L'OBLIGATION DE «PRIVACY BY DESIGN» EN SUISSE ET SON IMPLÉMENTATION DANS LES ÉTUDES D'AVOCATS

DEBORAH LECHTMAN
Avocate, modératrice du Forum de protection des données du Barreau de l'Ordre des avocats de Genève, CAS in Financial Regulations, OA Legal SA, Genève

Mots-clés: *Privacy by Design,* protection des données dès la conception, mesures techniques et organisationnelles appropriées, analyse des risques

La révision de la loi fédérale sur la protection des données introduit l'obligation pour le responsable du traitement de se conformer au principe de la protection des données dès la conception *(Privacy by Design),* conformément au droit européen. Dans le cadre de leurs activités professionnelles, les avocats suisses doivent s'interroger sur leur conformité avec cette obligation et prendre les mesures techniques et organisationnelles appropriées. Le processus est long et technique, si bien que les études d'avocats doivent anticiper l'entrée en vigueur de la loi révisée.

I. Introduction

Le concept de *Privacy by Design* (respect de la vie privée «dès la conception») est né dans les années 1990 face au constat que la protection de la vie privée ne saurait être assurée uniquement par le respect de normes juridiques[1]. Il vise à intégrer le respect de la vie privée lors de la conception des systèmes informatiques et des pratiques d'une entreprise.

Cette notion, déjà consacrée en droit européen (article 25 §1 RGPD[2]), a été introduite dans le cadre de la révision de la loi fédérale sur la protection des données (*«nLPD»*[3]*;* voir art. 7 al. 1 et 2 nLPD). Le Conseil National et le Conseil des Etats ont adopté la nLPD le 25. 9. 2020 et la date d'entrée en vigueur de la nLPD n'a pas encore été fixée[4].

Si la notion paraît abstraite, l'obligation qui en découle est quant à elle concrète. Les entreprises privées telles que les études d'avocats devront en principe se conformer à ce devoir dès l'entrée en vigueur de la nLPD.

La présente contribution a pour objectif de présenter l'obligation de protection des données dès la conception, d'examiner son étendue et de proposer certains moyens pratiques de mise en œuvre au sein des études d'avocats.

II. Protection des données personnelles dès la conception *(Privacy by Design)*

1. La notion de protection «dès la conception»

A) Prévenir plutôt que guérir

La protection des données dès la conception se caractérise par des mesures proactives visant à prévenir et minimiser les risques d'atteintes aux droits des personnes concernées[5]. L'obligation débute ainsi en amont des opérations de traitement, avant la collecte des données. Son but est d'assurer un traitement conforme à la loi du début à la fin du traitement des données (i. e. de la collecte à la suppression de la donnée, y compris l'archivage).

Ce principe ne doit pas être confondu avec la protection des données par défaut *(privacy by default),* qui exige de traiter le moins de données possibles par des préréglages appropriés (art. 7 al. 3 nLPD; voir aussi l'art. 25 §2 RGPD qui prévoit un principe similaire). À titre d'exemple, prévoir la possibilité pour un internaute de s'abonner *(opt-in)* à une newsletter est une mesure de protection des données par défaut. Les deux principes n'en restent pas

1 Voir les 7 principes fondamentaux développés par ANN CAVOUKIAN, Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada): https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf (consulté pour la dernière fois le 20. 9. 2020).

2 Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

3 Projet de loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15. 9. 2017, in: FF 2017 p. 6803 ss.

4 Texte de la nLPD: https://www.parlament.ch/centers/eparl/curia/2017/20170059/Texte%20pour%20le%20vote%20final%203%20NS%20F.pdf.

5 Voir ANN CAVOUKIAN, les 7 Principes Fondamentaux.

moins étroitement liés, dans la mesure où de telles fonctionnalités doivent être intégrées dès la conception[6].

Une étude d'avocats devra ainsi inventorier tous ses traitements de données personnelles, qu'il s'agisse de traitements informatiques ou physiques ou par le biais de sous-traitants, et déterminer au cas par cas si le traitement est conforme aux prescriptions en matière de protection des données pendant toute la durée du cycle de vie des données personnelles. Elle devra ainsi intégrer le principe de protection des données dès la conception dans les logiciels informatiques qu'elle utilise.

