callnet.ch
Swiss Contact Center Association

Révision de la loi fédérale sur la protection des données (loi sur la protection des données, LPD) au 1er septembre 2023 ; conséquences pour les centres d'appels

1. INTRODUCTION

La loi révisée sur la protection des données (LPD) entrera en vigueur le 1er septembre 2023. Cette révision entraîne diverses adaptations et de nouvelles exigences pour les entreprises. callnet.ch en informe ses membres par le biais de cette fiche d'information.

Les centres d'appels respectivement les centres de contacts existent sous différentes formes. Ils peuvent faire partie de l'entreprise elle-même ou être des prestataires d'externalisation (sous-traitants), c'est-à-dire des mandataires. On peut également distinguer les centres d'appels qui répondent principalement aux appels, les transfèrent ou/et prennent des rendez-vous (inbound) et ceux qui passent des appels pour le compte d'entreprises (outbound).

Les principes de la loi sur la protection des données s'appliquent à tous les types de centres d'appels. Les dispositions spéciales pour les sous-traitants ne s'appliquent toutefois qu'aux centres d'appels qui ne sont pas directement intégrés dans leur propre entreprise. Il convient en outre de noter que les membres de callnet.ch ont leur siège exclusivement en Suisse et travaillent en premier lieu pour des entreprises suisses.

Ce document ne tient pas compte des règles concernant les mandants (donneurs d'ordre) de l'UE/EEE et d'autres pays. Ce document est axé sur la loi révisée sur la protection des données, qui entrera en vigueur le 1er septembre 2023. L'abréviation "LPD" désigne donc toujours la nouvelle loi sur la protection des données et non pas celle qui est encore en vigueur actuellement.

2. PRINCIPALES NOUVELLES DISPOSITIONS DE LA LPD CONCERNANT LES CENTRES D'APPELS

Seules *les personnes physiques* peuvent invoquer la loi révisée sur la protection des données, et non plus *les personnes morales* (art. 2, al. 1 LPD) ; cela n'a que peu de conséquences au quotidien, car la loi sur la concurrence déloyale (LCD) est plus centrale pour les entreprises et les protège. Un centre d'appels ne peut plus invoquer la LPD - mais cela ne se faisait guère dans le passé.

En ce qui concerne les définitions, *le profilage* (art. 5, let. f, LPD) a été ajouté. Par profilage, on entend "toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique". Dans des cas exceptionnels, il peut arriver que les centres d'appels procèdent à des profilages. S'ils procèdent à un profilage, ils doivent s'assurer qu'ils le communiquent clairement aux personnes concernées. Les cookies ont différentes fonctions : des "first party cookies" – qui garantissent le bon fonctionnement d'un site Internet – aux cookies fonctionnels, qui enregistrent par exemple un choix de langue, en passant par les cookies de performance, qui enregistrent le comportement de l'utilisateur, jusqu'aux cookies de marketing, qui affichent des annonces publicitaires adaptées aux intérêts supposés de l'utilisateur. Ces derniers constituent certainement un profilage.

Principes (art. 6 et 8 LPD) : les principes de la loi révisée sur la protection des données ne diffèrent pas, sur le fond, des principes en vigueur jusqu'à présent. La notion de reconnaissabilité (principe de transparence) n'existe cependant plus, elle fait partie intégrante de la bonne foi qui est également explicitement mentionnée dans la nouvelle LPD. Désormais, la destruction la plus rapide possible ou l'anonymisation des données est expressément stipulée dès que celles-ci ne sont plus nécessaires au but du traitement (art. 6, al. 4 LPD). Jusqu'à présent, cette disposition était considérée comme relevant de la proportionnalité.

Les responsables doivent assurer la protection des données dès *la conception* et par défaut. Un nouvel article a été créé à cet effet (art. 7 LPD). Ils doivent veiller à ce que le traitement des données soit strictement limité au minimum nécessaire pour l'utilisation prévue – sauf si la personne concernée en décide autrement.

