Mémento

Nouvelle loi sur la protection des données à partir du 1er septembre 2023: l'essentiel pour les entreprises commerciales

1. Situation de départ et aperçu

Avec la nouvelle loi sur la protection des données (LPD), qui a été adoptée le 25 septembre 2020 par le Conseil national et le Conseil des États après d'intenses délibérations et qui entrera en vigueur le 1er septembre 2023 après un délai de mise en œuvre prolongé, la pression et les efforts pour se conformer à la protection des données augmentent considérablement, y compris pour les entreprises commerciales. La sensibilisation croissante au thème de la protection des données y contribue notamment. Avec le développement du numérique, la protection de la personnalité et l'autodétermination en matière d'information ne cessent de gagner en importance dans de larges cercles de la population.

Le Conseil fédéral concrétise la LPD dans l'ordonnance sur la protection des données (ordonnance sur la protection des données, OPD) et dans l'ordonnance sur les certifications en matière de protection des données (OCPD), toutes deux du 31 août 2022.

Les grandes entreprises et les entreprises liées à l'UE devraient avoir développé la protection des données en conséquence dès l'entrée en vigueur du règlement général européen sur la protection des données (RGPD). En effet, le RGPD s'applique également à de nombreuses entreprises suisses (voir à ce sujet le mémento du 16 mars 2018). La nouvelle LPD n'est certes pas une mise en œuvre complète du RGPD. Toutefois, elle reprendre de nombreuses règles sur le principe afin d'atteindre un niveau de protection des données comparable, ce qui facilite les échanges de données transfrontaliers. En outre, la révision de la LPD permet également de ratifier l'extension de la Convention européenne 108 sur la protection des données.

Sur le plan territorial, le principe de l'impact s'applique comme pour le RGPD. La LPD s'applique donc également à tous les faits qui se produisent à l'étranger, mais qui ont un impact sur la protection des données en Suisse.

En principe, le principe de l'application des normes en fonction des risques s'applique comme auparavant. Plus les données ou une opération de traitement sont sensibles en termes d'atteinte à la personnalité des personnes concernées, plus les précautions à prendre pour éviter toute atteinte sont importantes. La protection des données doit ainsi être intégrée dès la phase de planification des projets numériques. Inversement, les entreprises (selon la désignation de la LPD «les responsables») ou les organes de direction responsables doivent également se demander, dans le cadre de la gestion des risques, dans quelle mesure ils sont prêts à prendre *sciemment* des risques résiduels. Il est indéniable que la protection des données – associée à la sécurité de l'information – devient de plus en plus un thème stratégique qui doit figurer à l'ordre du jour de la direction et du conseil d'administration.

Seules les données qui se rapportent à une personne physique identifiée ou identifiable, appelées données personnelles, relèvent de la protection légale des données. Mais désormais, comme dans le RGPD, la protection des données se limitera aux données des personnes *physiques*. La protection qui existait jusqu'à présent pour les personnes *morales* est supprimée. Les affaires B2B sont ainsi facilitées. Les personnes morales restent toutefois protégées par l'article 28 du Code civil (protection de la personnalité) ou par l'article 162 du Code pénal (violation du secret de fabrication ou du secret commercial) ainsi que par les dispositions pertinentes de la loi sur les cartels (LCart) et de la loi sur la concurrence déloyale (LCD). Les données personnelles des entreprises individuelles continueraient d'être protégées par la LPD. Les données commerciales non personnelles devraient également être protégées de manière adéquate par les entreprises. La protection des données et la sécurité de l'information vont donc de pair et devraient être abordées ensemble, ne serait-ce que pour des raisons d'efficacité.

Jusqu'à présent, les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime et l'appartenance raciale, ainsi que les mesures d'aide sociale et les poursuites et sanctions administratives et pénales, faisaient partie des données personnelles *sensibles* dont le traitement était soumis à des exigences légales plus strictes (p. ex. le consentement doit être *explicite*). Les données génétiques et biométriques viennent s'y ajouter. En outre, des conséquences juridiques ou des conditions particulières sont désormais liées non plus à l'infraction «profil de la personnalité», mais au «profilage» ou à celle «à haut risque», qui s'adresse au processus de traitement automatisé (évaluation de profils de la personnalité). Toutefois, compte tenu de l'intensité du débat parlementaire qui a été consacré à cette évolution, les changements pratiques à cet égard sont marginaux.