B) Implémenter des mesures techniques et organisationnelles

La nLPD ne donne pas d'exemple de mesures techniques et organisationnelles à implémenter pour assurer qu'un traitement soit conforme à la protection des données. Le Conseil fédéral cite notamment la fixation d'échéances régulières pour supprimer ou anonymiser les données. Il recommande d'implémenter un système permettant de réduire le nombre de données personnelles traitées (minimisation des données) et de contrôler leur durée de conservation avant le début du traitement[7]. L'on peut aussi mentionner le guide publié par le Préposé fédéral à la protection des données et à la transparence (le *«Préposé»*) en matière de sécurité des données (selon le droit actuel)[8].

Afin de permettre une application effective de la règlementation, le Conseil fédéral insiste sur le recours à la technologie, qu'il considère «au service de la protection des données personnelles»[9]. Toutefois, l'obligation de protection des données dès la conception nécessite également des mesures ne recourant pas à des systèmes informatiques[10]. Le Comité Européen de la Protection des données donne l'exemple d'une formation basique pour employés permettant de les sensibiliser aux règles en matière de traitement des données personnelles[11].

Une étude d'avocat implémentera ainsi, à choix, des procédés techniques et organisationnels, tels que des directives et formations internes, ou des procédés de gestion électronique des données.

C) Choisir les mesures appropriées

Le devoir de protection des données dès la conception impose d'adopter des mesures techniques et organisationnelles «appropriées». Le caractère approprié d'une mesure s'analyse au regard notamment de l'état de la technique (i. e. progrès technologiques), du type de traitement, de son étendue ainsi que de la gravité du risque induit pour la personnalité et les droits fondamentaux des personnes concernées (art. 7 al. 2 nLPD).

Convient-il d'appliquer la mesure la plus stricte à tout type de traitement? Chaque traitement ne requiert pas le même niveau de protection. Plus le traitement est risqué pour les droits des personnes concernées, plus la mesure technique devra être efficace[12].

En tenant compte de la sensibilité de certaines données traitées au sein d'une étude, de l'utilisation croissante de systèmes informatiques ainsi que de l'efficacité des solutions digitales, une mesure technologique apparaîtra ainsi souvent nécessaire. Dans l'analyse des risques, il ne faut toutefois pas oublier que les incidents sont souvent le fait d'erreurs humaines, par exemple un employé qui transmettrait des données à la mauvaise personne ou qui ouvrirait un fichier frauduleux. La sensibilisation des employés aux risques ainsi que des processus internes clairs en cas d'incident sont ainsi nécessaires pour se conformer au principe de protection des données dès la conception.

Au vu de l'activité exercée et du type de structure, une étude d'avocats aura tendance à combiner les différents types de mesures selon les traitements effectués. Si l'aspect économique aura certainement un poids lors de ces choix, l'efficacité des mesures devra être analysée au cas par cas. Par ailleurs, une étude qui entame cette réflexion doit anticiper non seulement les coûts financiers, mais également la main d'œuvre requise pour implémenter et maintenir des mesures efficaces[13].

Le processus décrit ci-dessus ne doit pas être confondu avec l'analyse d'impact relative à la protection des données personnelles[14] *(privacy impact assessment; «AIPD»).* Une AIPD sera nécessaire si le traitement envisagé présente un risque qualifié d'«élevé» pour la personnalité ou pour les droits fondamentaux de la personne concernée[15].

2. Sujets de l'obligation

La LPD[16] ainsi que son ordonnance[17] s'appliquent en particulier aux personnes privées (art. 2 al. 1 let. a LPD et art. 2 al. 1 let. a nLPD). L'obligation de protection des données dès la conception incombe au responsable du traitement, soit la personne qui détermine les finalités et les moyens du traitement des données personnelles (art. 5 let. j nLPD).

A) Études d'avocats

Les études d'avocats sont sujettes au respect du droit de la protection des données personnelles. Le secret professionnel de l'avocat ne constitue pas une exception à cette règle[18].

