www.jusletter.ch

François Charlet

Le Data Protection Officer dans le secteur privé suisse

Avec l'application du Règlement général sur la protection des données dans l'Union européenne depuis le 25 mai 2018 et la révision totale de la loi fédérale sur la protection des données, le domaine de la protection des données va changer, se complexifier. Le droit recommande ou exige des acteurs privés l'engagement de professionnels compétents pour les conseiller et surveiller leurs activités. Les différences entre le droit suisse actuel et futur et le droit européen ne sont cependant pas aussi importantes qu'on pourrait le croire. Pourtant, un gommage des différences serait souhaitable.

Catégories d'articles : Contributions
Domaines juridiques : Protection des données

Proposition de citation : François Charlet, Le Data Protection Officer dans le secteur privé suisse, in : Jusletter 18 juin 2018

ISSN 1424-7410, https ://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Table des matières

I. Introduction
II. Le conseiller dans la LPD actuelle
A. Bases légales applicables
B. Raison d'être du conseiller : l'autorégulation
C. Désignation
D. Statut
E. Connaissances professionnelles
F. Missions
1) Contrôler les traitements
2) Proposer des mesures
3) Inventorier les traitements
4) Autres tâches
G. Excursus : le conseiller d'un organe fédéral
III. Dans le projet de LPD révisée
IV. Dans le RGPD
A. Introduction
B. Bases légales applicables
C. Raison d'être du délégué : garant de la conformité
D. Désignation
1) Obligatoire
a. Activités de base d'un responsable de traitement
b. En cas de traitement à grande échelle de catégories particulières de données ou de données personnelles relatives à des condamnations pénales et à des infractions
c. En cas de suivi régulier et systématique à grande échelle
2) Facultative
3) Formalités de désignation
E. Fonction et statut
F. Connaissances professionnelles
G. Missions
1) Informer et conseiller
2) Contrôler
3) Vérifier l'exécution des analyses d'impact
4) Coopérer avec l'autorité de contrôle
H. Excursus : le délégué d'une autorité suisse
V. Conclusion

I. Introduction

[Rz 1] *Dans la présente contribution, toutes les dénominations de personnes ou de fonctions dont le genre grammatical est masculin désignent indifféremment des personnes de sexe masculin ou féminin.*

[Rz 2] La loi fédérale sur la protection des données (LPD) actuellement en vigueur, le projet de LPD révisée et le Règlement général sur la protection des données (RGPD) mentionnent tous la possibilité, voire l'obligation, pour les responsables de traitement, privés ou publics, de désigner un conseiller ou un délégué à la protection des données (en anglais : data protection officer, ou DPO). Le durcissement des conditions pour traiter des données personnelles va sans doute rendre indispensable cette fonction, en particulier auprès des acteurs qui traitent de grandes quantités de données personnelles ou qui ont des activités commerciales à l'étranger. Généralement interconnectées, les données personnelles représentent une richesse dont il faut prendre soin, en particulier lorsqu'elles sont au cœur d'une stratégie, d'un modèle d'affaires ou simplement de

processus – les données clients, par exemple. Ainsi, lorsqu'elle n'est pas imposée par la législation, la désignation d'un conseiller ou délégué à la protection des données représente parfois une contrainte, mais elle peut aussi être perçue comme un avantage commercial et concurrentiel : le responsable de traitement donne ainsi l'image d'être respectueux et digne de confiance. Elle peut aussi découler d'un besoin d'adopter une stratégie cohérente en matière de protection des données, de la reconnaissance des données comme un actif de la société ou de la nécessité d'avoir un représentant spécialisé pour diriger la réglementation interne.

[Rz 3] En outre, le développement des technologies de l'information, des modèles prédictifs, du machine learning, des moyens de transport autonomes, de l'e-santé amène des questions juridiques, technologiques, éthiques et assurantielles (gestion du risque) auxquelles un responsable de traitement sera un jour ou l'autre confronté et dont il devra se préoccuper en amont. La désignation d'un conseiller ou délégué à la protection des données permettra en principe de couvrir ces dimensions avec sérénité. Mais son rôle n'est pas seulement de s'assurer du respect des normes juridiques et techniques grâce à ses connaissances transversales : il lui incombera aussi de diffuser une culture de la protection des données, de sensibiliser ses collègues et supérieurs, de participer dès le début à la mise en place de projets impliquant un traitement de données personnelles. Le conseiller ou délégué à la protection des données doit donc devenir un acteur central d'une entreprise ou d'un organe public.

