PROTECTION DES DONNEES
Dossier des membres du personnel

FICHE INFO DU PPDT

INTRODUCTION

L'employeur (entreprise privée ou institution publique) traite un certain nombre d'informations sur ses collaboratrices et collaborateurs (CV, contrat de travail, décisions d'engagement, évaluations, absences, courriers d'avertissement par exemple). Ces informations sont souvent consignées dans le "dossier personnel" de la collaboratrice ou du collaborateur.

Quel est le cadre juridique qui s'impose aux employeurs au regard de la protection des données? Les règles sont-elles les mêmes, qu'il s'agisse d'un employeur privé ou public? Quelles questions, en tant qu'employeur, dois-je me poser dans le cadre du traitement des données de membres du personnel? Qui peut avoir accès à ces données? Quels sont les droits des employé(e)s? Voici quelques questions qui seront notamment abordées dans le cadre de cette fiche informative.

CADRE JURIDIQUE

Les principales bases légales: LIPAD, loi fédérale sur la protection des données (LPD) et article 328 b CO

A Genève, les institutions publiques cantonales, communales et intercommunales entrent dans le champ d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD; RSGE A 2 08).

La loi fédérale sur la protection des données (LPD; RS 235.1) constitue le cadre juridique pour les autorités fédérales et le secteur privé, y compris pour les associations subventionnées par une entité publique genevoise, les fondations de droit privé ou les autres entreprises de droit privé qui travaillent avec l'Etat. La LPD est placée sous l'autorité du Préposé fédéral à la protection des données et à la transparence (PFPDT).

Ces lois visent la protection de la vie privée, en interdisant pratiquement tout traitement de données non explicitement autorisé par la loi ou par la personne intéressée, le but étant de protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.

En matière de droit du travail, le code des obligations prévoit une disposition spécifique concernant les données du travailleur. Elle a été introduite dans la loi au moment de l'adoption de la LPD; il s'agit de l'article 328b CO qui dispose que "*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*".

Finalement, des lois spécifiques, sur le personnel de l'Etat par exemple, peuvent trouver application. A Genève, l'on peut se référer notamment à la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux (LPAC; RSGE B 5 05) et son règlement d'application (RPAC; RSGE B 5 05.01).

Ainsi, en résumé et de manière non exhaustive:

Secteur privé	**Secteur public à Genève**
LPD Art. 328b CO	LIPAD LPAC – RPAC Autres lois réglant le statut du personnel des institutions publiques

D'autres lois ou dispositions légales peuvent également trouver application pour des questions spécifiques; certaines seront mentionnées ci-dessous.

FICHE INFO DU PPDT

PROTECTION DES DONNEES

Dossier des membres du personnel

Les principes fondamentaux communs en matière de protection des données:

Tout employeur privé ou institution publique qui traite[1] des données doit veiller au respect des principes suivants:

- **Principe de légalité/licéité**: tout traitement de données doit reposer sur une base légale/être licite et les données ne doivent pas être obtenues par crainte ou usurpation.
- **Principe de bonne foi**: le traitement et la collecte de données doivent être effectués en toute bonne foi, loyalement et de façon transparente.
- **Principe de finalité**: le but du traitement et de la collecte de données doit être clairement et préalablement défini. Dans le cas de données sensibles, le consentement de la personne concernée doit être explicite.
- **Principe de proportionnalité**: la collecte de données doit se limiter aux informations nécessaires exigées par le cas d'espèce.
- **Principe de destruction des données**: les données qui ne sont plus nécessaires doivent être détruites.
- **Principe de reconnaissabilité**: la collecte des données et les finalités du traitement de celles-ci doivent être reconnaissables pour la personne concernée.
- **Principe d'exactitude**: les données collectées doivent être exactes et mises à jour quand c'est nécessaire.
- **Principe de la sécurité**: toutes les mesures nécessaires, tant techniques qu'opérationnelles, doivent être mises en place pour protéger les données personnelles (sensibles ou non) et éviter tout traitement non autorisé de celles-ci.

Ces principes étant généraux, ils s'appliquent donc aussi au traitement des données des employé(e)s par l'employeur dans le cadre de leur dossier RH.

NOTION DE DONNEES PERSONNELLES

Qu'entend-on par données personnelles?

Il s'agit de toute donnée qui se rapporte à une personne identifiée ou identifiable, comme le lieu et la date de naissance, le numéro de téléphone, le nom et le prénom, l'adresse (physique ou électronique), l'adresse IP, le numéro AVS ou le numéro d'une carte de crédit. Les photos d'une personne sont aussi considérées comme des données personnelles.

Qu'entend-on par données personnelles sensibles?