---

6 Message du Conseil fédéral 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 du 15. 9. 2017, in FF: 2017, p. 6565 ss, p. 6649 (Message du 15. 9. 2017).
7 Message du 15. 9. 2017, p. 6649.
8 Préposé fédéral à la protection des données et à la transparence, Guide relatif aux mesures techniques et organisationnelles de la protection des données, 2015 (Guide du Préposé).
9 Message du 15. 9. 2017, p. 6648–6649.
10 Comité Européen de la Protection des Données, Lignes directives 4/2019 sur l'art. 25, Data Protection by Design and by Default, 13. 11. 2019, p. 6 (Lignes directrices du CEPD).
11 Voir Lignes directrices du CEPD, p. 6.
12 Message du 15. 9. 2017, p. 6649; Lignes directrices du CEPD, p. 6.
13 Lignes directrices du CEPD, p. 8.
14 Art. 22 nLPD; voir art. 35 RGPD.
15 DI TRIA L., L'analyse d'impact relative à la protection des données (AIPD) en droit européen et suisse, in: sic! 2020 p. 119, p. 126.
16 Loi fédérale sur la protection des données du 19. 6. 1992, RS 235.1 (LPD).
17 Ordonnance relative à la loi fédérale sur la protection des données du 14. 6. 1993, RS 235.11 (OLPD).
18 KAZEMI R./LENHARD T., Datenschutz und Datensicherheit in der Rechtsanwaltskanzlei, 3e éd., Bonn 2017, n. 13 à 15 p. 7 s.

Un nombre significatif de données personnelles est traité par les études en tant que responsables du traitement (i. e. employés, clients, prestataires, prospects et tiers). Celles-ci traitent des données personnelles dites «sensibles» telles que les données relevant de la sphère intime, de l'origine raciale ou ethnique ou portant sur des poursuites ou sanctions pénales et administratives (art. 3 let. c LPD, art. 5 let. c nLPD), pour lesquelles des obligations renforcées sont imposées par la loi[19].

Les études d'avocats sont d'ailleurs soumises au RGPD si elles tombent dans son champ d'application territorial. Ceci est vrai en particulier lorsque les activités de traitement remplissent le critère dit du ciblage (art. 3 al. 2 RGPD), soit (i) lorsqu'elles offrent des biens ou des services à des personnes situées dans l'Union Européenne (UE), qu'un paiement soit exigé ou non ou (ii) lorsqu'elles effectuent un suivi du comportement de personnes situées dans l'UE (i. e. clientèle visée, site internet)[20]. Dans cette hypothèse, les études concernées seraient d'ores et déjà soumises à l'obligation de protection des données dès la conception selon le droit européen (art. 25 RGPD)[21].

B) Qu'en est-il des sous-traitants et des prestataires?

L'art. 7 nLPD ne prévoit aucune obligation à charge des sous-traitants tels que les développeurs de logiciels ou les prestataires *clouds.* Le message du Conseil fédéral est également silencieux à ce sujet. Le responsable du traitement devra dès lors s'assurer du respect des exigences en matière de sous-traitance (art. 9 nLPD; actuellement l'art. 10*a* LPD) et assumera une responsabilité notamment dans le choix du sous-traitant, qui devra respecter à son tour l'obligation de protection des données dès la conception[22]. Cette approche s'aligne sur le droit européen[23]. Dans son choix, le responsable du traitement pourra par exemple s'appuyer sur des normes de certification reconnues, telle que la norme ISO 27701[24].

3. Portée de l'obligation

A) Principes généraux

La protection des données dès la conception vise à garantir que le traitement «respecte les prescriptions de protection des données et en particulier les principes fixés à l'art. 6» (art. 7 al. 1 nLPD).

L'article 6 nLPD énumère les principes généraux suivants:

- la licéité du traitement (i. e. justifié par la loi, un intérêt prépondérant ou un consentement, art. 31 nLPD);
- la bonne foi et la proportionnalité;
- la finalité et la reconnaissabilité du traitement;
- la durée de conservation des données personnelles;
- l'exactitude; et
- s'il est requis, un consentement valable (i. e. libre et éclairé, exprès quand nécessaire)[25].