Dans la pratique, il est recommandé aux entreprises – même si cela n'est pas toujours obligatoire du point de vue de la protection des données – d'édicter des directives internes de protection des données (un simple ensemble de règles peut suffire), de régler clairement les responsabilités et de former et sensibiliser les collaborateurs. Outre la protection contractuelle (p. ex. vis-à-vis des sous-traitants), il est également important de documenter de manière adéquate la protection des données et la sécurité de l'information, notamment pour pouvoir prouver, en cas d'incident, que la conformité a été respectée. Il va de soi que les processus nécessaires au sein de l'entreprise et vis-à-vis de tiers (autorités de surveillance, personnes concernées, etc.) doivent également être définis afin de pouvoir réagir efficacement en cas de besoin.

Ci-après, nous décrivons plus en détail, au chiffre 2, les règles essentielles pour les entreprises commerciales lors du traitement de données personnelles et, au chiffre 3, les droits des personnes concernées qu'il convient de respecter. Le chiffre 4 présente les conséquences possibles pour la gestion des risques en cas de violation de la protection des données. Les références à l'article (art.) et à l'alinéa (al.) se rapportent ici à la nouvelle LPD.

2. Quelles règles les entreprises concernées doivent-elles respecter lors du traitement de données personnelles?

Les entreprises commerciales doivent notamment respecter les règles suivantes lors du traitement de données personnelles. Il convient de noter que la loi se fonde sur une notion large de traitement des données, qui englobe pratiquement toute manipulation de données personnelles, de la saisie à la suppression:

- **Principe de légalité:** Les données personnelles doivent être traitées de manière licite (art. 6, al. 1 LPD), c'est-à-dire que le traitement est en principe autorisé tant qu'il n'est pas effectué en violation d'une norme juridique.

- **Principe de transparence:** Celui-ci découle du principe selon lequel le traitement des données doit être effectué de manière loyale et licite (art. 6, al. 2 LPD). La collecte et le traitement des données doivent en principe être effectués de manière à ce que la personne concernée en ait connaissance. Dans le cas contraire, la personne concernée ne peut pas faire valoir ses droits.

- **Principe de proportionnalité:** Conformément à ce principe, seules les données *nécessaires* et *appropriées* au but poursuivi peuvent être collectées (art. 6, al. 2 LPD). Le principe de proportionnalité implique également que les données ne peuvent être conservées que le *temps* nécessaire à la réalisation de l'objectif.

- **Principe de la finalité du traitement:** Selon ce principe, les données ne peuvent être collectées que dans un but précis et identifiable par la personne concernée et ne peuvent être traitées que de manière compatible avec ce but (art. 6 al. 3 LPD). Les données doivent être détruites ou rendues anonymes dès qu'elles ne sont plus nécessaires au but du traitement (art. 6, al. 4).

- **Principe d'exactitude:** Quiconque traite des données personnelles doit s'assurer de leur *exactitude* (art. 6, al. 4 LPD). Il doit prendre toutes les mesures raisonnables pour que soient rectifiées ou détruites les données qui sont inexactes ou incomplètes au regard du but pour lequel elles sont collectées ou traitées.

- **Principe de sécurité des données:** Le principe exige la protection des données par des *mesures techniques* et *organisationnelles (*Art. 8 LPD). Celles-ci garantissent les différents objectifs de protection que sont *la confidentialité*, la *disponibilité* et *l'intégrité* des données ainsi que la *traçabilité* du traitement des données. Ici aussi, le principe de proportionnalité s'applique et les mesures doivent correspondre à l'état de la technique. Plus les données sont sensibles, plus les exigences en matière de sécurité des données sont élevées. L'être humain étant régulièrement le maillon faible de la sécurité des données, les mesures techniques mais aussi et surtout organisationnelles sont d'une grande importance. Les mesures concrètes peuvent être les suivantes: les restrictions d'accès, le cryptage des données, la journalisation, les sauvegardes, les techniques d'élimination sûres, les contrôles d'accès, les règlements et les directives, la formation et la sensibilisation, les contrats de traitement des données et de confidentialité ainsi que les contrôles périodiques et les améliorations. Le principe de la sécurité des données est davantage concrétisé par le Conseil fédéral dans l'OPD (art. 1 à 6).