[Rz 4] La présente contribution étudiera la réglementation de la fonction de conseiller dans la LPD en vigueur et le projet de LPD révisée, et de la fonction de délégué dans le RGPD. Nous détaillerons notamment les différents scénarios de désignation d'un conseiller ou délégué, leurs fonctions, missions, statuts, et qualifications, tant du point de vue légal que pratique.

[Rz 5] *NB. La législation suisse utilise le terme « conseiller à la protection des données » (ci-après : conseiller) alors que la réglementation européenne le nomme « délégué à la protection des données » (ci-après : délégué). Bien que synonymes, nous respecterons cette terminologie pour distinguer les « conseillers suisses » des « délégués européens ». Par ailleurs, afin de faciliter la lecture et la compréhension de cette contribution, nous utiliserons exclusivement la terminologie modernisée proposée par le RGPD et le projet de LPD révisée. Ainsi, le terme « fichier » de l'actuelle LPD est remplacé par « traitement », et « maitre de fichier » par « responsable de traitement ».*

II. Le conseiller dans la LPD actuelle

A. Bases légales applicables

[Rz 6] La loi fédérale sur la protection des données du 18 juin 1992 (ci-après : LPD) mentionne à deux reprises l'existence du conseiller à la protection des données. L'article 11a alinéa 5 lettre e LPD dispose ainsi que « [le responsable de traitement] n'est pas tenu de déclarer son [traitement] s'il a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des [traitements] ». Plus bas, l'alinéa 6 délègue au Conseil fédéral la compétence de « préciser le rôle et les tâches des conseillers à la protection des données », ce qu'il a fait aux art. 12a et 12b de l'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (ci-après : OLPD). Nous y reviendrons plus en détail ci-dessous.

B. Raison d'être du conseiller : l'autorégulation

[Rz 7] Lors de son adoption, la LPD ne contenait aucune référence à la fonction de conseiller. Ce n'est qu'en 2008 qu'est entrée en vigueur une modification de la LPD qui a notamment ajouté l'art. 11a. Les travaux préparatoires[1] indiquent que « l'art. 11a al. 5 let. e LPD vise à encourager l'autoréglementation. [Le responsable de traitement] peut désigner un conseiller à la protection des données qui est chargé de tenir un inventaire des [traitements] et de surveiller que du point de vue interne les conditions-cadres de la protection des données sont respectées ». Cette volonté est répétée plus bas.[2] «Une grande autonomie sera laissée aux acteurs économiques qui pourront s'assurer d'un niveau de protection adéquat des données [...]. Des avantages seront également accordés aux entreprises qui pratiquent l'autocontrôle (conseiller interne, certifications)». Cette possibilité d'autorégulation se distingue des al. 2 et 3 de l'art. 11a LPD qui imposent aux responsables de traitement publics (organes fédéraux) et privés de déclarer leurs traitements de données personnelles au Préposé fédéral à la protection des données et à la transparence (ci-après : préposé) en cas de traitement régulier de données sensibles ou de communications régulières de données personnelles à des tiers.

C. Désignation

[Rz 8] La désignation d'un conseiller n'est pas du tout obligatoire dans le secteur privé, mais peut s'avérer intéressante, en particulier en fonction du type et de la quantité de données personnelles traitées, ainsi que de la taille de l'entreprise.

[Rz 9] Si le responsable de traitement souhaite être délié du devoir de déclaration des traitements décrit à l'art. 11a al. 2 et 3 LPD, il doit désigner un conseiller répondant à certaines conditions, notamment quant à son statut, ses connaissances professionnelles et ses tâches (cf. *infra* n^{os} II.D, II.E, II.F).[3] La désignation d'un service interne ou d'une personne chargée de répondre aux questions de protection des données ne constitue pas une désignation d'un conseiller, à moins de respecter les exigences posées aux art. 12a et 12b OLPD.[4]

[Rz 10] Le responsable de traitement est libre de désigner une personne à l'interne, comme un collaborateur soumis à un contrat de travail, ou un tiers par le biais d'un contrat de service.[5] Ce choix n'influence en rien les tâches du conseiller vis-à-vis du responsable de traitement, mais l'indépendance doit être garantie. Comme l'indique le préposé, la désignation de coordinateurs à la protection des données aux niveaux hiérarchiques inférieurs peut s'avérer utile, ces coordinateurs étant chargés d'assurer une communication efficace entre le conseiller et les départements

1 Message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données du 19 février 2003, FF 2003 1915, p. 1949.

2 Message, FF 2003 1915 (n° 1), p. 1961.

3 Art. 12a al. 1 let. a Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD ; RS 235.11).

4 Philippe Meier, Protection des données, Fondements, principes généraux et droit privé, Berne 2010, n° 1449.

5 Art. 12a al. 2 1^{e} phrase OLPD.

ou services.[6] Une telle organisation pyramidale de la fonction dépendra forcément de la taille de l'entreprise.

