# CHANGEMENT DE PARADIGME EN MATIÈRE DE PROTECTION DES DONNÉES

**ANTOINE AMIGUET**
LL. M. (NYU), avocat à Genève

**PHILIPP FISCHER**
LL. M. (Harvard), avocat à Genève

Mots-clés: protection des données

La règlementation en matière de protection des données a récemment été modifiée dans l'Union européenne, par l'adoption du Règlement général sur la protection des données (RGPD) qui sera pleinement applicable à compter du 25. 5. 2018 et qui dispose d'un effet extraterritorial. Un processus de révision de la loi fédérale suisse sur la protection des données est actuellement en cours. Dans le cadre de ses activités professionnelles, chaque avocat traite des données personnelles. Ces révisions règlementaires doivent donc être suivies avec attention.

## I. Introduction

Les règles applicables en matière de protection des données sont actuellement soumises à une profonde mutation, dans un premier temps au sein de l'Union européenne (avec l'adoption d'un nouveau cadre légal disposant d'un effet extraterritorial), puis en Suisse. Toutes les entreprises suisses, y compris les études d'avocats, sont concernées par ces changements.

Le droit européen de la protection des données a été uniformisé par le biais de l'adoption du Règlement général sur la protection des données (le *«RGPD»*). À compter du 25. 5. 2018, le RGPD introduira un régime unifié au sein de l'Union européenne, en remplacement de la Directive actuelle (directive 95/46/CE) qui avait été transposée de manière disparate par les États membres. Cette réglementation européenne a une portée extraterritoriale. Elle s'appliquera, par exemple, aux entreprises suisses qui traitent des données personnelles dans le cadre de l'offre de biens ou de services à des personnes localisées dans l'Union européenne.

C'est probablement la Cour de Justice de l'Union européenne qui a accéléré l'adoption du nouveau cadre réglementaire européen. En 2014, cette juridiction européenne a jugé qu'un particulier bénéficiait du droit d'obtenir son «déréférencement» de moteurs de recherche sur Internet (affaire *Google Spain SL*[1]). En 2015, cette même autorité a également contraint la Commission européenne à renégocier les conditions auxquelles des données personnelles peuvent être transférées aux États-Unis (affaire *Schrems*[2]).

La Suisse n'est pas restée immobile face à ces développements règlementaires et jurisprudentiels. La décision rendue dans l'affaire *Schrems* a eu pour effet indirect d'amener la Suisse à modifier les conditions auxquelles un transfert de données personnelles aux États-Unis est possible à des conditions simplifiées[3]. Par ailleurs, le 15. 9. 2017, le Conseil fédéral a publié une version révisée de la loi fédérale sur la protection des données (le *«P-LPD»*). Les principaux objectifs du P-LPD sont (i) de tenir compte des développements technologiques et sociaux intervenus depuis l'adoption de la version initiale de la LPD actuelle en 1992 et (ii) d'adapter le cadre réglementaire suisse en matière de protection des données aux standards internationaux, en particulier à la Convention 108 du Conseil de l'Europe et au RGPD. Comme d'autres projets législatifs soumis aux Chambres fédérales durant ces dernières années, le P-LPD vise à aligner le droit suisse avec le cadre règlementaire européen. Cet ajustement est nécessaire afin que la Suisse continue à être reconnue en tant que juridiction dont la législation en matière de protection des données est jugée «adéquate» dans la perspective de l'Union européenne. Le maintien de ce label de qualité est essentiel pour permettre un transfert de données person-

1 Arrêt de la Cour de justice de l'Union européenne du 13. 5. 2014 dans l'affaire C-131/12 *(Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González).*

2 Arrêt de la Cour de justice de l'Union européenne du 6. 10. 2015 dans l'affaire C-362/14 *(Maximilian Schrems/Data Protection Commissioner).*

3 Cf. Préposé fédéral à la protection des données et à la transparence, 24e rapport d'activités 2016/2017, p. 29.

nelles entre la Suisse et l'Union européenne à des conditions raisonnables pour les entreprises.