Le traitement sur mandat, c'est-à-dire le transfert du traitement des données par le responsable à un sous-traitant, par exemple un spécialiste, reste possible (article 9 LPD). Les obligations du sous-traitant sont les mêmes que celles du responsable ; si un sous-traitant veut faire appel à un tiers, il doit obtenir *l'autorisation préalable* du mandant. Il est essentiel que le mandant sache en particulier qui est impliqué dans le mandat – car la responsabilité du traitement des données reste celle du mandant.

Une nouveauté importante est *l'analyse d'impact relative à la protection des données* (AIPD) selon l'article 22 de la LPD. Pour les nouveaux projets, il faut toujours se demander si des données personnelles seront traitées. Dans l'affirmative, il convient de déterminer, dans le cadre d'une analyse dite des seuils – parfois aussi appelée analyse des besoins de protection –, si ce traitement présente un risque élevé pour les personnes concernées (cf. la liste de contrôle "Analyse des besoins de protection" du Service de protection des données du canton de Zoug, resp. l'annexe "Analyse des valeurs seuils"). Si l'analyse des seuils est positive, une analyse d'impact sur la protection des données (AIPD) doit être effectuée conformément à l'article 22 de la LPD.

Une telle AIPD paraît plus compliquée qu'elle ne l'est en réalité ; là aussi, il existe divers outils, actuellement proposés par plusieurs cantons, mais aussi, à moyen terme, par le Préposé fédéral à la protection des données et à la transparence (PFPDT). On trouve de bons exemples auprès du Service de protection des données du canton de Saint-Gall (lien) et du Service de protection des données du canton de Zoug (lien) – mais attention : les lois cantonales ne s'appliquent à callnet.ch et à ses membres que s'ils travaillent pour une autorité cantonale.

Il est judicieux de procéder à une AIPD comme à une gestion des risques classique ; important : il faut évaluer le risque concret pour les personnes concernées, comme le fait ISO 31000.

Au lieu d'une liste de fichiers, les entreprises de plus de 250 collaborateurs doivent établir *un registre des activités de traitement* (art. 12 LPD). Les responsables et les sous-traitants tiennent chacun un registre de leurs activités de traitement. Les points pertinents pour un registre sont clairement formulés à l'article 12. Divers bons modèles sont disponibles, entre autres, auprès de la FMH, l'Association Suisse des Sociétés de Leasing ou Fiduciaire|Suisse.

L'obligation d'informer lors d'un traitement de données a été élargi (art. 19 LPD). Elle incombe aux responsables conformément à la loi. Les personnes concernées peuvent être informées soit par une déclaration de protection des données sur Internet, soit par des conditions générales (CG), soit encore oralement. En cas d'information orale, il est recommandé de la documenter pour des raisons de preuve. Cette obligation concerne également les données qui ne sont pas collectées directement auprès de la personne concernée. Si un centre d'appels recueille des données parce que la personne concernée a

appelé et souhaite par exemple convenir d'un rendez-vous pour une réparation, il est toutefois évident et facilement reconnaissable pour la personne que ses données sont recueillies (art. 6 al. 3 LPD).

L'obligation d'informer incombe au responsable et non au mandataire. Dans cette mesure, un centre d'appels devrait probablement tout au plus assumer ces obligations d'information en cas de mandat par le mandant.

De plus en plus d'incidents se produisent par suite d'hacking (piratage), des données apparaissent sur le Darknet, etc. Il s'agit d'*une violation de la sécurité des données* qui doit être traitée conformément à l'article 24 LPD. Il faut à nouveau une évaluation des risques concernant les risques pour la personnalité et les droits fondamentaux des personnes concernées et, en cas de risque élevé, une notification au PFPDT. Un processus devrait être établi à cet effet (cf. également le modèle FMH – doit être légèrement adapté, mais toutes les étapes pertinentes y sont décrites).

Une violation de la sécurité des données peut souvent devenir un événement médiatique. Il vaut donc la peine de connaître le processus ainsi que les principaux interlocuteurs. Si des services informatiques sont fournis par des tiers, ceux-ci doivent être impliqués dans le processus.

Les dispositions pénales (art. 60 et suivants LPD) ont été étendues lors de la révision et le montant des amendes est passé de CHF 10'000 à CHF 250'000. Ce qui n'a pas changé, c'est qu'il s'agit de délits intentionnels. Délibérément signifie avec "connaissance et volonté", du moins le résultat doit avoir été "considéré comme possible et accepté consciemment".