La révision de la LPD, qui vise à renforcer la protection conférée aux personnes concernées et à s'aligner sur le droit européen[26], ne change pas l'essence des principes applicables. À titre d'exemple, la limitation de la durée de conservation des données, qui figure explicitement à l'art. 6 al. 4 nLPD, découle actuellement du principe de proportionnalité (art. 4 al. 2 LPD)[27].

Outres les principes généraux de l'art. 6 al. 1 nLPD, d'autres prescriptions telles que la sécurité des données (art. 8 nLPD) ou le devoir d'information (art. 19 nLPD) doivent également être intégrées dès la conception du traitement[28].

La modification majeure apportée par la protection des données dès la conception porte sur l'intégration de tous ces principes dans les systèmes d'une entreprise avant même de traiter les données.

B) En pratique

Quelques exemples permettront d'éclaircir plus concrètement l'obligation de protection des données dès la conception:

- outils informatiques et *clouds*[29]: pour se conformer à la protection des données dès la conception (et par ailleurs au secret professionnel de l'avocat qui serait mis en péril par un transfert à l'étranger[30]), le responsable du traitement doit contrôler dès le départ le(s) pays d'hébergement des serveurs utilisés pour traiter les données personnelles de clients[31] (y compris pour les sauvegardes) et s'assurer que les *data centers* soient (en principe) situés en Suisse et qu'ils offrent un niveau de sécurité élevé. L'hébergement en Suisse des données de clients n'est pas suffisant. Les études doivent encore vérifier l'impact

19 Voir art. 4 al. 5 LPD, art. 7 LPD ou art. 11*a* al. 3 let. a LPD; art. 6 al. 6 nLPD et art. 8 nLPD.
20 Voir Lignes directrices du CEPD; AMIGUET A./FISCHER P., Changement de paradigme en matière de protection des données, in: Revue de l'avocat 1/2018, p. 28 ss.
21 Voir Lignes directrices du CEPD.
22 Voir Arrêt du Tribunal fédéral 2C_1083/2017 du 4. 6. 2019, consid. 7.2; Message du 15. 9. 2017, 6651.
23 Voir Lignes directrices CEPD, p. 10; Considérant 78 du RGPD.
24 Voir la publication de la Commission Nationale Informatique & Libertés (CNIL) sur la norme ISO 27701: https://www.cnil.fr/fr/liso-27701-une-norme-internationale-pour-la-protection-des-donnees-personnelles (dernière consultation le 19. 9. 2020).
25 Message du 15. 9. 2017, p. 6647.
26 Pour des informations sur les modifications apportées par la révision, voir AMIGUET A./FISCHER P.
27 Message du 15. 9. 2017, p. 6645; ROSENTHAL D./JÖHRI Y., Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, 2008, n. 24 p. 85.
28 La formulation de l'art. 7 al. 1 nLPD n'est pas exhaustive. Cette interprétation est par ailleurs alignée au droit européen, voir Art. 25 §1 RGPD; Lignes directrices du CEPD, p. 6.
29 Voir Arrêt du TF 2C_1083/2017; CHAPPUIS B./ALBERINI A., Secret professionnel de l'avocat et solutions *cloud,* in: Revue de l'avocat 11/12/2019, p. 473 ss; BENHAMOU Y./ERARD F./KRAUS D., L'avocat a-t-il aussi le droit d'être dans les nuages?, in: Revue de l'avocat 3/2019, p. 119 ss.
30 CHAPPUIS B./ALBERINI A., p. 341.
31 Sur le principe même, des données personnelles peuvent être transférées à l'étranger si le pays concerné dispose notamment d'une législation assurant un niveau de protection adéquat (voir art. 6 LPD; art. 16 nLPD). Toutefois, pour les avocats, le secret professionnel impose une contrainte supplémentaire et les *data centers* devraient dès lors être localisés en Suisse.