Il s'agit d'opinions ou activités religieuses, philosophiques ou politiques, de l'ethnicité, de tout ce qui a trait à la sphère intime, de tout ce qui touche à la santé, des données génétiques ou biométriques, des mesures d'aide sociale, des poursuites pénales ou administratives. Les profils de personnalité sont assimilés à des données sensibles.

LES QUESTIONS A SE POSER

Sur la base des principes fondamentaux en matière de protection des données, il appartient à l'employeur de se poser les questions suivantes, lors du traitement de données des membres du personnel:

- Quelles sont les données que je collecte concernant mes collaboratrices et collaborateurs? Suis-je légitimé à faire cette collecte? Y a-t-il des données sensibles parmi les données collectées?
- Dans quel but est-ce que je collecte ces données?
- Comment est-ce que je collecte ces données? Est-ce l'employé(e) qui me les a remises ou est-ce que je les ai obtenues par un autre biais?
- Toutes les données collectées, sans exception, sont-elles nécessaires pour atteindre le but de la collecte ou pourrais-je me passer de certaines données? Est-ce que je conserve certaines données simplement "au cas où"?
- Combien de temps est-ce que je conserve ces données et pourquoi les conserver durant une telle période?
- Les données collectées sont-elles exactes et à jour? Comment est-ce que je m'en assure?

[1] La LPD, à son art. 3 litt. e et la LIPAD, à son art. 4 litt. e, définissent le traitement de données comme "toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données".

- Comment est-ce que je protège les données des membres du personnel? Est-ce que je prends toutes les mesures organisationnelles et techniques nécessaires?

D'autres questions à se poser ont trait à l'accès et à la communication des données; qui peut avoir accès aux données de mes employé(e)s? A quel titre?

QUE PEUT CONTENIR LE "DOSSIER" DE L'EMPLOYE(E)?

Secteur privé	Secteur public à Genève
Art. 328b CO: *"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".* **Art. 14 al. 1 LPD**: *"Le maître du fichier a l'obligation d'informer la personne concernée de toute collecte de données sensibles ou de profils de la personnalité la concernant, que la collecte soit effectuée directement auprès d'elle ou auprès d'un tiers".*	**Art. 35 al. 1 LIPAD**: *"Les institutions publiques ne peuvent traiter des données personnelles que si, et dans la mesure où, l'accomplissement de leurs tâches légales le rend nécessaire".* **Art. 35 al. 2 LIPAD**: *"Des données personnelles sensibles ou des profils de la personnalité ne peuvent être traités que si une loi définit clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée".*

Quelles informations?

Il ressort des dispositions susmentionnées que le dossier du personnel ne doit contenir que des données indispensables à l'exécution du contrat de travail.

De manière générale, les dossiers du personnel contiennent les données suivantes: les coordonnées de l'employé(e), son dossier de candidature, les éventuels tests psychologiques et références, le contrat de travail, le cahier des charges, les arrêts de travail, le décompte relatif aux vacances, les données relatives au salaire et aux assurances, les évaluations, les cours de formation continue, les mesures disciplinaires, la correspondance entre employé(e) et employeur, des extraits de registre, etc.[2].

Certaines de ces données, comme les tests psychologiques, sont des données sensibles. Il importe donc pour les institutions publiques d'avoir une base légale formelle avant de les effectuer.

Les données relatives à la capacité de travail des membres du personnel sont également des données sensibles.

Pour quelle durée?

Les données doivent être effacées lorsqu'elles ne sont plus nécessaires.

Selon le Préposé fédéral à la protection des données et à la transparence, il convient de trier tous les deux ans les dossiers du personnel afin d'en retirer les documents inutiles. Il s'agit d'une déclinaison du principe de la proportionnalité.

Afin de déterminer quels sont les documents utiles ou inutiles, plusieurs éléments peuvent servir de "guide" et la durée de conservation va dépendre du type de données. Premièrement, certaines règles liées au droit des assurances sociales ou au droit fiscal par exemple peuvent imposer à l'employeur de conserver des données, parfois même après la fin des rapports de travail. Deuxièmement, l'employeur peut conserver toutes les données liées à des prétentions, financières notamment, découlant du rapport de travail et qui ne seraient pas prescrites (5 ou 10 ans selon les prétentions). Finalement, évidemment, toutes les données nécessaires à l'exécution du contrat de travail peuvent être conservées, le temps que dure le contrat de travail.

Ainsi, il conviendrait de passer en revue le dossier du personnel tous les deux ans afin de trier les données qui sont encore utiles ou non, en se demandant parmi les données collectées, lesquelles sont utiles aujourd'hui à l'exécution du contrat de travail, si un document doit être conservé en vertu d'une obligation légale ou si la collaboratrice ou le collaborateur pourrait faire valoir une prétention pour laquelle il serait nécessaire de conserver ces données. Si certaines données figurant au dossier ne ressortent pas d'un des cas de figure susmentionnés, elles doivent être détruites.