Le Conseil fédéral escompte une entrée en vigueur du P-LPD le 1. 8. 2018[4], ce qui paraît optimiste. Compte tenu du processus parlementaire, une entrée en vigueur au début de l'année 2019 apparaît plus réaliste. Par ailleurs, le P-LPD prévoit un délai transitoire de deux ans à compter de son entrée en vigueur[5]. Ce nonobstant, toutes les entreprises suisses concernées, y compris les études d'avocats, devraient d'ores et déjà initier des travaux de mise en conformité[6].

Une *helicopter view* sur les projets de révision dans l'Union européenne et en Suisse permet de dégager les grands axes suivants:

- La transparence des processus de traitement de données personnelles sera significativement accrue. Chaque responsable devra informer en détail les personnes concernées du but et des modalités du traitement de leurs données personnelles. Vu que le responsable du traitement n'a pas nécessairement un contact direct avec les personnes concernées, des *privacy notices* – à la fois complètes et aisément compréhensibles – devront être publiées sur le site Internet des responsables de traitement. Par ailleurs, le droit d'accès, à savoir la possibilité pour une personne concernée d'obtenir des informations sur les données personnelles qui sont traitées, est également renforcé.
- Les nouvelles règles européennes et suisses visent à améliorer la mise en œuvre *(enforcement)* de la protection des données en renforçant les droits des personnes concernées par un traitement de données personnelles et en accordant des pouvoirs coercitifs aux autorités de contrôle. En Suisse, le Préposé fédéral à la protection des données et à la transparence (le *«Préposé»*) pourra procéder à des enquêtes, même si le prononcé des sanctions restera du ressort des autorités pénales[7]. Par ailleurs, les autorités de surveillance devront être informées immédiatement en cas de perte *(leak)* de données personnelles[8].

## II. Champ d'application du P-LPD

### *1. Qui est visé par le P-LPD?*

Le P-LPD s'applique aux traitements de données personnelles relatives aux personnes physiques (individus) par (i) des personnes privées (personnes physiques ou morales) et (ii) des organismes fédéraux suisses (article 2 [1] P-LPD). Les autorités cantonales sont régies par des normes cantonales de protection des données, lesquelles devraient être ajustées aux nouveaux standards fixés par le P-LPD[9]. La présente contribution se concentre essentiellement sur les règles applicables aux traitements de données personnelles par des personnes privées.

### *2. Quelles données sont visées par le P-LPD?*

Le P-LPD s'applique aux données personnelles, soit toutes les informations concernant une personne physique identifiée ou identifiable (article 4 [a] P-LPD). Contrairement à la LPD actuelle, le P-LPD ne s'applique plus au traitement des données personnelles des personnes morales. Cette approche est conforme au RGPD, qui se concentre également exclusivement sur les personnes physiques (individus).

Le P-LPD s'applique au *traitement de données personnelles,* défini comme toute opération relative à des données personnelles – quel que soit le moyen et les procédés utilisés –, en particulier la collecte, l'enregistrement, le stockage, l'utilisation, la modification, la communication (y compris naturellement la communication en dehors de Suisse), l'archivage, l'effacement ou la destruction des données (article 3 [d] P-LPD).

Sur le plan des définitions, il convient de noter les deux nouveautés suivantes:

(1) La définition des «données personnelles sensibles» a été élargie aux données génétiques et aux données biométriques identifiant une personne sans ambiguïté (article 4 [c] P-LPD).

(2) Le concept actuel de «profil de la personnalité» (une approche statique) sera remplacé par le concept de «profilage», qui est défini comme tout traitement automatisé de données personnelles dans le but d'analyser ou de prédire certaines caractéristiques personnelles d'un individu (telles que son rendement au travail, sa situation économique ou sa santé) (article 4 [f] P-LPD).

Ces définitions sont importantes dans la mesure où, lorsque le consentement de la personne concernée est requis, un consentement «exprès» est exigé si le traitement vise des données personnelles sensibles ou consiste en un profilage[10].