- **Protection des données dès la conception** (dite Privacy by Design, art. 7 al. 1 et 2 LPD): Les systèmes utilisés pour le traitement des données personnelles doivent être conçus dès le départ de manière à ce que la protection des données puisse être respectée. Les mesures techniques et organisationnelles doivent notamment être adaptées à l'état de la technique, à la nature et à l'ampleur du traitement des données ainsi qu'au risque que le traitement comporte pour la personnalité ou les droits fondamentaux des personnes concernées.

- **Protection des données par défaut (dites Privacy by Default, art. 7 al. 3 LPD):** Les responsables doivent choisir les paramètres par défaut de l'appareil ou du logiciel de manière à ce que le traitement des données personnelles soit limité au minimum nécessaire pour l'utilisation prévue, à moins que la personne concernée n'en décide autrement. Dans la pratique, cette règle s'applique en particulier à l'acceptation de ce que l'on appelle les cookies sur Internet. Si l'on accepte les paramètres par défaut, seuls les cookies strictement nécessaires au service peuvent être activés. La personne concernée peut toutefois accepter d'autres cookies dans les paramètres du site Internet.

- **Consentement et opposition:** Le consentement de la personne concernée au traitement des données par une entreprise n'est en principe pas nécessaire, même pour les données personnelles sensibles. En revanche, il y a atteinte à la personnalité au sens de l'article 30 LPD lorsque la personne concernée s'oppose expressément à un traitement de ses données. Dans ce cas, l'atteinte à la personnalité ne peut être justifiée que par une base légale ou par les intérêts prépondérants du responsable au sens de l'art. 31 LPD (voir également la règle sur l'atteinte à la personnalité ci-dessous).

- **Obligation d'information:** L'obligation d'information étendue selon les art. 19 ss. LPD est un aspect important dans le cadre du principe de transparence. La personne concernée doit savoir quelles données liées à sa personne sont collectées et traitées et dans quel but. En principe, cela doit se faire *avant* l'obtention des données. Si les données ne sont pas collectées directement auprès de la personne concernée, l'information a lieu dans un délai d'un mois à compter de leur réception. Conformément à l'art. 13 de l'OPD, l'information doit être fournie sous une forme précise, transparente, compréhensible et facilement accessible. Sauf exception justifiée par la loi, une obligation d'information s'applique à chaque collecte planifiée de données personnelles. Sont exclues de l'obligation d'information les données personnelles qui sont saisies de manière accessoire ou par hasard. Cela vaut également la collecte involontaire ou accidentelle de données.

Les clients existants ne doivent pas être informés lors de l'entrée en vigueur de la nouvelle LPD. En outre, une personne concernée ne doit pas être informée de ce qu'elle sait déjà. Les personnes sont considérées comme informées en amont lorsqu'elles mettent leurs données personnelles à la disposition du responsable du traitement sans l'intervention de ce dernier. De même, il n'est pas nécessaire d'informer des modifications ultérieures. Ce n'est que si le but de l'utilisation des données change qu'il faut informer. Le contenu doit indiquer l'identité et les coordonnées du responsable, le but du traitement et, le cas échéant, les destinataires auxquels les données sont communiquées. Si les données sont communiquées à l'étranger, les pays concernés doivent être indiqués. Divers autres motifs légaux de limitation et d'exception limitent ou suppriment l'obligation d'information, p. ex. lorsque le traitement des données est prévu par la loi ou lorsqu'il est en contradiction avec les intérêts prépondérants de tiers. Si le responsable ne peut identifier la personne concernée qu'au prix d'efforts disproportionnés, elle ne doit pas être informée en cas de collecte indirecte de données. Dans un cas concret, il vaut la peine de consulter les dispositions d'exception de l'art. 20 LPD. Si les traitements conduisent à des décisions individuelles automatisées, les responsables doivent assumer d'autres obligations d'information vis-à-vis de la personne concernée et lui accorder les droits de consultation et de vérification qui lui reviennent (art. 21 LPD). Les entreprises se conforment généralement à l'obligation d'information en publiant une déclaration de protection des données sur leur site Internet ou dans leurs conditions générales. Il n'y a toutefois aucune exigence de forme. Toute ambiguïté sera interprétée en faveur de la personne concernée ou du client et à la charge du responsable ou de l'auteur. Le RGPD (art. 12 et suivants) contient des obligations d'information qui vont au-delà de celles de la LPD et qui sont réglées de manière plus détaillée.