[Rz 11] Le choix d'une désignation d'un collaborateur interne ou d'un prestataire externe reposera sur plusieurs critères. S'il semble plus facile d'éviter des conflits d'intérêts et de garantir l'indépendance du conseiller en externalisant la fonction, le responsable de traitement devra prendre en compte différents critères comme sa taille, son organisation interne, la complexité de sa structure et le budget à allouer au conseiller. Il apparait qu'une grande structure, complexe, aura besoin d'un conseiller interne à plein temps et qui connaisse l'organisation du responsable de traitement. Rien n'exclut cependant de désigner à la fois un conseiller interne et un mandataire[7] de façon à mutualiser la fonction, ce qui permettrait d'avoir un regard différencié sur les problématiques à résoudre. Le choix doit *in fine* répondre aux besoins du responsable de traitement. Il est important de noter qu'en termes de gestion des risques, la sous-traitance des tâches de conseiller ne permet pas de partager le risque avec le sous-traitant, comme nous le verrons ci-dessous concernant la responsabilité du conseiller. Quoi qu'il en soit, les règles exposées ci-après s'appliqueront au conseiller, qu'il soit interne ou externe.

[Rz 12] Ni la LPD ni l'OLPD ne prévoient de formalités quant à la désignation du conseiller, si ce n'est d'informer le préposé de cette désignation.[8] Comme le conseiller est une fonction transverse à toute l'entreprise, il se justifie d'informer l'ensemble des collaborateurs, voire des fournisseurs, clients et prestataires, de la désignation du conseiller. Sa désignation devrait être avalisée ou confirmée par la direction générale ou le comité, à tout le moins par un organe de gouvernance. Le contrat de travail du conseiller interne devra mentionner les règles quant à son statut, en particulier son indépendance. Si un collaborateur interne est désigné avec un prestataire externe, ou si plusieurs prestataires externes sont désignés, il conviendra d'attribuer à l'un d'eux la charge d'être le point de contact unique vis-à-vis du responsable de traitement et des tiers. Idéalement, les coordonnées (génériques) du conseiller devraient être publiées et accessibles à tout un chacun.

D. Statut

[Rz 13] Le conseiller n'est pas nécessairement une personne physique, mais peut être un groupement de plusieurs personnes (par exemple un juriste spécialisé en protection des données et un spécialiste de la sécurité informatique). Le terme « conseiller à la protection des données » se réfère donc à une fonction.

[Rz 14] Le conseiller doit être **indépendant**, qu'il soit désigné parmi les collaborateurs du responsable de traitement ou mandaté en tant que tiers externe. Cette exigence est explicitement mentionnée à l'art. 11a al. 5 let. e LPD. Le Message du Conseil fédéral concernant cette disposition[9] ne mentionne que l'indépendance organisationnelle ; l'OLPD ne donne pas plus d'informations à cet égard.

---

6 « Les conseillers à la protection des données en entreprise », fiche d'information disponible sur le site web du préposé www.edoeb.admin.ch, consultée en mars 2018 (ci-après : Fiche d'information du préposé sur les conseillers).

7 Par ex. un cabinet d'avocats, une société de service spécialisée, un indépendant.

8 Art. 12 al. 1 let. b OLPD.

9 Message, FF 2003 1915 (n° 1), p. 1949.

[Rz 15] L'indépendance organisationnelle revient d'abord à interdire au conseiller d'exercer des activités incompatibles avec sa fonction (art. 12a al. 2 2e phrase OLPD). Autrement dit, il doit **éviter les conflits d'intérêts**. S'il ne fait pas partie de l'entreprise, un conflit d'intérêts ne saurait surgir du simple fait qu'il assume la même fonction pour d'autres entreprises, pour autant que des garanties de confidentialité aient été prévues et soient appliquées. Si le conseiller est désigné parmi les collaborateurs de l'entreprise, le préposé indique que le poste ne doit pas être intégré dans la hiérarchie directe. En outre, il serait inacceptable que le conseiller désigné à l'interne soit également le responsable de l'informatique, le responsable des ressources humaines, le responsable financier, le directeur général ou un membre du conseil d'administration. Le conseiller ne peut pas non plus occuper un poste hiérarchiquement inférieur s'il participe à des tâches décisionnelles concernant des traitements de données. Cela ne signifie pas, cependant, que le conseiller ne puisse pas être organiquement rattaché à une unité, comme le service informatique, juridique ou des ressources humaines, voire la direction.[10]