4 Message du 15. 9. 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (Message du 15. 9. 2017), FF 2017 6783.

5 Cf. articles 63 ss du P-LPD. Ce délai transitoire s'applique à la mise en conformité des processus de traitement de données personnelles en cours au moment de l'entrée en vigueur de la loi (cf. toutefois l'exception figurant à l'article 64 [3] P-LPD). Les nouveaux traitements de données personnelles mis en œuvre après l'entrée en vigueur du P-LPD sont toutefois soumis immédiatement aux nouvelles dispositions.

6 Pour un aperçu d'un plan de mise en œuvre (qui est destiné principalement à de grandes entreprises et qui devra être ajusté aux spécificités des études d'avocats), cf. TIM WYBITUL/CHRISTINA BREUNIG/LUKAS STRÖBEL, Praktische Hinweise zur DSGVO-Umsetzung, digma 2017, pp. 20 ss.

7 Sur la question des sanctions, cf. SYLVAIN MÉTILLE/DAVID RAEDLER, Révision de la LPD, des sanctions à contre-courant et à contre-raison, in: plaidoyer 2/2017, pp. 38 ss.

8 Sur la question du devoir d'information en cas de *leak,* cf. JAN KLEINER, Meldepflicht bei Datenschutzverletzungen, digma 2017, pp. 170 ss.

9 Dans ce contexte, cf. le Guide pratique rédigé par la Conférence des gouvernements cantonaux, disponible à l'adresse: http://www.dsb.bs.ch/datenschutz/privatim-und-kdk-leitfaden.html (consultation le 16. 11. 2017). Cf. également BEAT RUDIN, Anpassungsbedarf in den Kantonen, digma 2017, pp. 58 ss.

10 Cf. § IV.2 ci-dessous.

### *3. Champ d'application territorial du P-LPD*

Contrairement au RGPD[11], le P-LPD n'indique pas expressément son champ d'application territorial. Cela dit, il est généralement admis que les règles suisses de protection des données s'appliquent à toutes les activités de traitement de données qui se déroulent en Suisse.

Pour autant que la mise en œuvre du P-LPD par la voie d'une action civile soit concernée, le P-LPD s'appliquera si:

- la personne concernée a sa résidence habituelle en Suisse (pour autant que celui qui traite les données puisse s'attendre à ce que le préjudice financier se produise en Suisse);
- celui qui traite les données a sa résidence habituelle ou son siège social en Suisse; ou
- le préjudice financier résultant du traitement des données se produit en Suisse (pour autant que celui qui traite les données puisse s'attendre à ce que le préjudice financier se produise en Suisse) (cf. article 139 de la loi fédérale sur le droit international privé).

En outre, le Tribunal fédéral a indiqué dans une décision de principe[12] que les règles suisses de protection des données s'appliquent dès que les données personnelles sont collectées en Suisse, même si ces données personnelles sont enregistrées par la suite sur des serveurs situés en dehors de la Suisse.

## III. Nouvelles règles européennes

Le RGPD a été adopté le 27. 4. 2016 et remplacera la Directive n° 95/46/EC en matière de protection des données. Le RGPD sera pleinement applicable à compter du 25. 5. 2018[13].

L'objectif du RGPD est d'assurer un niveau de protection des personnes physiques élevé et cohérent en:

- renforçant les droits des individus;
- assurant une mise en œuvre accrue des règles en matière de protection des données;
- rationnalisant les transferts internationaux de données personnelles; et
- mettant en place des standards globaux de protection des données et faisant de la conformité à ces standards un élément de la gouvernance d'entreprise de toute organisation publique ou privée[14].

### *1. Portée extraterritoriale du champ d'application du RGPD*

Le RGPD s'appliquera avant tout au traitement de données par des responsables de traitement ou des sous-traitants situés dans l'Union européenne.