- **Traitement par le sous-traitant:** La sous-traitnce signifie qu'un responsable confie l'exécution du traitement de ses propres données à un tiers (sous-traitant) pour son compte. Le responsable doit notamment garantir contractuellement la finalité et la sécurité des données vis-à-vis du sous-traitant (art. 9 LPD). Le sous-traitant ne peut confier le traitement à un tiers qu'avec l'autorisation préalable du responsable. Celui-ci peut être de nature générale ou spécifique (voir également l'art. 7 OPD). Aucun contrat n'est nécessaire lorsqu'une loi prévoit la sous-traitance. Dans ce cas également, il convient toutefois de garantir la finalité et la sécurité des données.

- **Communication de données à l'étranger:** Selon les rt. 16 ss LPD**,** les données personnelles ne peuvent être communiquées à un destinataire à l'étranger (même par le biais d'un accès à un serveur en Suisse) que si le niveau de protection des données dans le pays concerné est similaire à celui de la Suisse. Le Préposé fédéral à la protection des données et à la transparence (PFPDT) – le Conseil fédéral après l'entrée en vigueur de la nouvelle LPD – tient à cet effet une liste des États qui, du point de vue suisse, présentent un niveau de protection des données suffisant. Si un pays tiers ne dispose pas d'un niveau de protection des données équivalent à celui de la Suisse, la communication est néanmoins autorisée si le responsable règle par contrat avec le destinataire étranger des données le respect des normes suisses de protection des données. Les accords les plus fréquemment utilisés dans la pratique sont les clauses types de la Commission européenne qui existent pour les sous-traitants et les responsables en tant que destinataires. Le PFPDT approuve et publie également de telles clauses. Le Conseil fédéral concrétise davantage la communication de données à l'étranger dans l'OPD (art. 8 à 12).

- **Liste des activités de traitement:** Les responsables et les sous-traitants des grandes entreprises doivent tenir chacun un registre de tous les traitements de données (art. 12 LPD). Les entreprises de moins de 250 collaborateurs ne sont pas concernées, sauf si elles traitent des données personnelles sensibles à grande échelle ou si elles procèdent à un profilage (art. 24 OPD). Pour chaque activité de traitement, les données prévues par la loi doivent être enregistrées. En l'occurrence: l'identité du responsable ou du sous-traitant, le but du traitement, la description des catégories de personnes concernées et des catégories de données personnelles traitées, les catégories de destinataires, la durée de conservation ou les critères pour la déterminer, si possible la description des mesures prises pour assurer la sécurité des données ainsi que les éventuels pays de destination si

les données sont envoyées à l'étranger. Le registre doit toujours être à jour et donner une vue d'ensemble des activités liées à la protection des données dans l'entreprise. Comme cela est fondamental pour toute protection des données, il vaut donc la peine pour les petites entreprises de tenir un registre correspondant, même si elles ne sont pas soumises à l'obligation légale. Il n'y a pas de condition de forme, ce qui signifie que de simples documents Word ou Excel suffisent. Les registres qui ont éventuellement été établis en application du RGPD peuvent être repris. Désormais, les entreprises n'ont plus l'obligation d'enregistrer leurs fichiers, comme le prévoyait l'ancienne LPD, mais cette obligation n'était guère appliquée dans la pratique.