de l'application de législations étrangères aux traitements effectués, en particulier pour les *clouds* si le prestataire fait partie d'un groupe américain, ainsi que les possibilités de transferts indus de données à l'étranger[32];
- sécurité des communications: correspondre avec un client qui utilise une messagerie de type «Gmail» (Google) n'est pas propre à assurer la sécurité des données. L'avocat devrait sensibiliser le client et lui présenter une alternative si nécessaire[33]. De son côté, l'avocat devrait prévoir d'utiliser une messagerie ou une plateforme sécurisée avec un chiffrement des données;
- site internet: conformément aux développements précédents, seules les informations nécessaires au regard de la finalité poursuivie peuvent être collectées. Si la finalité d'un formulaire de contact est une première communication, la collecte par ce biais des dates de naissance des internautes sera excessive. Le formulaire de contact devrait être préalablement sécurisé, par exemple par une mesure de chiffrement. Dans ce cadre, les études doivent analyser les outils utilisés par les développeurs de sites internet, certains pouvant collecter et transférer des données personnelles à un tiers (à l'étranger)[34];
- gestion de l'accès aux données: il appartient aux études de prévoir un système de limitation des accès aux données utiles[35]. À titre d'exemple, la personne en charge de la facturation doit accéder aux factures, mais non à l'intégralité des dossiers des clients. Le Préposé recommande, par exemple dans le cadre de l'activité d'employés, de restreindre leur accès aux données utiles pour diminuer les risques et prévenir les abus[36];
- accès à distance: pour être conforme, un accès à distance devrait être préalablement sécurisé, par exemple avec un VPN *(virtual private network)* ou par l'utilisation d'un *cloud* sécurisé;
- durée de conservation des données: la durée de conservation des données doit être préalablement définie au cas par cas, en fonction du type de donnée et de l'objectif de la collecte (voir art. 6 al. 4 nLPD). Un système efficace de suppression une fois le délai dépassé devra ainsi être implémenté. Le délai variera généralement en fonction des délais de prescription et des obligations légales des avocats en matière de conservation;
- archivage intermédiaire électronique: les données qui ne sont plus utilisées, mais qui doivent encore pouvoir être consultées de manière ponctuelle (par exemple un dossier clos qui doit être conservé durant minimum dix ans) devraient être séparées des données actives, de sorte que leur accès soit restreint (voir ci-dessus gestion des accès);
- information aux personnes concernées: les informations devront être aisément accessibles, complètes et compréhensibles[37];
- procédure en cas d'accès indu *(data breach):* afin de garantir que les droits des personnes concernées soient respectés en cas d'accès indu à leurs données, il appartient au responsable du traitement de prévoir une directive interne fixant la marche à suivre.

Les cas d'application ci-dessus sont présentés à titre exemplatif. Comme développé ci-avant, une analyse doit être effectuée au cas par cas et les particularités liées à la profession, tel que le secret de l'avocat, doivent inévitablement être prises en compte.

4. Délai de mise en conformité

Aucun délai transitoire n'est prévu, étant précisé que l'obligation de protection dès la conception ne s'appliquera pas rétroactivement aux traitements de données effectués avant l'entrée en vigueur de la nLPD, pour autant que les finalités du traitements restent inchangées et que de nouvelles données ne soient pas collectées[38].

Dès lors que les études d'avocats traitent continuellement de nouvelles données personnelles et que les finalités de traitement sont susceptibles d'évoluer, ces exceptions auront une portée restreinte pour les études.

Par ailleurs, les études ne devraient pas négliger l'analyse des traitements de données ayant débutés avant l'entrée en vigueur de la nLPD, dans la mesure où ces traitements doivent se conformer aux dispositions du droit en vigueur. À titre d'exemple, les études doivent déjà limiter l'accès aux données et déterminer leur durée de conservation[39].

5. Conséquences en cas de violation

La sanction pénale initialement prévue par la nLPD en cas de violation du devoir de protection des données dès la conception a été abandonnée. Celle-ci faisait écho aux règles européennes en la matière et prévoyait une sanction allant (sur plainte) jusqu'à CHF 500 000.– en cas d'acte intentionnel ou jusqu'à CHF 250 000.– pour un acte négligent. Si l'amende n'a pas été retenue dans la nLPD, pour les études d'avocats soumises au RGPD, la sanction est une amende administrative pouvant s'élever jusqu'à EUR 10 000 000 ou pour les entreprises jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précé-

32 Voir le Clarifying Lawful Overseas Use of Data Act du 23. 3. 2018; Foreign Intelligence Surveillance Act (FISA) Section 702 (modification de 2008); Arrêt de la Cour de justice de l'Union européenne (CJUE) C-311/18 du 16. 7. 2020 invalidant le Privacy Shield entre les États-Unis et l'Union Européenne (affaire Schrems II); Prise de position du PFPDT du 8. 9. 2020 qui a retiré les États-Unis de la liste d'adéquation de la Suisse.