Exemple: X a travaillé durant 5 ans dans le service A, puis a postulé dans le service B où elle exerce depuis 15 ans. X demande à consulter son dossier et constate que les documents relatifs à son congé maternité datant d'il y a 17 ans figurent toujours au dossier. Ces éléments ne devraient plus figurer au dossier, car ils n'ont plus d'utilité à l'exécution du contrat.

[2] Voir le "Guide pour le traitement des données personnelles dans le secteur du travail" du PFPDT et, pour un exemple de structure commune de dossier du personnel, la fiche y relative dans le mémento des instructions de l'Office du personnel de l'Etat de Genève (MIOPE 01.07.10).

FICHE INFO DU PPDT

PROTECTION DES DONNEES

Dossier des membres du personnel

QUI PEUT AVOIR ACCES AU DOSSIER DE L'EMPLOYE(E)?

L'accès aux données contenues dans le dossier personnel soulève différentes questions: celle de l'accès de la personne concernée à ses propres données, celle de savoir qui au sein de l'entreprise peut avoir accès aux données et celle de la communication de ces données à d'autres services ou groupes de l'entreprise/autres institutions ou à des tiers de droit privé.

L'accès à ses propres données:

Secteur privé	Secteur public à Genève
Art. 8 LPD: *"[1] Toute personne peut demander au maître d'un fichier si des données la concernant sont traitées.* *[2] Le maître du fichier doit lui communiquer:* *a. toutes les données la concernant qui sont contenues dans le fichier, y compris les informations disponibles sur l'origine des données;* *b. le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données".* **Art. 9 al. 1 LPD**: *"Le maître du fichier 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".* **Art. 9 al. 4 LPD**: *"Un maître de fichier privé peut en outre 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".*	**Art. 44 LIPAD**: *"[1] Toute personne physique ou morale de droit privé justifiant de son identité peut demander par écrit aux responsables désignés en vertu de l'article 50, alinéa 1, si des données la concernant sont traitées par des organes placés sous leur responsabilité.* *[2] Sous réserve de l'article 46, le responsable doit lui communiquer:* *a) toutes les données la concernant contenues dans un fichier, y compris les informations disponibles sur l'origine des données;* *b) sur demande, les informations relatives au fichier considéré contenues dans le catalogue des fichiers".* **Art. 46 LIPAD**: *"[1] L'accès aux données personnelles ne peut être refusé que si un intérêt public ou privé prépondérant le justifie, en particulier lorsque:* *a) il rendrait inopérantes les restrictions au droit d'accès à des dossiers qu'apportent les lois régissant les procédures judiciaires et administratives;* *b) la protection de données personnelles sensibles de tiers l'exige impérativement;* *c) le droit fédéral ou une loi cantonale le prévoit expressément.* *[2] Un accès partiel ou différé doit être préféré à un refus d'accès dans la mesure où l'intérêt public ou privé opposé reste sauvegardé".* **Art. 17 RPAC**: *"[1] Tout membre du personnel peut prendre connaissance de l'ensemble des rapports administratifs le concernant, notamment lorsqu'il demande à être nommé fonctionnaire ou fait acte de candidature à un autre poste de l'administration.* *[2] Aucun document ne peut être utilisé contre un membre du personnel sans que celui-ci n'en ait eu connaissance et qu'un délai ne lui ait été fixé pour faire part de son point de vue.* *[3] Toutefois, même si une pièce est utilisée, sa consultation peut être refusée si l'intérêt public ou des intérêts privés prépondérants l'exigent".*

L'employé(e) peut donc avoir accès à *toutes* les données le concernant. Cela signifie que l'employeur ne peut pas avoir deux dossiers concernant les membres de son personnel, l'un auquel le collaborateur ou la collaboratrice aurait accès et l'autre soustrait à son droit d'accès ("dossier gris"). Cela serait clairement contraire à la loi.

Les éventuelles restrictions au droit d'accès sont listées exhaustivement dans la loi.

Pour le secteur privé, les restrictions doivent découler soit d'une loi, soit des intérêts prépondérants de tiers ou du maître de fichier. En pratique, elles sont peu nombreuses. Elles peuvent viser par exemple le bon déroulement d'une procédure en cours, la protection de l'informateur en cas de dénonciation d'un employé suite à des agissements répréhensibles (infractions pénales, mobbing), au moins le temps nécessaire pour établir si les soupçons sont fondés ou pas, ou encore des informations sur la planification de carrière du travailleur dans l'entreprise, dans l'intérêt prépondérant de l'entreprise[3].