- **Analyse d'impact relative à la protection des données (AIPD):** Si un traitement de données prévu présente un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées, le responsable doit procéder au préalable à une AIPD (art. 22 LPD). Le risque élevé résulte des technologies et de la nature ou des circonstances des traitements de données (profilage à haut risque, traitement de données sensibles). L'accent n'est pas mis sur l'éventuelle atteinte à la personnalité, mais sur les conséquences du traitement des données pour les personnes concernées et sur la manière de les éviter, en fonction de la probabilité d'occurrence. Un traitement de données est notamment délicat lorsqu'il s'agit d'une surveillance systématique ou du traitement de données personnelles confidentielles, ou lorsqu'il s'agit de décisions automatisées qui peuvent influencer la conclusion d'un contrat par l'utilisation de la technique. Le responsable doit conserver l'AIPD pendant au moins deux ans après la fin du traitement des données (art. 14 OPD). Si un risque élevé subsiste après l'AIPD, un avis doit être demandé au PFPDT. Celui-ci peut faire des objections et proposer des mesures (art. 23 LPD). Le PFPDT peut également exiger une AIPD. S'il existe un certificat ou un code de conduite, ou si un conseiller à la protection des données est engagé (nous y reviendrons plus loin), il est possible de renoncer à l'AIPD. En ce qui concerne le principe de la protection des données dès la conception (Privacy by Design), il vaut la peine d'effectuer au moins une AIPD «rapide» pour chaque projet numérique.

- **Conseiller à la protection des données:** Les entreprises peuvent désigner volontairement un conseiller à la protection des données (art. 10 LPD). Celui-ci peut, mais ne doit pas nécessairement, être lié au responsable par un contrat de travail. Outre les conseils généraux et la formation, le conseiller à la protection des données examine les projets de traitement de données qui présentent encore un «risque élevé» malgré la réalisation de l'AIPD et la définition de mesures. Si l'examen est effectué par le conseiller à la protection des données, le PFPDT ne doit plus être consulté. Dans ce contexte, le conseiller à la protection des données doit disposer des connaissances techniques appropriées. En même temps, il ne devrait pas être lui-même impliqué dans le traitement des données personnelles en question, afin de pouvoir conserver l'indépendance nécessaire, qui est davantage concrétisée à l'art. 23 du RGPD. Pour les petites entreprises en particulier, on peut se demander si ces exigences strictes peuvent être justifiées par le (seul) «avantage» de ne pas devoir consulter le PFPDT. Les responsabilités en matière de protection des données et de sécurité de l'information peuvent ou doivent être réglées au sein de chaque entreprise, indépendamment de la mise en place d'un conseiller à la protection des données au sens de l'art. 10 LPD.

- **Code de conduite:** Les associations professionnelles, sectorielles et économiques peuvent élaborer leurs propres codes de conduite et les soumettre au PFPDT (art. 11 LPD). Il n'y a pas d'obligation de soumettre un code, mais si un code est soumis, le PFPDT doit prendre position. Les prises de position du PFPDT sont publiées. Des codes de conduite régissent les aspects de la protection des données pour les membres de l'association. S'il existe un tel code de conduite, l'obligation de procéder à une AIPD concernant ces aspects ne s'applique pas (art. 22, al. 5 LPD). La condition préalable est que le code de conduite soit basé sur une AIPD.

- **Certification:** Même si un responsable utilise un système ou un programme de traitement des données qui est certifié en conséquence (art. 13 LPD), l'obligation de procéder à une AIPD ne s'ap-

plique pas à celui-ci (art. 22, al. 5 LPD). La certification est l'expression d'une certaine «adéquation», mais ne signifie pas qu'il n'y aura pas de violation de la protection ou de la sécurité des données par la suite.

- **Atteinte à la personnalité et motifs de justification:** Quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées (art. 30 LPD). Il y a atteinte à la personnalité notamment (mais pas uniquement) lorsque (a) les principes du traitement des données selon les art. 6 et 8 LPD sont enfreints, (b) des données personnelles sont traitées contrairement à la déclaration de volonté expresse de la personne concernée ou (c) des données personnelles sensibles sont communiquées à des tiers.

  Une atteinte à la personnalité n'est pas illicite, mais licite ou «réparée» si l'un des motifs justificatifs suivants est présent (art. 31 al. 1 LPD): (a) le consentement de la personne concernée, (b) un intérêt privé ou public prépondérant, ou (c) une base légale.