Le RGPD s'appliquera également à des responsables de traitement ou des sous-traitants situés hors de l'Union européenne (par exemple en Suisse) qui traitent des données personnelles, lorsqu'ils:

- offrent des biens ou des services à des personnes situées dans l'Union européenne (la réponse à cette question présuppose de déterminer si le comportement du responsable du traitement [par exemple les formulations utilisées sur son site Internet] permet de conclure que ce dernier entend offrir des biens ou des services à des personnes localisées dans l'Union européenne *[Marktortprinzip]*[15]); ou
- procèdent au «suivi du comportement» de personnes situées dans l'Union européenne, par exemple en analysant le comportement de visiteurs d'un site Internet *(cookies)* ou des utilisateurs d'une *app* (article 3, paragraphe 2 RGPD).

Le RGPD pourra également s'appliquer à des sociétés suisses si elles traitent des données personnelles pour le compte de responsables de traitement européens ou recourent à des sous-traitants situés dans l'Union européenne.

Par conséquent, toute entité suisse devrait examiner l'application possible du RGPD à ses activités de traitement de données, si cette entité suisse:

- a des clients ou des employés situés dans l'Union européenne (ou traite des données personnelles de tierces personnes situées dans l'Union européenne, telles que des fournisseurs de services);
- recourt à des sous-traitants situés dans l'Union européenne;
- suit les activités en ligne de personnes situées dans l'Union européenne, par exemple en suivant les visites faites sur un site Internet ou l'utilisation d'une *app;* ou
- prend part au traitement de données personnelles en tant que sous-traitant, pour le compte d'un responsable de traitement situé dans l'Union européenne.

### *2. Principales conséquences pratiques*

L'application du RGPD à un responsable de traitement ou à un sous-traitant en Suisse entraînera principalement les conséquences suivantes:

- Le responsable de traitement/sous-traitant devra se conformer aux dispositions du RGPD, d'ici au 25. 5. 2018.

---

**11** Cf. § III ci-dessous.

**12** ATF 138 II 346, c. 3 *(Google Street View).*

**13** Sur ces questions, cf. SÉBASTIEN FANTI, Le nouveau règlement général sur la protection des données et la Suisse, ExpertFocus 2017/11, pp. 856 ss.

**14** Compte tenu du fait qu'un certain nombre de concepts-clés du RGPD ne sont pas définis avec précision dans le texte du règlement, il convient de suivre avec attention les notices interprétatives publiées au fur et à mesure sur le site du «Groupe de travail Article 29», auquel succédera prochainement le «Comité européen de la protection des données» (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [consultation le 16. 11. 2017]).

**15** Sur ces questions, cf. également LUKAS BÜHLMANN/MICHAEL REINLE, Extraterritoriale Wirkung der DSGVO, digma 2017, pp. 8 ss, 9. Ces auteurs indiquent que les critères développés dans la jurisprudence de la Cour de justice de l'Union européenne en matière de contrats de consommation pourront être utilisés à titre de points de repère (cf. notamment arrêt de la Cour de justice de l'Union européenne du 7. 12. 2010 dans les affaires C-585/08 et C-144/09[Pammer/Alpenhof] qui définit les conditions auxquelles une entreprise est réputée «diriger ses activités» vers un État).

De manière générale, les termes du RGPD sont relativement semblables aux termes du P-LPD, qui entrera toutefois en vigueur seulement le 1. 8. 2018 (selon les vœux du Conseil fédéral). En tout état de cause, l'on peut constater que le RGPD offre un niveau significativement plus élevé de protection des données que la LPD actuelle.

- Le responsable de traitement/sous-traitant devra examiner la nécessité de nommer un «représentant» au sein de l'Union européenne (article 27 RGPD). Dans ce contexte, les points suivants doivent être considérés:
  - un seul représentant devra être nommé au sein de l'Union européenne (et non pas un représentant dans chaque État membre de l'Union européenne);
  - le représentant devra être établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi;
  - le représentant peut être une entité affiliée du responsable de traitement/sous-traitant;
  - le représentant devra être la personne de contact pour les autorités de contrôle des États membres de l'Union européenne.

## IV. Questions de fond (aspects choisis)

Cette section de notre contribution est consacrée à la discussion de deux aspects saillants des nouvelles règles en matière de protection des données, à savoir le devoir d'information (cf. § IV.1 ci-dessous) et le consentement (cf. § IV.2 ci-dessous).