Les infractions comprennent :

- *Violation des obligations d'information, de renseignement et de collaboration* : une collecte de données ne devrait donc pas être effectuée en secret. Si une demande de renseignements est faite, elle doit être remplie de manière complète et conforme à la vérité. Les données qui ne sont plus disponibles ne peuvent toutefois pas être remises, de même que l'on ne peut pas se rendre punissable si, par mégarde, toutes les données ne sont pas remises ; comme décrit ci-dessus, c'est le responsable du traitement et non le sous-traitant qui est tenu de respecter le droit d'accès ;
- *Violation du devoir de diligence*, en ce sens que
    - des données sont transmises pour traitement dans un pays ne disposant pas d'une protection adéquate des données ou ne disposant pas des garanties ou des contrats/clauses contractuelles nécessaires,
    - des données sont transmises à un sous-traitant alors que leur transmission est interdite ou que celui-ci ne peut pas garantir une sécurité adéquate des données,
    - les exigences minimales en matière de sécurité des données, que l'on trouve dans le règlement aux articles 1 et suivants, ne sont pas respectées.

  Même cette infraction ne devrait guère être intentionnelle dans le cadre d'un traitement normal et soigneux des données personnelles.
- *Violation du secret professionnel* : il convient de noter que ce ne sont pas seulement certaines professions, comme les médecins, les avocats, les ecclésiastiques, le personnel soignant ou les fonctionnaires, qui sont tenus au secret professionnel, mais toutes les personnes en ce qui concerne le traitement de données personnelles, dans la mesure où ces données personnelles ont un rapport avec leur activité professionnelle. La violation du secret professionnel constituant

également un délit intentionnel, un comportement maladroit dans un bar ou un train ne constitue pas encore une violation. Un tel comportement peut plutôt entraîner une perte de réputation de l'employeur.

En résumé, le risque est faible : le risque de recevoir une amende est très faible, à condition de se comporter raisonnablement et de ne pas vouloir délibérément nuire à une personne.

3. PRINCIPALES DISPOSITIONS DE LA LPD APPLICABLES SANS CHANGEMENT

Les dispositions relatives à *la transmission de données à l'étranger* restent inchangées et doivent absolument être respectées : si des données sont transmises à un donneur d'ordre à l'étranger – attention : il peut également s'agir d'un prestataire de services cloud – il faut veiller à ce que les directives soient respectées. Les données peuvent être communiquées à l'étranger si la législation de l'État destinataire garantit une protection adéquate. Sinon, les règles selon l'art. 16 s. LPD s'appliquent.

Comme le droit actuel, la loi révisée accorde à toute personne le droit d'exiger du responsable du traitement qu'il lui indique si des données personnelles la concernant sont traitées. *(Droit d'accès* selon les articles 25 et suivants de la LPD). Ici aussi, il est recommandé de définir un processus de manière que les documents nécessaires puissent être remis dans le délai légal de 30 jours en cas d'éventuelle demande de renseignements. Il convient de noter que les demandes de renseignements portant sur des données du donneur d'ordre doivent également être traitées par le donneur d'ordre et non par le centre d'appels, si celui-ci agit en tant que mandataire.

En outre, même contre la volonté de la personne concernée, ses données peuvent être traitées à des fins de contrôle de solvabilité. Il est important que les données ne datent pas de plus de 10 ans et qu'aucune donnée concernant des personnes mineures ne soit traitée (art. 31, al. 2, let. c, LPD).

4. BON A SAVOIR : AUTRES DISPOSITIONS DE LA LPD

Désormais, le responsable doit également informer les personnes concernées *des décisions individuelles automatisées* qui ont une conséquence juridique ou qui affectent considérablement les personnes concernées (article 21 LPD). La pertinence de cette information augmente en raison de l'évolution technologique et de l'augmentation des décisions automatisées. L'utilisation de l'intelligence artificielle (IA) gagne en importance dans la vie quotidienne – et peut ainsi conduire à de nouvelles discriminations. Cela ne devrait pas être une priorité pour les centres d'appels actuellement, mais devrait devenir plus important à moyen terme.