S'agissant du secteur public, l'art. 17 RPAC prévoit que des restrictions sont possibles en cas d'intérêt public ou privé prépondérant (conformément à l'art. 46 al.1 LIPAD). Les cas de figure qui peuvent se présenter ont trait par exemple à l'existence d'une procédure en cours lors de laquelle toutes les informations ne sont pas encore accessibles à l'employé(e) faisant l'objet de la procédure, ou encore si une loi cantonale le prévoit expressément.

[3] Meier, p. 683; Guide PFPDT, p. 13.

Finalement, il sied de souligner qu'il n'y a pas de droit d'accès aux notes personnelles de l'employeur (art. 2 al. 2 litt. a LPD; art. 3 al. 3 litt. a LIPAD).

L'employeur doit en principe répondre à la demande écrite de l'employé(e) dans un délai de 30 jours, selon l'art. 1 al. 4 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD; RS 235.11). Selon l'art. 49 al. 2 LIPAD, la demande doit être traitée "*avec célérité*". Selon notre autorité, un délai de 30 jours répond à cette condition.

L'accès aux données du collaborateur par des employé(e)s de l'entreprise / de l'institution publique:

Le Préposé fédéral rappelle que les données contenues dans les dossiers du personnel doivent être "*traitées uniquement par le service du personnel et n'être accessibles qu'aux services fondés à les utiliser de par la fonction qu'ils exercent*"[4]. Cette exigence découle des principes de finalité et de proportionnalité. Elle s'applique donc tant au secteur privé qu'au secteur public.

Exemples:

- Si le service des paies est fondé à avoir accès aux coordonnées bancaires d'un collaborateur ou d'une collaboratrice, son supérieur hiérarchique direct n'a pas besoin d'avoir accès à cette information.
- S'il est fondé qu'un supérieur hiérarchique (ainsi que la "ligne hiérarchique") et le responsable des ressources humaines aient accès aux évaluations d'un collaborateur ou d'une collaboratrice, l'adjoint(e) du supérieur hiérarchique qui n'a pas de responsabilité managériale vis-à-vis du collaborateur ou de la collaboratrice n'a pas à avoir accès à ladite évaluation, ni l'assistant(e) du supérieur hiérarchique. Les collègues du collaborateur ou de la collaboratrice encore moins.
- Le solde de vacances d'un(e) employé(e) ou le nombre d'heures supplémentaires à son actif n'a pas à apparaître sur un horaire accessible à l'ensemble du service. Par contre, doivent y avoir accès tant le ou la responsable du service, pour la planification des horaires, que les ressources humaines, afin de décompter le solde restant de vacances ou la rémunération des heures supplémentaires.
- Si un(e) employé(e) est absent pour cause de maladie, il convient de mentionner uniquement son absence et le type d'absence de manière générique (maladie, accident, vacances); par contre, il ne faut pas que soit mentionné au dossier RH l'affection dont l'employé(e) serait atteint(e) (dépression, burn out, jambe cassée). Ces dernières informations relèvent uniquement du service de santé du personnel de l'Etat.
- Les ressources humaines du département A n'ont pas à avoir accès aux données des membres du personnel du département B.
- Au sein d'une même direction de ressources humaines, chaque responsable consulte uniquement les dossiers dont il ou elle s'occupe; toutefois, pour assurer son remplacement (vacances, maladie, par exemple) ou la cohérence des pratiques (s'assurer que tous les cas soient traités de manière similaire, quel que soit le ou la responsable RH), d'autres responsables RH peuvent avoir accès aux données.
- L'employeur ne peut tenir une liste des téléphones privés des employé(e)s et en permettre l'accès aux autres collaborateurs que si elle est nécessaire aux activités professionnelles. Tel est le cas lorsque des employés doivent être régulièrement contactés à leur domicile. Par contre, s'il suffit que la centrale téléphonique puisse atteindre les employés à leur domicile, l'employeur ne doit remettre la liste des coordonnées qu'à ce service[5].

Il est intéressant de souligner que le Tribunal fédéral a confirmé le bien-fondé du licenciement d'un employé qui avait récolté des données au sujet d'une collègue sans raison valable, utilisant ainsi son accès à une base de données de manière indue[6].

Il sied de préciser que dans le cas d'espèce, cette récolte de données contrevenait également à une convention de confidentialité signée par l'employé. C'est plutôt sous cet angle que le Tribunal Fédéral a examiné la question. Toutefois, sous l'angle de la protection des données, une telle collecte aurait été contraire au principe de la finalité[7].

Finalement, il sied de rappeler que plus les données sont sensibles (données relatives à la santé notamment), plus les principes de la protection des données s'appliquent avec rigueur.

[4] Guide PFPDT, p.12.
[5] Exemple proposé par le Guide pratique du droit du travail des éditions WEKA.
[6] TF 8C_62/2014 du 29 novembre 2014, c. 2.3.2.
[7] Flueckiger, p. 12.

