des Obligations (CO) qui renvoie expressément à la LPD. Selon cet article, « *L'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables* ». Ce principe s'applique aussi bien dans les rapports précontractuels, soit avant la conclusion du contrat de travail, que durant les rapports de travail, mais également à la fin des rapports de travail. Si le précédent article traitait de la phase de recrutement, le présent article traite de la phase d'engagement, soit la période pendant laquelle l'employeur et l'employé sont liés par un rapport de travail *(Le présent article se base principalement sur les ouvrages suivants : Philippe Carruzzo Le contrat de travail individuel, Commentaire des articles 319 à 341 du Code des obligations, 2009; Guide pour le traitement des données personnelles dans le secteur du travail, Traitement par des personnes privées, PFPDT, octobre 2014 ; Marie Major, Questions spécifiques – le droit d'accès de l'employé à son dossier personnel, in La protection des données dans les relations de travail, CERT 2017.)*

Dossier médical

L'employeur n'a aucun droit d'accès au dossier médical de l'employé même si ce dernier délie son médecin du secret médical.

Avec l'accord de l'employé, le médecin conseil de l'employeur peut cependant avoir accès au dossier médical. Il ne peut cependant que déterminer si l'employé est apte ou non à remplir sa fonction et il ne peut communiquer à l'employeur que l'aptitude ou non au travail.

Des exceptions sont possibles pour certaines professions. Ainsi, les questions par exemple en relation avec la séropositivité ou les tests de dépistage de drogue ou d'alcool ne sont autorisés que pour certaines professions et si cela présente des risques pour l'employé, les autres employés, les usagers ou des tiers (par exemple service de premier secours ou urgence, ou chauffeur professionnel, pilote, contrôleur aérien et personnel de la santé). L'employeur ne peut cependant pas avoir un accès direct au résultat. Comme mentionné ci-dessus, l'accès est réservé au médecin conseil *(Philippe Carruzzo Le contrat de travail individuel, Commentaire des articles 319 à 341 du Code des obligations, ad. art. 328b, p. 328; Guide pour le traitement des données personnelles dans le secteur du travail, Traitement par des personnes privées, PFPDT, octobre 2014, p. 10).*

Dossier personnel

Le dossier personnel de l'employé ne doit contenir que des données indispensables à l'exécution du contrat de travail.

Le dossier personnel peut contenir les documents suivants : documents et renseignement obtenus de manière licite pendant la phase de recrutement, test d'aptitude, comptes rendus des entretiens d'évaluation, avertissements ou blâmes, échanges de correspondances, décomptes d'heures supplémentaire, décompte des vacances, fiches de salaire, cours de perfectionnement, plan de carrière, certificats médicaux, lettre de résiliation, et éventuelle suite.

L'employeur n'est en principe pas obligé de déclarer ses fichiers au préposé (art. 11a al. 5 LPD).

L'employeur doit cependant déclarer ses fichiers s'il traite des profils de personnalité et données sensibles (art. 11 al. 3 LPD).

L'employeur n'a dans ce cas pas l'obligation de déclarer s'il a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers (art. 11 al. 5

LPD).

Le dossier du personnel doit être trié régulièrement, soit tous les deux ans selon le préposé afin d'en retirer les documents inutiles (Guide pour le traitement des données personnelles dans le secteur du travail, Traitement par des personnes privées, PFPDT, octobre 2014, p. 12).

Communication au sein de l'entreprise ou au sein d'un groupe de sociétés

Seuls les supérieurs hiérarchiques dans la ligne verticale directe, la direction de l'entreprise ou l'employeur lui-même ont accès au dossier personnel de l'employé.

Le service du personnel doit également avoir un accès au dossier relativement large. Il est cependant conseillé de leur faire signer un accord de confidentialité lors de l'engagement.

Un cadre qui n'est pas hiérarchiquement responsable de l'employé ne peut ainsi pas avoir accès au dossier du fait de sa seule position hiérarchique.

Une exception est cependant possible lorsque l'employé postule à l'interne dans un autre service ou au sein d'une autre société du groupe.

Dans les autres cas, même au sein d'une même société ou d'un même groupe, les communications à un cadre non supérieur hiérarchique ou un autre organe d'une société d'un même groupe de sociétés ou toute autre personne non habilitée sont considérées comme des communications à des tiers.

Ainsi par exemple, une communication du service du personnel à un autre service est considérée comme une communication à un tiers qui doit respecter les principes énoncés ci-dessous.