### *1. Devoir d'information*

*A) Modalités*

Un responsable de traitement doit informer les personnes concernées du traitement de leurs données personnelles. Cette obligation doit être respectée, que les données personnelles soient collectées auprès des personnes concernées elles-mêmes (collecte directe) ou non (collecte indirecte) (article 17 [1] P-LPD).

Le devoir d'information est un corollaire du consentement (cf. § IV.2 ci-dessous). En effet, lorsque le consentement de la personne concernée est requis pour justifier un traitement de données personnelles le respect du devoir d'information est une condition pour que le consentement soit valablement donné. Le devoir d'information doit toutefois être respecté même lorsque le consentement de la personne concernée n'est pas requis.

Un responsable de traitement doit communiquer les informations permettant aux personnes concernées d'exercer leurs droits. Le degré de détail des informations à fournir dépendra du type de données personnelles qui sont traitées, ainsi que de la nature et de l'étendue du traitement. Le responsable de traitement doit fournir au minimum les informations suivantes aux personnes concernées (article 17 [2] P-LPD):

- l'identité et les coordonnées du responsable de traitement;
- la finalité du traitement;
- la communication éventuelle de données personnelles à une tierce personne; et
- la communication éventuelle de données personnelles vers une juridiction autre que la Suisse.

Le responsable de traitement doit veiller à ce que les personnes concernées puissent effectivement prendre connaissance de ces informations par un moyen facilement accessible, mais pas à ce qu'elles s'informent effectivement[16].

En cas de collecte directe, le responsable de traitement doit fournir les informations requises aux personnes concernées lorsque les données personnelles sont obtenues (article 17 [2] P-LPD *ab initio*). En cas de collecte indirecte, le responsable de traitement doit communiquer les informations requises au plus tard un mois après qu'il a obtenu les données personnelles. S'il communique les données personnelles avant l'échéance de ce délai à des destinataires, les informations doivent être fournies à la personne concernée au plus tard lors de la communication (article 17 [5] P-LPD).

Le P-LPD ne prévoit pas d'exigence spécifique quant à la forme que doit revêtir la communication de l'information. Pour des raisons de preuve, il est cependant recommandé de fournir l'information requise par écrit. L'information peut être fournie sur une base individuelle ou collective, par exemple par le biais des conditions générales ou d'une *privacy notice* publiée sur un site Internet.

*B) Exceptions et restrictions*

Le devoir d'information ne s'applique pas notamment lorsque (article 18 [1] P-LPD):

- la personne concernée a déjà été informée. Cela peut se présenter dans différentes situations, par exemple lorsque la personne concernée a valablement donné son consentement par l'intermédiaire de conditions générales. Lorsque la personne a elle-même rendu accessible les données, sans intervention du responsable du traitement (par exemple la remise d'un dossier de candidature), elle est en principe considérée comme informée de la collecte de données[17], mais pas nécessairement de tous les traitements envisagés;
- le traitement de données personnelles est prescrit par la loi. Cela est notamment le cas pour un intermédiaire financier lorsque la loi l'oblige à traiter certaines données, par exemple dans le cadre de la lutte contre le blanchiment d'argent;
- le responsable du traitement est également délié du devoir d'informer lorsqu'il est soumis à une obligation légale de garder le secret. Cette disposition prévient un conflit de normes en confirmant la primauté du devoir de confidentialité sur le devoir d'information.

**16** Message du 15. 9. 2017, FF 2017 6668.
**17** Message du 15. 9. 2017, FF 2017 6671.

En cas de collecte indirecte, le devoir d'information ne s'applique pas non plus lorsque l'information est impossible à donner ou que sa communication nécessite des efforts disproportionnés (article 18 [2] P-LPD):
- l'information est impossible lorsque la personne concernée n'est pas identifiable (par exemple la photo d'une personne inconnue)[18]. Cela dit, il ne suffit pas de supposer que l'identification est impossible. Il faut procéder à un minimum de recherche, dans les limites du raisonnable;
- les efforts déployés pour informer la personne concernée sont disproportionnés dès lors qu'ils paraissent injustifiés par rapport aux bénéfices que la personne concernée retirerait de l'information. Dans ce contexte, il faut notamment tenir compte du nombre de personnes concernées. Cette dernière exception doit être interprétée de manière restrictive: le responsable du traitement doit déployer tous les efforts qu'on est en droit d'attendre de lui dans le cas d'espèce pour remplir son devoir d'information. Ce n'est que si ces efforts restent vains que l'on considérera que l'information n'est pas possible[19].