FICHE INFO DU PPDT

PROTECTION DES DONNEES
Dossier des membres du personnel

La communication des données du membre du personnel à d'autres services ou groupes de l'entreprise/autres institutions ou à des tiers de droit privé (en Suisse)

Il est ici question de la communication des données personnelles, que cette communication intervienne au sein de l'entreprise/institution (différents services) ou auprès de tiers de droit privé.

La LIPAD prévoit expressément d'autres cas de figure (tels que la communication à une autre institution publique soumise à la LIPAD, à un établissement de droit public non soumis à la LIPAD ou encore à un établissement de droit public étranger) qui ne seront pas traités dans la présente fiche info.

Outre les principes généraux en matière de protection des données, il convient de citer les dispositions suivantes:

Secteur privé	Secteur public à Genève
Art. 12 LPD Atteintes à la personnalité *[1] Quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées.* *[2] Personne n'est en droit notamment de:* *a. traiter des données personnelles en violation des principes définis aux art. 4, 5, al. 1, et 7, al. 1;* *b. traiter des données contre la volonté expresse de la personne concernée sans motifs justificatifs;* *c. communiquer à des tiers des données sensibles ou des profils de la personnalité sans motifs justificatifs.* *[3] En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement.* **Art. 13 Motifs justificatifs** *[1] Une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.* *[2] Les intérêts prépondérants de la personne qui traite des données personnelles entrent notamment en considération si:* *a. le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant;* *b. le traitement s'inscrit dans un rapport de concurrence économique actuel ou futur avec une autre personne, à condition toutefois qu'aucune donnée personnelle traitée ne soit communiquée à des tiers;* *c. les données personnelles sont traitées dans le but d'évaluer le crédit d'une autre personne, à condition toutefois qu'elles ne soient ni sensibles ni constitutives de profils de la personnalité et qu'elles ne soient communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter un contrat avec la personne concernée;* *d. les données personnelles sont traitées de manière professionnelle exclusivement en vue d'une publication dans la partie rédactionnelle d'un média à caractère périodique;* *e. les données personnelles sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées;* *f. les données recueillies concernent une personnalité publique, dans la mesure où ces données se réfèrent à son activité publique.*	**Art. 39 LIPAD Communication** **A une autre institution publique soumise à la loi** *[1] Sans préjudice, le cas échéant, de son devoir de renseigner les instances hiérarchiques supérieures dont elle dépend, une institution publique ne peut communiquer des données personnelles en son sein ou à une autre institution publique que si, cumulativement:* *a) l'institution requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait aux exigences prévues aux articles 35 à 38;* *b) la communication des données considérées n'est pas contraire à une loi ou un règlement.* *[2] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 1 et, une fois la communication effectuée, d'en informer le responsable sous la surveillance duquel il est placé, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement.* **A une tierce personne de droit privé** *[9] La communication de données personnelles à une tierce personne de droit privé n'est possible, alternativement, que si:* *a) une loi ou un règlement le prévoit explicitement;* *b) un intérêt privé digne de protection du requérant le justifie sans qu'un intérêt prépondérant des personnes concernées ne s'y oppose.* *[10] Dans les cas visés à l'alinéa 9, lettre b, l'organe requis est tenu de consulter les personnes concernées avant toute communication, à moins que cela n'implique un travail disproportionné. A défaut d'avoir pu recueillir cette détermination, ou en cas d'opposition d'une personne consultée, l'organe requis sollicite le préavis du préposé cantonal. La communication peut être assortie de charges et conditions, notamment pour garantir un niveau de protection adéquat des données.*

PROTECTION DES DONNEES
Dossier des membres du personnel

Secteur privé:

Conformément aux principes généraux de protection des données ainsi qu'aux dispositions susmentionnées, l'employeur ne peut communiquer aucun renseignement à des tiers sans le consentement de la personne concernée.

En effet, dans cette hypothèse, il contreviendrait à un ou plusieurs principes généraux de protection des données, comme la bonne foi, la reconnaissabilité de la collecte ou encore la finalité de la collecte. Et l'on ne voit pas quel intérêt prépondérant l'employeur pourrait faire valoir afin de rendre l'atteinte à la personnalité licite. Le consentement de l'employé(e) est donc nécessaire.

Le Préposé fédéral souligne que cette règle vaut également lorsqu'un organe d'un même groupe d'entreprises veut obtenir des renseignements sur un(e) employé(e)[8]. Cela est considéré comme une communication de données à des tiers.

C'est uniquement si la loi lui en fait l'obligation que l'employeur peut communiquer des données personnelles de son employé(e) sans son consentement (ex: données destinées à l'AVS).