  Dans la pratique, un motif de justification important pour les entreprises est, outre le consentement, l'intérêt privé prépondérant. Celui-ci est davantage concrétisé dans la loi. L'art. 31 al. 2 LPD contient une liste non exhaustive des intérêts prépondérants possibles du responsable dans les contextes suivants: (a) l'exécution d'une relation contractuelle, (b) entre des personnes en situation de concurrence économique, (c) la vérification de la solvabilité, (d) la publication dans les médias, (e) les personnes publiques et (f) la recherche, la planification et les statistiques.

  Ce faisant, les conditions d'une justification par contexte sont davantage concrétisées. Un cas de justification souvent invoqué est l'examen de la solvabilité. La loi sur la protection des données impose quatre restrictions à cet égard: premièrement, seules les données relatives aux personnes majeures peuvent être traitées. Deuxièmement, les données ne doivent pas dater de plus de dix ans. Après dix ans, une information selon laquelle une personne a fait faillite, par exemple, ne peut plus être traitée. Troisièmement, les vérifications de solvabilité ne doivent pas être basées sur un profilage à haut risque ou sur des données particulièrement sensibles. Quatrièmement, les données relatives à la solvabilité ne peuvent être communiquées à des tiers que si ceux-ci ont besoin de ces données pour conclure ou exécuter un contrat avec la personne concernée. Un système de feux de signalisation concernant la capacité de paiement peut continuer à être utilisé.

  Concernant les droits juridiques qui résultent pour une personne concernée d'une atteinte injustifiée à sa personnalité, voir le chiffre 3.

- **Obligation de notification en cas de violation de la sécurité des données:** Les violations de la *sécurité des données* (p. ex. divulgation à des personnes non autorisées, perte de données, cyberattaque, etc.) qui font courir aux personnes concernées un risque élevé pour leur personnalité ou leurs droits fondamentaux doivent être notifiées par le responsable au PFPDT «dans les meilleurs délais» (au sens de «en temps utile») (art. 24 LPD). Le fait de conserver des données trop longtemps (principe de proportionnalité ou de finalité) ne constitue pas une violation de la *sécurité des données*, bien qu'il s'agisse d'une violation de la*protection des données*. Une déclaration est par exemple nécessaire en cas de perte de données non cryptées relatives aux collaborateurs (dossier personnel avec qualifications et données salariales). Le risque que les personnes concernées puissent être affectées est élevé. Si des données cryptées des collaborateurs sont perdues, la situation doit être évaluée différemment. Les faits, les conséquences possibles et les mesures prises (p. ex. les personnes concernées sont informées) sont soumis à l'obligation de notification. Les personnes concernées doivent être informées si cela est nécessaire pour leur protection ou si le PFPDT le demande. L'obligation de notification est davantage concrétisée à l'art. 15 du RGPD. Il est notamment prescrit que la violation de la sécurité des données qui doit être notifiée doit être documentée. La documentation doit être conservée pendant deux ans.

3. Quels sont les (autres) droits des personnes concernées?

Les règles et obligations des responsables décrites au chiffre 2 entraînent naturellement des droits correspondants pour les personnes concernées. En outre, la LPD contient d'autres droits des personnes concernées, dont certains sont encore étendus par la révision. En l'occurrence:

- **Droit d'accès:** Le droit d'accès des personnes concernées en vertu de l'art. 25 LPD va plus loin que l'obligation d'information du responsable. La personne concernée peut en apprendre plus que ce que le responsable est tenu de révéler en vertu de son obligation d'information. Le but de l'information est de savoir si des données personnelles sont traitées et, si oui, lesquelles, afin que la personne concernée puisse faire valoir ses autres droits. En font partie, outre les données personnelles traitées en tant que telles, des informations sur l'identité du responsable, le but du traitement, la durée de conservation, l'origine des données et, le cas échéant, des informations sur les décisions individuelles automatisées et les destinataires (également en tant que catégories). L'objectif est donc de proposer une large transparence dans le traitement des données pour une personne concernée qui en fait la demande. En règle générale, les renseignements doivent être fournis gratuitement et dans un délai de 30 jours. La personne qui demande des renseignements doit s'identifier clairement. L'art. 26 LPD règle les restrictions du droit d'accès. Ainsi, les demandes quérulentes ne doivent pas être traitées. De même, une demande peut être rejetée en raison d'intérêts prépondérants de tiers. D'autres exceptions sont prévues, notamment pour les médias (art. 27 LPD). D'autres dispositions relatives au droit d'accès figurent dans le RGPD (art. 16 à 19).

