RÉSUMÉ DES OBLIGATIONS AU TITRE DE LA NOUVELLE LOI SUR LA PROTECTION DES DONNÉES (nLPD)

Cette note préparée par HDC sur mandat du Service de la culture de la Ville de Lausanne fournit un résumé des principales obligations s'appliquant en matière de protection des données personnelles. Les entreprises du pays doivent s'y conformer depuis le 1er septembre 2023. Cette note a un but informatif général et ne remplace pas un avis juridique dans un cas concret.

UN CHAMP D'APPLICATION LARGE

La Loi fédérale sur la protection des données (LPD) s'applique à toute personne physique ou morale (responsable du traitement) qui traite des **données personnelles**, soit des informations concernant une personne physique identifiée ou identifiable (personne concernée). C'est par exemple le nom, l'adresse, le numéro de téléphone, le numéro de réservation, l'adresse IP, le compte client, le numéro IBAN, le numéro AVS, etc. La notion de traitement est aussi large et inclut la simple collecte ou conservation des données personnelles. Les organes cantonaux sont soumis à des règles cantonales similaires à celles de la LPD. Quant aux responsables du traitement qui visent les résidents de l'EEE, ils peuvent être soumis au RGPD européen en plus du droit suisse.

LES PRINCIPES DE LA PROTECTION DES DONNÉES

En règle générale, un consentement n'est pas nécessaire pour traiter des données personnelles, mais elles doivent être traitées de **bonne foi** et de manière **transparente** pour les personnes concernées. Elles ne peuvent être utilisées que pour atteindre le **but** pour lequel elles ont été collectées

Dans la mesure du possible, le responsable du traitement doit s'assurer que les données qu'il traite sont **exactes**. Il doit aussi prendre des mesures techniques et organisationnelles pour assurer leur **sécurité**. Plus les données sont sensibles et plus les mesures de sécurité doivent être fortes.

Le **principe de proportionnalité** est la clé de voûte de la législation en matière de protection des données personnelles. Des données ne peuvent être traitées que si elles sont aptes et nécessaires pour le but prévu. On doit donc se demander si les données permettent d'atteindre le but, et si on ne peut pas y arriver avec moins de données. La proportionnalité implique aussi de limiter les accès aux données aux personnes qui en ont besoin et de les détruire ou anonymiser dès qu'elles ne sont plus nécessaires.

LE DEVOIR D'INFORMER

Le responsable du traitement doit informer la personne concernée de manière claire, même si les données ne sont pas collectées directement auprès d'elle. Cela peut se faire par une **politique de confidentialité**, par exemple sur le site web ou une affiche à l'entrée des locaux. Il faut indiquer l'identité et les coordonnées du responsable du traitement, le but du traitement, les catégories de données traitées, les catégories de destinataires des données et la liste des pays vers lesquels les données sont transmises.

LA SOUS-TRAITANCE ET LA COMMUNICATION À L'ÉTRANGER

Le responsable du traitement peut déléguer certains traitements de données à un sous-traitant, par exemple l'hébergement de données, la fourniture du service de billetterie, etc. Un contrat doit être conclu avec le sous-traitant, dans lequel le responsable du traitement donne des instructions au sous-traitant et lui rappelle notamment qu'il n'a le droit d'utiliser les données que pour lui fournir le service convenu. Le responsable du traitement reste responsable vis-à-vis des personnes concernées pour les actes de son sous-traitant.

Des données personnelles peuvent être communiquées **à l'étranger** sans formalités dans les pays de l'EEE, le Canada, la Nouvelle Zélande ou l'Uruguay. Pour les autres pays (considérés comme n'offrant pas un niveau de protection adéquat), des garanties supplémentaires sont nécessaires, par exemple un engagement contractuel sous la forme de clauses types de protection des données. Dans certaines limites, des dérogations peuvent s'appliquer.

LES SANCTIONS

En plus d'un risque de réputation ou d'une décision interdisant de traiter des données collectées en violation de la loi, certains comportements sont des contraventions pénales punies d'une amende pouvant aller jusqu'à CHF 250'000.-. C'est généralement la personne physique qui a intentionnellement violé l'obligation d'informer, qui a eu recours à un sous-traitant sans contrat, qui a communiqué des données dans un pays inadéquat sans garanties suffisantes ou encore qui a communiqué des informations fausses ou incomplètes.

LA PUBLICITÉ EN MASSE ET LES COOKIES

L'envoi de toute forme de publicité électronique en masse (newsletter, campagne de marketing, etc.) exige **le consentement** préalable des destinataires (opt-in), de mentionner clairement l'émetteur de la publicité et d'informer les personnes de leur droit de se désabonner gratuitement et facilement. Une exception existe pour **les clients**. S'ils ont été informés que de la publicité électronique serait envoyée et de leur droit de s'y opposer, un consentement n'est pas nécessaire pour de la publicité pour ses propres prestations ou activités. Ils doivent néanmoins pouvoir se désabonner à tout moment (opt-out).

Si des cookies sont placés sur un site web, les visiteurs doivent être informés et pouvoir s'y opposer (par exemple via les paramètres du navigateur). Un consentement est notamment nécessaire en cas de profilage.

OBLIGATION DE CONFIDENTIALITÉ

Les collaborateurs et collaboratrices sont soumis au devoir de discrétion, comme les sous-traitants. Seules les personnes qui ont besoin de traiter des données doivent y avoir accès. Celui qui communique sans droit à tiers des données personnelles secrètes dont il a eu connaissance en raison de son travail commet une infraction pénale, qui peut aussi être punie d'une amende pouvant aller jusqu'à CHF 250'000.-.

RÉCAPITULATIF DES DOCUMENTS À ÉTABLIR

☐	**Des contrats de sous-traitance** – avec chaque sous-traitant traitant des données personnelles et comprenant des instructions sur les traitements délégués et des garanties de confidentialité et de sécurité.	⚠ Obligatoire
☐	**Une déclaration ou politique de confidentialité** – à établir afin d'informer les personnes concernées des traitements de données effectués.	⚠ Obligatoire
☐	**Une annonce au Préposé fédéral à la protection des données (PFPDT) et à la personne concernée** – en cas de violation de sécurité entraînant un risque élevé pour les personnes concernées ou si cela est nécessaire pour protéger les personnes concernées.	Uniquement en cas de violation de sécurité des données
☐	**Un registre des activités de traitements** – il s'agit d'une cartographie interne des traitements de données personnelles qui recensera les traitements, les catégories de personnes concernées et les données traitées, les destinataires, les délais de conservation, les mesures de sécurité etc.	Uniquement pour les entreprises de plus de 250 collaborateurs, sauf en cas de risque élevé
☐	**Une analyse d'impact relative à la protection des données personnelles** – en cas de risque élevé, par exemple en cas de traitement de données sensibles à grande échelle ou de surveillance systématique de grandes parties du domaine public. Elle contient une description du traitement, une évaluation des risques ainsi que les mesures prévues pour y remédier.	Uniquement en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées
☐	**Un règlement de traitement** – contenant des informations sur l'organisation interne, sur les procédures de traitement et de contrôle des données, ainsi que sur les mesures visant à garantir la sécurité des données.	Uniquement lors de traitement de données sensibles à grande échelle ou de profilage à risque élevé