Le cas de la communication des données du travailleur qui postule pour une mutation interne dans un autre service ou au sein d'une autre société du groupe est délicat. Selon Caruzzo, il s'agit d'une exception et "*il paraît logique d'admettre que le supérieur hiérarchique en charge de ce service puisse accéder au dossier personnel, la demande de mutation équivalant à une offre de services, par laquelle le candidat consent à la communication des données le concernant*"[9]. Selon cet auteur, cela inclut les données sensibles (profils de personnalité par exemple) pour autant que ces éléments aient été recueillis, en amont, avec le consentement exprès du travailleur et qu'ils présentent un intérêt pour le poste à repourvoir. Il semble pourtant qu'il serait plus conforme à la protection des données de demander l'aval du collaborateur avant de communiquer l'ensemble du dossier.

Une autre situation intéressante est celle relative au transfert d'entreprises. Une fois le transfert réalisé, les données nécessaires à la continuité du rapport de travail doivent passer à l'acquéreur[10]. Par contre, lors des étapes liées à la négociation (et donc avant transfert des relations de travail), il convient d'examiner à chaque étape de la transaction et suivant les circonstances du projet en cause les données que l'employeur est en droit de communiquer[11]. Obtenir le consentement de l'employé(e) avant toute communication assure d'être en conformité avec les règles de protection des données.

Secteur public à Genève:

S'agissant du secteur public à Genève, une communication à des tiers ne peut pas non plus intervenir sans l'accord de la personne concernée. En effet, conformément à l'art. 39 al. 9 et 10 LIPAD, une communication à une tierce personne de droit privé n'est possible qu'en cas d'intérêt digne de protection du requérant et sans intérêt prépondérant de la personne concernée (du collaborateur/de la collaboratrice); et dans un tel cas de figure, le collaborateur doit être consulté et s'il/si elle s'oppose à la communication, le préavis du Préposé cantonal doit être sollicité. Or, l'on ne voit pas dans quelle situation un préavis favorable contre l'accord du collaborateur/de la collaboratrice pourrait intervenir.

Par contre, comme pour le secteur privé, si une loi ou un règlement prévoit explicitement la communication des données à un tiers, cette communication est alors possible (par exemple, en lien avec les assurances sociales).

Comme pour le secteur privé, plus délicate est la question de la communication de données d'un membre du personnel en cas de transfert ou lors de sa candidature à un autre poste, mais au sein de la même institution publique ou d'une autre institution publique soumise à la LIPAD. Dans ce cas de figure, les données relatives au membre du personnel ne peuvent être communiquées que si cette communication n'est pas contraire à une loi ou à un règlement et si les principes généraux en matière de protection des données (art. 35 à 38 LIPAD) sont respectés. Sur ce dernier point, l'art. 14 al. 2 RIPAD précise que la démonstration du respect des conditions susmentionnées *"peut s'effectuer de manière simplifiée en indiquant cumulativement:*

a) le contexte légal ou réglementaire dans lequel s'inscrit la mission de l'institution requérante, y compris l'existence d'éventuelles règles spéciales ou la mention de leur défaut;

b) le fait que le fichier destiné à recevoir les données personnelles figure ou non dans le catalogue institué par l'article 43 de la loi, avec son numéro de référence;

c) la finalité de la transmission souhaitée".

Ainsi, en cas de transfert d'un membre du personnel, conformément à l'art. 12 LPAC par exemple, son dossier peut être transmis à la direction RH du département dans lequel l'intéressé-e est transféré-e. En effet, ces données sont nécessaires à la bonne continuité des rapports de service. Avant d'opérer cette communication, il convient de s'assurer que seuls les documents encore nécessaires figurent au dossier, conformément au principe de la proportionnalité.

---

[8] Guide PFPDT, p.13.
[9] Caruzzo, p.333.
[10] Sauf s'agissant des travailleurs qui se sont opposés au transfert, puisqu'il n'y a pas continuité du rapport de travail.
[11] Sur cette question, voir Carron/Weniger.

La question de l'accès au dossier du collaborateur ou de la collaboratrice avant que le transfert ne soit décidé et effectif est plus délicate. Si la personne concernée donne son accord à la transmission de son dossier, lorsqu'elle fait acte de candidature, il n'y a pas de problème à opérer cette communication. Par contre, si la personne concernée s'y oppose, la question reste ouverte quant à savoir si l'institution pourrait tout de même communiquer le dossier en s'appuyant notamment sur l'art. 39 al. 1 et 2 LIPAD.

A QUOI FAUT-IL AUSSI ETRE ATTENTIF?

Les institutions publiques doivent déclarer leurs fichiers au catalogue des fichiers, conformément à l'art. 43 LIPAD[12]. Les données personnelles relatives aux membres du personnel sont contenues dans un fichier et doivent donc faire l'objet d'une déclaration.