Communication à des tiers

Toute communication de données à des tiers est interdite si l'employé n'y a pas donné son consentement (art. 13 LPD).

Le consentement est ainsi nécessaire pour fournir des renseignements à des tiers sur la situation financière de l'employé (par exemple si l'employé veut contracter un crédit, obtenir une carte de crédit ou conclure un bail).

Le consentement est également nécessaire pour une communication au sein de l'entreprise ou d'un groupe de sociétés s'il ne s'agit pas d'un supérieur hiérarchique ou une personne habilitée par sa fonction.

Le consentement est également nécessaire par exemple dans le contexte d'un plan social si une société d'outplacement est mandatée.

Il existe bien évidemment une exception à ce principe si la loi oblige l'employeur à communiquer des données. C'est notamment le cas des données destinées à l'AVS.

Il existe également une exception en cas de transfert d'entreprises au sens de l'article 333 CO.

Communication à l'étranger

En cas de communication à l'étranger, l'article 6 LPD pose des exigences strictes.

Aucune donnée ne peut être communiquée à l'étranger si la personnalité de l'employé s'en trouve menacée notamment parce que le pays ne présente pas de législation assurant un niveau de protection de données adéquate.

Si une telle législation n'existe pas, la communication n'est possible que si l'une des conditions de l'article 6 al. 2 LDP est remplie (soit consentement ou contrat portant sur la protection des données, ou encore règles de protection des données édictées par un groupe de société).

Ces règles s'appliquent donc également en cas de communication à l'étranger au sein d'un groupe de sociétés (art. 6 al. 2 let. g LPD).

Ces règles s'appliquent bien évidemment également en cas d'externalisation de certains services, soit par exemple l'externalisation de la gestion des salaires à l'étranger ou l'outsourcing.

S'agissant du consentement de l'employé, en principe, le consentement doit être donné pour un cas d'espèce.

Il est cependant admis qu'un seul et même consentement peut servir de base, par exemple, aux communications à une société-mère à l'étranger par exemple des rapports annuels d'évaluation des performances des travailleurs.

Un seul consentement est également admis pour la communication à un tiers externe à l'étranger des données nécessaires au traitement des salaires *(Philippe Carruzzo, Le contrat de travail individuel, Commentaire des articles 319 à 341 du Code des obligations,*

2009, ad. 328b CO, p. 335-337).

A noter que le préposé doit être informé des garanties données visées à l'al. 2, let. a, et des règles de protection des données visées à l'al. 2, let. g (au sein d'un groupe).

Si l'employeur a procédé à cette communication au préposé, le devoir d'information est considéré comme respecté pour toutes les communications suivantes qui se basent sur les mêmes garanties, concernent les mêmes catégories de destinataires, ont la même finalité, et concernent les mêmes catégories de données *(Philippe Carruzzo, Le contrat de travail individuel, Commentaire des articles 319 à 341 du Code des obligations, 2009, ad. 328b CO, p. 336-337).*

Droit à l'image de l'employé (droit à l'image pour l'interne pour les employés (trombinoscope, communication interne, journal d'entreprise, intranet, etc.) et droit à l'image externe (réseaux sociaux notamment)

Les grands principes en matière de droit à l'image sont les suivants :

1. Le consentement de l'employé ne vaut que dans le contexte dans lequel il a été donné ;
2. L'image et/ou les informations doivent être utilisées à des fins commerciales.
   La question des réseaux sociaux pose la question de l'utilisation à des fins commerciales. Si cette utilisation fait défaut, l'image de l'employé ne peut pas être utilisée.
   De plus, l'employé ne peut pas donner de directives à ses employés s'agissant de l'utilisation, à titre privé, des réseaux sociaux.
   De tels directives peuvent éventuellement se justifier si l'entreprise est une entreprise dite « à tendance », soit les entreprises qui n'ont pas un but essentiellement lucratif et qui exercent une activité à caractère spirituel ou intellectuel, soit politique, confessionnel, syndical, scientifique, artistique, caritatif ou similaire. En effet, pour ces sociétés, les employés sont soumis à un devoir de fidélité plus exigeant.
3. Les informations sur l'employé ne devraient contenir que les données indispensables pour contacter la personne recherchée ;
4. Des exceptions sont admises, suivant le type d'activité. La publication de photos ainsi que d'informations sur la carrière de certains collaborateurs peuvent en effet se justifier notamment pour des raisons d'image de marque de l'entreprise, de valorisation du profil des employés ou pour faciliter la prise de contact par le client.
5. En principe, lorsque l'employé quitte l'entreprise, les images et les données doivent être supprimées.
   Des exceptions sont cependant admises en matière de prospectus ou de film publicitaire, si l'employé a consenti à ce que sa photo figure, « sans mention de son nom ou de sa fonction, qu'il n'est pas photographié en gros plan, mais de profil et qu'il est entouré d'autres collaborateurs ».
   Dans ce cas, il ne peut interdire la diffusion du prospectus s'il quitte l'entreprise avant que le stock ne soit écoulé. Dans ces cas, il faudra mettre en balance l'intérêt de l'employé ainsi que les intérêts de l'employeur et les coûts engendrés par le film publicitaire ou la publication du prospectus.
   En revanche, la mise à jour du site internet n'étant pas complexe, l'employé peut exiger que son nom ou son image ne figurent plus sur le site après son départ.