[Rz 16] Selon l'Office fédéral de la justice, il n'existe pas d'incompatibilité de principe pour le cumul des fonctions de conseiller et de responsable de la sécurité informatique ou de directeur du service juridique.[11] Nous sommes d'avis cependant que la charge de responsable de la sécurité informatique ou de directeur du service juridique ne peut être cumulée avec celle de conseiller. En effet, le conseiller pourrait, par exemple, devoir procéder à une analyse des risques et évaluer les mesures de sécurité qu'il aura lui-même recommandées ou prises en tant que responsable de la sécurité. Une situation semblable pourrait se présenter si le conseiller est également le directeur du service juridique.

[Rz 17] En tout état de cause, il nous apparait que la fonction de conseiller devrait être dédiée, et non cumulée avec une autre fonction. C'est à notre avis un moyen efficace de garantir son indépendance lorsqu'il est désigné parmi les collaborateurs d'un responsable de traitement.

[Rz 18] Dans l'exercice de ses fonctions, le conseiller **ne peut pas recevoir d'instructions** de la part du responsable de traitement (art. 12b al. 2 let. a OLPD), qu'il soit son employeur ou son mandant. Le responsable ne peut pas, par exemple, lui imposer une méthode de travail, d'analyse ou d'enquête particulière ni le contraindre à traiter une affaire dans un sens plutôt que dans un autre, lui fixer des résultats ou objectifs à atteindre ou lui interdire de consulter le préposé. Cependant, des instructions d'ordre organisationnel ne font pas obstacle à l'indépendance matérielle du conseiller s'il est désigné parmi les collaborateurs de l'entreprise.[12] Le conseiller ne peut être directement ou indirectement menacé de sanctions (avertissement, licenciement, refus de promotion, résiliation du mandat, etc.) ou de mesures de rétorsion en raison de l'accomplissement de ses tâches conformément à la législation. Le conseiller a le droit, si ce n'est le devoir, d'exprimer son opinion (dissidente) et ses inquiétudes auprès de la direction, d'émettre des recommandations et de donner des conseils. Pour le reste, le droit des contrats et le droit pénal restent applicables pour traiter des conséquences des actions qui ne sont pas inhérentes à la réalisation licite des tâches du conseiller.

[Rz 19] Le statut du conseiller ne suppose pas, à moins que cela ne soit explicitement prévu par le responsable de traitement, qu'il dispose du pouvoir de prendre des **décisions** dans le cadre

10 Fiche d'information du préposé sur les conseillers (n° 6).

11 Commentaire de l'Office fédéral de la justice à l'appui de l'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 [état au 1er janvier 2008], n° 7.1.1, p. 14 (ci-après : Commentaire OLPD).

12 Meier (n° 4), n° 1455.

de ses activités typiques. Bien que les traductions allemande (*Datenschutzverantwortliche*) et italienne (*responsabile della protezione dei dati*) laissent supposer une capacité décisionnelle, il faut s'en tenir à la terminologie française qui reflète mieux l'activité du conseiller telle que décrite dans l'OLPD.[13]

[Rz 20] Pour accomplir ses tâches, le conseiller doit bénéficier d'un **accès complet** à tous les traitements contenant des données personnelles et sensibles, ainsi qu'à tous les traitements (art. 12b al. 2 let. c OLPD). Cet accès doit lui être octroyé au minimum sur simple demande et dans les plus brefs délais. Il doit aussi avoir accès à toutes les informations dont il a besoin pour connaitre tous les traitements de données au sein de l'entreprise. Sont incluses parmi ces informations toutes les personnes qui détiennent des renseignements sur des traitements de données, y compris les sous-traitants et mandataires externes. Les secrets légaux ou contractuels ne font pas obstacle au droit d'accès du conseiller.

[Rz 21] Afin d'éviter que la fonction de conseiller ne soit une coquille vide ou un prétexte, elle doit disposer des **ressources nécessaires** (art. 12b al. 2 let. b OLPD), tant financières, temporelles et humaines. S'il est désigné à l'interne de l'entreprise, cette dernière peut lui octroyer son propre budget ou lui allouer des ressources lorsqu'il en fait la demande. Plus les traitements réalisés par l'entreprise sont importants ou complexes, ou si les données traitées sont composées de données sensibles, plus les ressources allouées au conseiller seront grandes. Ainsi, en fonction de la taille de l'entreprise par exemple, une équipe placée sous la responsabilité du conseiller sera tout indiquée.