S'agissant du secteur privé, cette déclaration n'est pas obligatoire, pour autant que les données personnelles des employés soient traitées en vertu d'une obligation légale[13] (art. 11a LPD).

L'employeur doit également être attentif à la sécurité des données. Il s'agit d'un thème en soi qui ne fait pas l'objet de la présente fiche info. De même, la question de la sous-traitance des données ou celle de leur communication à l'étranger font l'objet de règles spécifiques, qui ne sont pas traitées par la présente fiche info.

QUELS SONT LES DROITS DE L'EMPLOYE(E)?

Le droit d'accès de la personne concernée à ses données personnelles a été traité ci-dessus. Outre ce droit d'accès, qui est le prérequis nécessaire à l'exercice des autres droits de la personne concernée, les prétentions qu'un(e) employé(e) peut faire valoir quant à ses données personnelles figurent à l'art. 15 LPD pour le secteur privé et à l'art. 47 LIPAD pour les institutions publiques genevoises.

Dans un premier temps, l'employé(e) s'adressera à l'employeur; dans un deuxième temps, il ou elle pourrait faire valoir ses droits en justice. La procédure pour faire valoir ses droits en justice ne fait pas l'objet de la présente fiche info. Seules les principales prétentions sont brièvement présentées, ainsi que la procédure à suivre pour faire valoir ses droits en matière de protection des données traitées par des institutions publiques genevoises.

Secteur privé	Secteur public à Genève
Art 15 LPD Prétentions *[1] Les actions concernant la protection de la personnalité sont régies par les art. 28, 28a et 28l du code civil. Le demandeur peut requérir en particulier que le traitement des données, notamment la communication à des tiers, soit interdit ou que les données soient rectifiées ou détruites.* *[2] Si ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peut être établie, le demandeur peut requérir que l'on ajoute à la donnée la mention de son caractère litigieux.* *[3] Le demandeur peut demander que la rectification ou la destruction des données, l'interdiction de la communication, à des tiers notamment, la mention du caractère litigieux ou la décision soient communiquées à des tiers ou publiées.* **Art 28 CC** *[1] Celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe.* *[2] Une atteinte est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.*	**Art. 47 LIPAD Prétentions** *[1] Toute personne physique ou morale de droit privé peut, à propos des données la concernant, exiger des institutions publiques qu'elles:* *a) s'abstiennent de procéder à un traitement illicite;* *b) mettent fin à un traitement illicite et en suppriment les effets;* *c) constatent le caractère illicite du traitement;* *d) s'abstiennent de les communiquer à des personnes de droit privé à des fins d'exploitation commerciale.* *[2] Sauf disposition légale contraire, elle est en particulier en droit d'obtenir des institutions publiques, à propos des données la concernant, qu'elles:* *a) détruisent celles qui ne sont pas pertinentes ou nécessaires;* *b) rectifient, complètent ou mettent à jour celles qui sont respectivement inexactes, incomplètes ou dépassées;* *c) fassent figurer, en regard de celles dont ni l'exactitude ni l'inexactitude ne peuvent être prouvées, une mention appropriée, à transmettre également lors de leur communication éventuelle;*

[12] Le catalogue des fichiers des institutions soumises à la LIPAD est disponible sur le lien suivant: http://outil.ge.ch/chacatfich/#/catalog/institution.
[13] Guide PFPDT, p.12.