Droit d'accès de l'employé

L'employé a un droit d'accès à son dossier et aux données en tout temps (art. 8 LPD) et ce même après la fin des rapports de travail.

Il existe cependant des limites au droit d'accès.

Le droit d'accès ne porte pas sur les notes personnelles prises par le supérieur hiérarchique (art. 2 al. 2 let a LPD).

Les échanges d'e-mails entre supérieurs hiérarchiques concernant un employé préalablement à son licenciement constituent des actes internes de formation de volonté et ne sont pas à inclure dans le dossier personnel (8C.467/2013 du 21 novembre 2013 c. 3.2).

Le droit d'accès doit être exercé de bonne foi.

L'article 9 LPD prévoit également des restrictions.

L'employeur peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où : a. une loi au sens formel le prévoit ; b. les intérêts prépondérants d'un tiers l'exigent.

Il peut y avoir un intérêt prépondérant d'un tiers en cas de dénonciation par un autre employé par exemple.

L’employeur peut également refuser ou restreindre la communication des renseignements demandés ou en différer l’octroi, dans la mesure où ses intérêts prépondérants l’exigent et à condition qu’il ne communique pas les données personnelles à un tiers.

Ces intérêts prépondérants peuvent par exemple être des craintes d’espionnage industriel, la mise en danger ou l’atteinte aux droits de la personnalité de l’employeur ou encore des intérêts financiers prépondérants.

En cas de litige entre l’employé et l’employeur, le tribunal fédéral interdit le « fishing expedition », cependant il considère comme licite le fait de demander une copie du profil client dans l’optique de faire valoir des prétentions futures (ATF 138 III 425 ; SJ 2013 I 81) *(Marie Major, Questions spécifiques – le droit d’accès de l’employé à son dossier personnel, in La protection des données dans les relations de travail, CERT 2017).*

La loi n’impose aucune forme pour la requête de l’employé. La requête peut être globale ou ciblée.
L’employeur doit donner suite à la requête ou transmettre sa décision de refus dans un délai de 30 jours dès réception de la requête (art. 1 al. 4 OLPD).

L’employé n’a pas le droit de consulter l’original de son dossier. La règle est donc en principe la communication par écrit de l’employeur de photocopies du dossier.

L’employeur doit fournir le dossier ou les données gratuitement, mais une participation aux frais équitable est possible si les renseignements désirés ont déjà été communiqués au requérant dans les douze mois précédant la demande, et que ce dernier ne peut justifier d’un intérêt légitime, telle la modification non annoncée des données le concernant, ou si la communication des renseignements demandés occasionne un volume de travail considérable (art. 2 OLPD).

En cas de refus de l’employeur, l’employé a les moyens prévus à l’article 15 LPD.

Action en rectification de l’employé

Si l’employé constate que son dossier comporte des données inexactes, il peut en exiger la rectification (art. 5 LPD).

L’employeur est également tenu de vérifier l’exactitude des données.

****

Comme pour le précédent article, le but de la présente contribution est d’attirer l’attention de l’employeur sur le fait qu’il doit être attentif à la protection des données et se doit de former le personnel qui traite des données des autres employés.

L’employeur doit être particulièrement vigilent lorsque l’entreprise fait partie d’un groupe de sociétés et que des données doivent être transmises au sein du groupe et éventuellement à l’étranger. Une transmission de données, qui peut sembler évidente pour la bonne organisation du groupe, peut être contraire aux principes posés par le droit suisse et le RGPD.

La dernière phase, soit la phase de fin des rapports de travail, sera traitée dans un prochain article.

Source : https://www.wg-avocats.ch/actualites/droit-du-travail/protection-donnees-employe/