- **La portabilité des données** comprend désormais le droit à la communication et à la transmission des données (art. 28 LPD). Les personnes concernées peuvent demander à récupérer les données qu'elles ont communiquées à un responsable dans un format électronique courant, lorsque les données sont traitées de manière automatisée et que la personne concernée a donné son consentement au traitement ou que le traitement est effectué dans le cadre d'un contrat correspondant. Dans ces conditions, il est également possible d'exiger le transfert des données à un tiers, si cela n'entraîne pas d'efforts disproportionnées. La portabilité des données peut être limitée pour des raisons similaires à celles du droit d'accès (art. 29 LPD). D'autres dispositions relatives à la portabilité des données figurent dans le RGPD (art. 20 à 22).

- **Droit de rectification:** Une personne concernée peut exiger, conformément à l'art. 32 al. 1 LPD**,** que des données personnelles inexactes soient rectifiées; cela devrait notamment entrer en ligne de compte après l'exercice du droit d'accès**.** Le responsable peut refuser la rectification si une disposition légale l'interdit (p. ex. règles de comptabilité et de conservation). Si l'exactitude ou l'inexactitude des données personnelles concernées ne peut être établie, la personne concernée peut demander qu'une mention de contestation soit apposée sur les données (art. 32 al. 3 LPD).

- **Droit à la suppression des données («droit à l'oubli»):** Comme nous l'avons mentionné, il y a atteinte à la personnalité au sens de l'art. 30 LPD, entre autres, lorsque des données personnelles sont traitées contrairement à la déclaration de volonté expresse de la personne concernée et qu'il n'existe pas de base légale ni d'intérêt privé prépondérant de tiers au sens d'une justification au sens de l'art. 31 LPD. Il en résulte pour la personne concernée un droit limité à la suppression des données.

- **Autres droits juridiques:** En cas d'atteinte injustifiée à la personnalité, les personnes concernées peuvent faire valoir d'autres prétentions de droit civil. Selon l'art. 32 al. 2 LPD, il s'agit (a) de l'interdiction d'un traitement de données déterminé, (b) de l'interdiction d'une communication déterminée de données personnelles à des tiers et (c) également de l'effacement ou de la destruction de données personnelles. En raison du renvoi de l'art. 32 al. 2 LPD au Code civil, les autres droits suivants existent le cas échéant: la constatation, l'omission ou la suppression de la violation du droit ainsi que les prétentions en dommages-intérêts, en réparation du tort moral ainsi que la restitution du gain.

4. Quelles sont les conséquences des violations de la protection des données?

- Comme dans le droit actuel, la violation des obligations en matière de protection des données peut, dans la nouvelle LPD, relever aussi bien du droit de surveillance (art. 49 ss. LPD), mais aussi du droit pénal (art. 60 ss. LPD) et du droit civil (art. 30 ss. LPD). Alors que dans l'ancien droit, la violation de pratiquement aucune obligation légale n'était punissable, la partie pénale de la LPD révisée est fortement développée et les peines possibles sont considérablement plus élevées. La partie relative à la surveillance est également développée, puisque le PFPDT se voit attribuer des compétences plus étendues. En revanche, la voie du droit civil reste pratiquement inchangée.