PROTECTION DES DONNEES
Dossier des membres du personnel

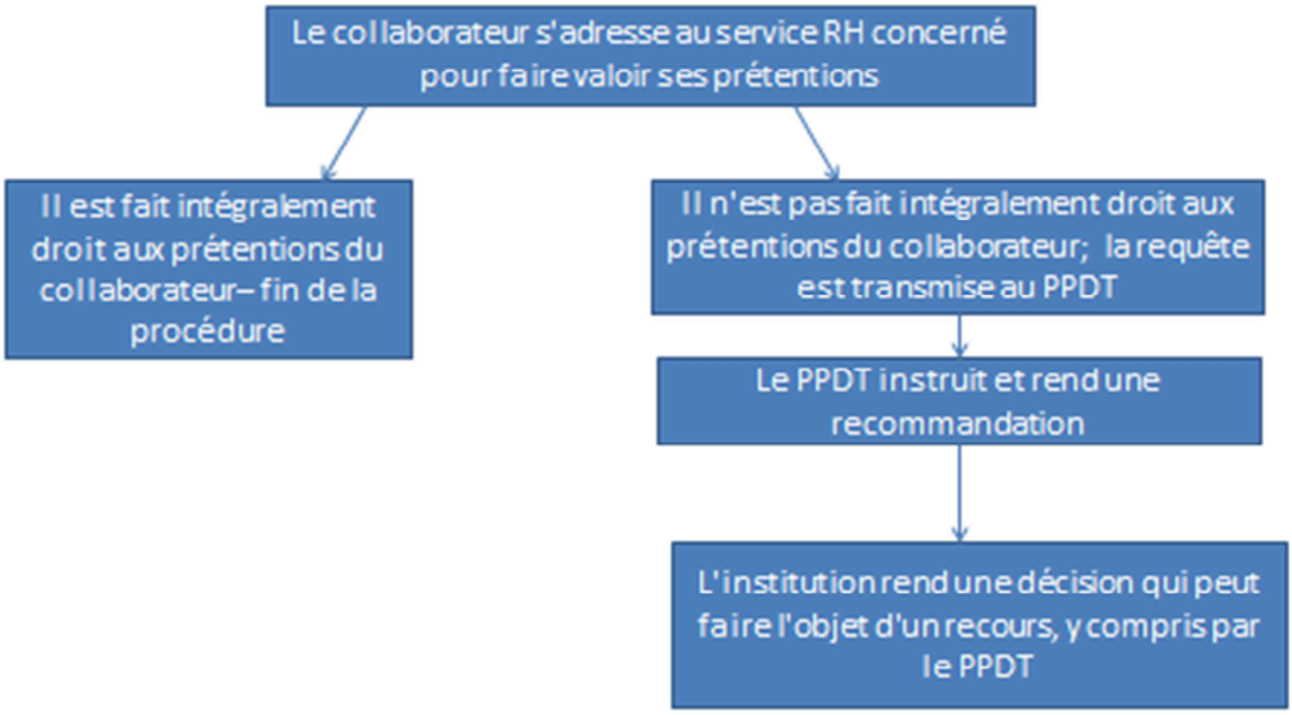
FICHE INFO DU PPDT

Art 28a al. 1 CC *[1] Le demandeur peut requérir le juge:* *1. d'interdire une atteinte illicite, si elle est imminente;* *2. de la faire cesser, si elle dure encore;* *3. d'en constater le caractère illicite, si le trouble qu'elle a créé subsiste.*	*d) s'abstiennent de communiquer celles qui ne répondent pas aux exigences de qualité visées à l'article 36;* *e) publient leur décision prise suite à sa requête ou la communiquent aux institutions publiques ou tiers ayant reçu de leur part des données ne répondant pas aux exigences de qualité visées à l'article 36.* *[3] Les prétentions en dommages-intérêts et en indemnité pour tort moral fondées sur la loi sur la responsabilité de l'Etat et des communes, du 24 février 1989, sont réservées.*

Les prétentions susmentionnées s'appliquent de manière générale à tout traitement de données que la personne concernée considèrerait comme illicite.

Les moyens de droit peuvent être dits défensifs (action en interdiction/en cessation de l'atteinte/action en constatation du caractère illicite de l'atteinte, par exemple) ou réparateurs (demande de dommages et intérêts ou tort moral par exemple).

S'agissant des données traitées par les institutions publiques genevoises, la procédure est la suivante:



QUELQUES REFERENCES POUR ALLER PLUS LOIN:

- Carron Vincent/Weniger Catherine, Protection des données des employés dans le cadre de transferts d'entreprises et de fusions, *in* Dunand Jean-Philippe/Mahon Pascal (éd.), La protection des données dans les relations de travail, Collection CERT, Genève/Zurich 2017.
- Caruzzo Philippe, Le contrat individuel de travail, Commentaire des articles 319 à 341 du Code des obligations, Zurich 2009.
- Dunand Jean-Philippe/Mahon Pascal (éd.), Commentaire du contrat de travail, Berne 2013.
- Dunand Jean-Philippe/Mahon Pascal (éd.), *La protection des données dans les relations de travail*, Collection CERT, Genève/Zurich 2017.
- Flueckiger Christian, Principes généraux de la protection des données et communications transfrontières dans le cadre des relations de travail, *in* Dunand Jean-Philippe/Mahon Pascal (éd.), La protection des données dans les relations de travail, Collection CERT, Genève/Zurich 2017.
- Meier Philippe, Protection des données, fondements, principes généraux et droit privé, Berne 2011.
- Préposé fédéral à la protection des données et transparence, Guide pour le traitement des données personnelles dans le secteur du travail, octobre 2014.
- Wyler Rémy, Droit du travail, Berne 2008.

- Le site internet http://www.thinkdata.ch contient divers scénarios, dont certains concernent le dossier du collaborateur.
- Pour une approche comparative avec la France, sur le site internet de la CNIL: https://www.cnil.fr/fr/declaration/ns-046-gestsion-du-personnel

PPDT : 12.09.2019