En voici un exemple : si des candidats sont présélectionnés par un programme sur la base des mots-clés figurant dans leur CV et leurs certificats de travail, il s'agit d'une décision individuelle automatisée qui peut porter préjudice à la personne concernée ; il en va de même si la décision d'accorder un crédit est prise de manière automatisée. En revanche, il ne s'agit pas d'une décision discrétionnaire lorsque, lors d'un retrait au Bancomat, un certain montant n'est pas donné en raison de l'état du compte.

La réglementation de la transmission des données (*portabilité des données*) a été ajoutée et est réglée à l'article 28 LPD. Au quotidien, elle est surtout pertinente pour les plateformes telles que les canaux de médias sociaux. Il s'agit en premier lieu de données qui ont été communiquées par la personne concernée ou qui ont été créées avec son consentement.

5. SUITE DE LA PROCEDURE

Pour la suite de la procédure, il est recommandé d'établir *un plan de mesures* qui comprend les tâches suivantes.

Prochaines tâches pour les centres d'appels

- *Formaliser le flux d'informations* : si un centre d'appels agissant en tant que mandataire souhaite faire appel à d'autres tiers, le mandant doit en être informé au préalable. Cela peut également se faire au début du mandat. Si de nouveaux tiers sont ajoutés, le client doit à nouveau en être informé.
- Vérifier *la déclaration de protection des données* sur le site Internet – en particulier en ce qui concerne le traitement des données ; si le centre d'appels est le mandataire, l'obligation d'information incombe au mandant.
- Si plus de 250 employés : établir *un registre des activités de traitement des données*.
- Établir *des processus* pour traiter les demandes de renseignements et les violations de la sécurité des données.
- Pour les nouveaux projets, vérifier au moyen d'*une analyse des seuils s'*il y a lieu d'établir une AIPD.
- *Former* et sensibiliser les collaborateurs au traitement des données personnelles ; il est recommandé de se baser sur un règlement de protection des données.
- Le cas échéant, nommer une personne qui porte le "chapeau de la protection des données" ; la nomination d'un conseiller à la protection des données au sens de l'art. 10 LPD est facultative et n'est recommandée que sous certaines conditions. La fonction de conseiller/ère à la protection des données requièrent des connaissances approfondies en matière de protection des données.
- Vérifier si *un contrat de traitement des mandats* a été établi avec les sous-traitants (en particulier les prestataires de services informatiques) similaire à la convention de traitement des données en sous-traitance (cf. modèle FMH).
- *Effacer* les données qui ne sont plus nécessaires au sens de l'art. 6, al. 4, LPD.

6. CONCLUSION

A première vue, les exigences semblent élevées. Il convient toutefois de noter que la LPD révisée ne constitue pas une révolution et n'apporte pas de nouvelles exigences, mais qu'elle maintient pour l'essentiel les réglementations existantes. Il existe toutefois quelques exigences supplémentaires importantes telles que la AIPD et une obligation d'information plus étendue lors du traitement de données personnelles. Dans ce sens, on peut dire ce qui suit :

> "La législation suisse se limite à ce qui est important et le règle de manière générale, abstraite et neutre sur le plan technologique. **L'avantage de cette culture législative est que son application n'exige pas en premier lieu des connaissances, mais de la réflexion.**
>
> En étant prêt à **se mettre mentalement dans la peau de ses clients** et en **faisant preuve d'un peu de bon sens**, chaque entreprise peut trouver des solutions acceptables avec le texte concis de la loi et de l'ordonnance".
>
> Adrian Lobsiger, PFPDT, lors d'un exposé au Symposium on Privacy and Security 2023

Pour conclure, une remarque sur le règlement général sur la protection des données de l'UE (RGPD) : le

RGPD n'est guère applicable, car le principe du lieu du marché s'applique – à moins que : on recherche activement des clients dans l'espace UE/EEE. Dans ce cas, le RGPD s'applique à ces données clients et un traitement nécessite toujours un motif justificatif au sens de l'article 6 du RGPD.

Zurich, en juillet 2023