- Le PFPDT ouvre une enquête, d'office ou sur dénonciation, lorsqu'il existe suffisamment d'indices qu'un traitement de données pourrait enfreindre les dispositions sur la protection des données (art. 49 LPD). En cas de violations mineures, il peut renoncer à un examen (principe d'opportunité). Le PFPDT dispose désormais de pouvoirs d'investigation étendus à l'égard des entreprises, pouvant aller jusqu'à des perquisitions et à l'audition de témoins (art. 50 LPD). En cas de violation de la protection des données, le PFPDT peut décider d'adapter, d'interrompre ou d'annuler tout ou partie du traitement et d'effacer ou de détruire les données personnelles (art. 51 LPD). Les décisions du PFPDT peuvent faire l'objet d'un recours auprès du Tribunal administratif fédéral. Les arrêts du Tribunal administratif fédéral peuvent faire l'objet d'un recours devant le Tribunal fédéral. Les recours dans le cadre de la Convention européenne des droits de l'homme sont également réservés.

- Contrairement aux autorités européennes de protection des données, le PFPDT ne dispose pas non plus, selon le nouveau droit, de pouvoirs de sanction (directs) *en matière de surveillance*. Les personnes fautives sont sanctionnées par les autorités cantonales de poursuite pénale. Le PFPDT peut uniquement déposer une plainte pénale et exercer les droits de la partie civile dans la procédure (art. 65, al. 2 LPD).

- Dans la nouvelle LPD, les contrevenants s'exposent à un système de sanctions *pénales* avec des amendes pouvant aller jusqu'à CHF 250 000 (art. 60 ss. LPD). Seuls les actes et les omissions *intentionnels* sont passibles de sanction, et non la négligence. Ne sont sanctionnés que sur demande d'une personne concernée le non-respect des obligations d'information, de renseignement et de communication ainsi que la violation du secret professionnel et des obligations de diligence en rapport avec la sécurité des données, la communication de données à l'étranger et la sous-traitance. En revanche, le non-respect des décisions du PFPDT est poursuivi d'office (pouvoir de sanction indirect). Celui-ci peut également porter plainte, mais il n'a pas le droit de déposer une plainte pénale. Les autorités cantonales sont compétentes pour l'application de la peine, avec les voies de recours traditionnelles. En principe, les amendes sont infligées aux personnes *physiques* responsables. Cela devrait concerner en premier lieu les membres responsables des organes de décision tels que la direction et le conseil d'administration, notamment dans le cadre de leur devoir d'organisation stratégique, mais aussi les différents collaborateurs dans le cadre de leurs activités opérationnelles. Désormais, l'entreprise elle-même peut être condamnée à une amende pouvant aller jusqu'à CHF 50 000 si l'identification de la personne physique coupable au sein de l'entreprise ou de l'organisation entraîne des frais d'enquête disproportionnés.

  Contrairement à la LPD, les sanctions prévues par le RGPD visent exclusivement les personnes *morales*. Les autorités de protection des données de l'UE peuvent infliger aux entreprises fautives des amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.

- Pour faire valoir des prétentions civiles découlant d'atteintes à la personnalité conformément à l'art. 32 LPD, les personnes concernées doivent passer par la voie de la justice civile.

- Il ne faut pas non plus oublier de mentionner les risques de réputation et de confiance liés aux violations de la protection des données, qui peuvent dépasser de loin les risques prudentiels et pénaux. Les événements liés à la protection des données et à la sécurité de l'information représentent parfois des risques existentiels pour les entreprises (continuité des activités, responsabilité, etc.). Il convient d'en tenir dûment compte dans le cadre de la gestion des risques.

5. Clause de non-responsabilité

Le présent mémento est diffusé uniquement à titre d'information. Il ne constitue pas une check-list complète et ne peut se substituer à un conseil juridique. L'Union suisse des arts et métiers usam décline toute responsabilité qui pourrait découler de l'application ou de l'omission d'une recommandation par le présent document. Nous vous recommandons en outre de vous adresser à l'organisation sectorielle compétente, qui pourra vous fournir des indications supplémentaires.

6. Annexe: Documents-types

- Déclaration de protection des données (site Internet)
- Politique de protection des données (interne)
- Registre de traitement des données (structure)
- Analyse d'impact sur la protection des données (structure)
- Contrat de sous-traitance
- Clause de protection des données CGV

Mise à jour: 6 décembre 2022

Responsable du dossier

Dieter Kläy, Responsable des dossiers marché du travail, formation professionnelle et droit économique
Tél. 031 380 14 45, e-mail d.klaey@sgv-usam.ch