Dans certaines circonstances, la communication de l'information requise peut également être restreinte, repoussée ou supprimée. Ce sera notamment le cas lorsque (article 18 [3] [a] et [c] P-LPD):
- les intérêts prépondérants d'un tiers le requièrent. Cette disposition vise en premier lieu les cas dans lesquels les informations concernant le traitement des données personnelles de la personne concernée contiennent aussi des informations sur des tiers. Dans certains cas, les intérêts de ce tiers peuvent être lésés par l'accomplissement du devoir d'information[20];
- les intérêts prépondérants du responsable du traitement l'exigent, à condition qu'il ne communique pas les données personnelles à des tiers. Un tel intérêt prépondérant ne peut pas être admis facilement. Il convient d'effectuer une pesée entre l'intérêt de la personne concernée à être informée d'un traitement de données personnelles afin de faire valoir ses droits et l'intérêt éventuel du responsable du traitement[21].

*C) Sanctions*

La violation intentionnelle du devoir d'information peut entraîner une sanction pénale sous la forme d'une amende de CHF 250 000.– au plus, aux conditions prévues par les dispositions pénales du P-LPD (cf. article 54 P-LPD).

*D) Règles plus strictes du RGPD*

Les informations à fournir aux personnes concernées selon le RGPD sont sensiblement plus nombreuses que celles exigées par le P-LPD (cf. articles 13 et 14 RGPD). Les informations doivent en principe être données par écrit ou par d'autres moyens, y compris, lorsque c'est approprié, par voie électronique (article 12, paragraphe 1 RGPD).

Les exceptions au devoir d'information sont semblables à celles prévues par le P-LPD. Toutefois, sauf lorsque la personne concernée dispose déjà des informations, les exceptions prévues par le RGPD s'appliquent seulement en cas de collecte indirecte de données personnelles (article 13, paragraphe 4 et article 14, paragraphe 5 RGPD).

*E) Conséquences pratiques*

Les *privacy notices* existantes doivent être revues avec soin afin de s'assurer qu'elles sont conformes aux exigences accrues prévues par le P-LPD. Pour autant que le RGPD s'applique à leurs activités, les responsables de traitement ou sous-traitants localisés en Suisse doivent également tenir compte des règles européennes plus strictes en matière de devoir d'information.

### *2. Consentement*

Tout traitement de données personnelles doit être licite (article 5 [1] P-LPD). Pour que cette condition soit réalisée, le traitement de données personnelles doit être justifié par la loi, par un intérêt prépondérant public ou privé, ou par le consentement de la personne concernée (article 27 P-LPD). Contrairement à une idée répandue, le consentement de la personne concernée n'est ainsi pas la seule alternative disponible pour s'assurer qu'un traitement de données personnelles soit licite.

Parmi les motifs justificatifs prévus par la loi, on peut citer par exemple les obligations de vérification prévues par la loi fédérale sur le blanchiment d'argent ou l'obligation de conservation prévue par l'article 958*f* du Code des obligations.

Un intérêt prépondérant du responsable de traitement existe notamment lorsque le traitement de données personnelles est en relation directe avec la conclusion ou l'exécution d'un contrat si les données personnelles traitées concernent le cocontractant. Cet exemple ne constitue toutefois pas un motif justificatif absolu. Une pesée des intérêts en présence doit toujours être effectuée entre, d'une part, l'intérêt du responsable du traitement à traiter ces données et, d'autre part, l'intérêt de la personne concernée à en disposer librement.