33 Par exemple la messagerie sécurisée ProtonMail: https://www.arobase.org/messageries/protonmail.html;

34 Voir le rapport de la CNIL sur l'application «StopCovid» française du 20. 7. 2020 et la demande de la supression de l'outil «re-captcha Google», un système automatisé permettant de vérifier que l'application est utilisée par une personne physique, qui collectait et transférait des données personnelles (i. e. adresses IP) à Google; aussi pour les *cookies* (témoins de connection).

35 Pour plus d'informations voir BYDZOVSKY P., Gestion des accès internes aux dossiers des clients et protection des données, in: Revue de l'avocat 8/2017, p. 473 ss.

36 Guide du Préposé, p. 11.

37 Message du 15. 9. 2017, p. 6668.

38 Voir l'art. 69 nLPD.

39 Pour plus d'informations, voir BYDZOVSKY P.

dent, le montant le plus élevé étant retenu (art. 83 ch. 4 RGPD).

Bien que la violation du principe de protection des données dès la conception ne soit pas elle-même sanctionnée, des sanctions pénales sont prévues sous forme d'amende de CHF 250 000.– si le responsable du traitement viole intentionnellement son devoir d'informer la personne concernée, ou faillit à son devoir de diligence en violant par exemple des dispositions en matière de transfert à l'étranger, de sécurité des données ou de sous-traitance (art. 60 et 61 nLPD). La personne concernée pourrait également agir civilement à l'encontre du responsable du traitement en invoquant notamment une atteinte à sa personnalité (art. 28, 28*a* et 28l CC[40]).

Les pouvoirs du Préposé seront renforcés (art. 49 ss nLPD). Ce dernier pourra ouvrir une enquête à l'encontre du responsable du traitement. Il pourra notamment ordonner la suspension, la modification ou la cession de tout ou partie du traitement et imposer de prendre des mesures pour informer les personnes concernées. Le non-respect d'une décision du Préposé peut entraîner une amende pouvant s'élever à CHF 250 000.– (art. 60 al. 2 nLPD).

Enfin, dans la mesure où la nLPD prévoit des annonces tant au Préposé qu'aux personnes concernées, en particulier lorsque la sécurité des données est compromise (art. 24 nLPD), le non-respect des règles applicables pourrait ainsi nuire à la réputation des études.

III. Conclusion

Avec l'introduction du principe de protection des données dès la conception, le responsable du traitement veillera à se conformer aux prescriptions de la nLPD et à les intégrer en amont de tout traitement. Si les obligations générales du responsable du traitement ne changent pas dans leur essence, la protection des droits des personnes concernées est néanmoins renforcée. Les études d'avocats ne sauraient faire l'impasse sur cette obligation et devront faire preuve de diligence pour y satisfaire.

L'obligation est vaste et concerne tous les traitements de données personnelles. Elle requiert notamment d'inventorier tous les traitements de données et de déterminer les risques liés aux traitements concernés. Dans ce cadre, les études d'avocat devront tant revoir leurs processus et organisation interne, que choisir des solutions techniques adéquates pour assurer que les données personnelles soient traitées conformément au droit de la protection des données du début à la fin du traitement. En matière de traitements informatisés, les études doivent déterminer au cas par cas si les outils utilisés ou contemplés sont conformes à ce principe.

La nLPD ne prévoyant pas de délai transitoire, les études ne doivent pas trop tarder à faire un état des lieux afin de déterminer les mesures appropriées et efficaces à implémenter. Certaines études y sont par ailleurs déjà soumises par le biais de l'application du RGPD. Ces démarches ne doivent pas être sous-estimées, tant sur le plan technique que juridique. Elles nécessitent du temps et des ressources humaines et financières, l'un des défis principaux étant certainement de maîtriser les coûts.

40 Code civil suisse du 10.12.1907, RS.210; voir également l'art. 30 nLPD.