*A) Principes généraux*

Lorsque le consentement de la personne concernée est requis, celle-ci ne consent valablement que si elle exprime librement et clairement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée (article 5 [6] P-LPD *ab initio*). La déclaration de la personne concernée doit exprimer la volonté de celle-ci sans ambiguïté. Conformément au principe de la proportionnalité, plus le processus peut porter atteinte aux droits

**18** Message du 15. 9. 2017, FF 2017 6671.
**19** *Idem.*
**20** Message du 15. 9. 2017, FF 2017 6672.
**21** Message du 15. 9. 2017, FF 2017 6673.

des personnes concernées, plus le consentement doit être clair[22]. En règle générale, un consentement «ordinaire» [cf. § a] ci-dessous) suffit. Dans deux cas, le consentement doit toutefois être «exprès» [cf. § b] ci-dessous).

a) Consentement ordinaire

Le P-LPD ne prévoit pas de forme particulière pour le consentement ordinaire (article 5 [6] P-LPD *ab initio*). En particulier, il n'est pas lié à une déclaration écrite.

La personne concernée peut ainsi donner son consentement par la manifestation tacite de sa volonté. Dans ce cas, la manifestation de la volonté ne découle pas de la déclaration elle-même, mais d'un comportement qui, compte tenu des circonstances, peut être compris par le responsable du traitement comme l'expression claire de la volonté de la personne concernée. Celle-ci peut, par exemple, manifester sa volonté par actes concluants, notamment en accomplissant ses obligations contractuelles.

Une manifestation de la volonté est toutefois nécessaire. Sauf exception, le simple silence ou l'inaction ne peuvent pas constituer un consentement valable au traitement de données personnelles.

b) Consentement exprès

Le P-LPD prévoit que le consentement doit être exprès dans les deux cas suivants (article 5 [6] P-LPD *in fine*):

- le traitement concerne des données sensibles. Les données sensibles sont définies comme les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; les données sur la santé, la sphère intime ou sur l'origine raciale ou ethnique; les données génétiques; les données biométriques identifiant une personne physique de façon unique; les données sur des poursuites ou sanctions pénales et administratives; les données sur des mesures d'aide sociale (article 4 [c] P-LPD);
- le traitement consiste en un profilage. Comme indiqué ci-dessus, le profilage est défini comme un processus consistant à évaluer de manière automatisée certaines caractéristiques d'une personne sur la base des données personnelles traitées, par exemple pour analyser son comportement ou ses préférences (article 4 [f] P-LPD).

Une déclaration de volonté est «expresse» lorsqu'elle est formulée oralement, par écrit ou par un signe, et découle directement des mots ou du signe employés[23]. La déclaration de volonté en tant que telle doit manifester clairement la volonté dans sa forme même. Cela peut se faire notamment en signant un document ou en cochant une case. Lorsqu'un consentement exprès est requis, il ne peut pas être tacite[24].

*B) Sanctions*

En l'absence d'autres motifs justificatifs, un traitement de données effectué sans le consentement de la personne concernée constitue une atteinte illicite à sa personnalité. Dans ce cas, la personne concernée peut notamment requérir l'interdiction du traitement et/ou l'effacement des données personnelles le concernant (articles 28 ss du Code civil).

Lorsqu'un traitement illégal de données s'accompagne de la violation du devoir d'informer la personne concernée (ce qui sera généralement le cas), la personne qui contrevient intentionnellement à ce devoir pourra être punie, sur plainte, d'une amende de CHF 250 000.– au plus aux conditions prévues par les dispositions pénales du P-LPD (cf. article 54 P-LPD).

*C) Règles plus strictes du RGPD*

Les conditions applicables au consentement prévues par le RGPD sont plus strictes que celles du P-LPD. En particulier, lorsque le consentement est requis, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données personnelles la concernant (article 7, paragraphe 1 RGPD) pour une ou plusieurs finalités spécifiques (article 6 [1] [a] RGPD)[25].

Le RGPD contient également des exigences de forme qui vont au-delà de celles prévues par le P-LPD. En particulier, si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement doit être présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples (article 7, paragraphe 2 RGPD).

Le RGPD précise également que, pour que le consentement soit donné librement, il ne faut pas que le consentement soit une condition à l'offre du service si le traitement des données personnelles n'est pas nécessaire à l'exécution du contrat (article 7, paragraphe 4 RGPD). En d'autres termes, le consentement à un traitement de données qui n'est pas nécessaire à l'exécution du contrat (par exemple le traitement de données personnelles à des fins de *marketing*) n'est pas donné librement s'il constitue une condition à l'offre de services.

*D) Conséquences pratiques*

Dans une perspective pratique, la question du «consentement» peut être abordée après l'établissement du registre des traitements de données personnelles. En effet, en vertu de l'article 11 P-LPD, les responsables du traitement et les sous-traitants doivent tenir un registre des activités de traitement. Dans le cadre de ce registre, il est possible d'identifier les traitements qui doivent être couverts par un consentement, puis de s'assurer que ce consentement a été obtenu valablement.

**22** Message du 15. 9. 2017, FF 2017 6647, et références citées.
**23** Pour une discussion de ces questions, cf. DAVID ROSENTHAL, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. 2. 2017.
**24** Message du 15. 9. 2017, FF 2017 6648
**25** Sur ces questions, cf. BARBARA WIDMER, Ist Einwilligung gleich Einwilligung?, digma 2017, pp. 188–189.

## V. Impact sur les études d'avocats

Comme indiqué ci-dessus, le nouveau cadre légal en matière de protection des données s'articule principalement autour (i) d'un renforcement des exigences en matière de transparence des processus de traitement de données personnelles et (ii) d'une mise en œuvre *(enforcement)* accrue de ces normes, tant sous l'angle (a) des droits à disposition des personnes concernées que (b) dans la perspective des moyens d'action du Préposé et des autorités pénales.

Le corollaire de ce renforcement des moyens d'action à disposition des particuliers et des autorités est la nécessité d'adapter la documentation et les processus internes au sein de toutes les entreprises concernées. Il appartiendra en effet à chaque responsable du traitement d'apporter la preuve qu'il a pris toutes les mesures nécessaires pour se conformer aux nouvelles règles[26].

Compte tenu du fait qu'ils traitent des données personnelles (notamment de clients et d'employés), les avocats sont directement concernés par cette évolution. De notre point de vue, chaque étude d'avocats devrait nommer en son sein une (ou plusieurs) personne(s) plus spécifiquement en charge de la mise en œuvre de ces nouvelles règles. Cette personne devra travailler en étroite collaboration avec la personne (interne ou externe) en charge de l'infrastructure informatique de l'étude. Le cahier des charges d'une telle personne devrait, notamment, comprendre les points suivants:

- établir un inventaire de tous les traitements de données personnelles auxquels procède l'étude d'avocats, soit directement, soit par le biais de sous-traitants[27];
- examiner s'il convient d'ajuster le modèle de lettre d'engagement de l'étude à la lumière des nouvelles exigences en matière de protection des données;
- définir des processus internes pour le traitement des requêtes des personnes concernées (tel que le droit d'accès aux données personnelles ou le droit à l'oubli);
- définir un processus en cas de *leak* de données personnelles;
- examiner la nécessité de nommer un «représentant» au sein de l'Union européenne (si le RGPD s'applique à l'étude d'avocats).

En Suisse, la LPD a longtemps été considérée comme un tigre de papier. Après une décennie pendant laquelle la transparence et l'échange de données personnelles dominaient le débat public (notamment s'agissant de données bancaires), les questions de protection de la sphère privée et des données personnelles reviennent sur l'avant de la scène. Le nouveau cadre légal sortira sans doute le tigre de sa torpeur.

---

**26** Cf. notamment le principe de l'*accountability* visé spécifiquement à l'article 5 (2) RGPD.

**27** Sur ces questions, cf. BENOÎT CHAPPUIS/ADRIEN ALBERINI, Secret professionnel de l'avocat et solutions *cloud,* Revue de l'Avocat 8/2017, pp. 337 ss.