[Rz 22] L'activité du conseiller se limite essentiellement à des tâches de surveillance et de conseil, de sorte qu'il n'est pas directement responsable du respect de la protection des données par son employeur ou mandant. Cette **responsabilité** incombe exclusivement au responsable de traitement,[14] même s'il suit les recommandations et directives du conseiller. Les responsabilités pénale et contractuelle (basée sur le contrat de travail ou le contrat de mandat) sont réservées. Evidemment, si le conseiller fait preuve de légèreté ou de négligence vis-à-vis des situations non conformes dont il a connaissance, sa responsabilité pourra être engagée. Celle-ci sera analysée à l'aune des ressources mises à sa disposition dans le cas d'espèce.

E. Connaissances professionnelles

[Rz 23] L'ordonnance fédérale exige que le conseiller possède les « connaissances professionnelles nécessaires » à l'exercice de sa fonction (art. 12a al. 2 in fine OLPD). Ces connaissances regroupent au moins les notions juridiques, techniques et spécifiques au responsable de traitement. Les connaissances et qualifications du conseiller devraient être proportionnelles à la com-

13 Commentaire OLPD (n° 11), n° 7.1.1, p. 13. A noter que le Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données indique que pour éviter toute confusion avec le terme « Verantwortliche », respectivement avec le mot « responsabile », le projet de LPD révisée adoptera en allemand et en italien les notions de « Datenschutzberater » respectivement « consulente per la protezione dei dati », uniformisant ainsi la terminologie dans les trois langues (Message 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 septembre 2017, FF 2017 6565, p. 6652).

14 Pour le responsable de traitement privé, cf. notamment art. 55 du Code des obligations du 30 mars 1911 (RS 220) ; pour les organes fédéraux, cf. notamment art. 16 de la loi fédérale sur la protection des données du 19 juin (LPD, RS 235.1), art. 3 et 8 de la loi fédérale sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires du 14 mars 1958 (RS 170.32).

plexité des traitements de données, à la quantité de données sensibles traitées et au niveau de sécurité exigé.

[Rz 24] Les **connaissances juridiques** se rapportent à la LPD et à l'OLPD, ainsi qu'à la législation spéciale applicable dans le domaine d'activité du responsable de traitement.[15] Le conseiller devra être en mesure de comprendre et d'appliquer ces normes et leurs principes, ainsi que de déterminer si et quand un traitement de données porte atteinte ou est susceptible de porter atteinte aux droits des personnes concernées par un traitement de données personnelles. Le préposé recommande le suivi d'une formation de six mois ou une expérience professionnelle de la même durée dans le domaine de la protection des données pour le conseiller ne bénéficiant pas d'une formation juridique.[16] Une formation certifiée comme le CIPP/E constitue une base solide.

[Rz 25] Le conseiller doit également posséder des **connaissances techniques**, c'est-à-dire avoir une bonne compréhension des opérations effectuées sur les données personnelles ou sensibles, des systèmes informatiques utilisés par le responsable de traitement et des mesures de sécurité prises et à prendre. L'obtention – préalable ou subséquente à la désignation – de certifications reconnues est recommandée (ISO 29100, ISO 27001 par exemple), en particulier pour les conseillers non-juristes.

[Rz 26] Quant aux **connaissances spécifiques**, elles se rapportent à l'organisation du responsable de traitement, aux types d'activités déployées par ce dernier, aux exigences du secteur économique dans lequel il évolue et, dans le cas d'un organe fédéral, aux règles administratives et aux procédures. Il s'agit ici pour le conseiller de comprendre comment la protection des données doit être implémentée chez ce responsable de traitement afin qu'elle s'intègre au mieux dans l'activité commerciale ou administrative de celui-ci.

[Rz 27] Au niveau des « **soft skills** », le conseiller doit faire preuve d'intégrité et d'une grande éthique professionnelle. Il est souhaitable qu'il soit capable de communiquer avec les autorités, de s'adresser aux personnes concernées par un traitement de données, de gérer leurs plaintes et leurs requêtes (par ex. le droit d'accès). Il doit en outre être capable de s'évaluer et de compléter les lacunes qui apparaissent au fil du temps dans ses connaissances en raison notamment de l'évolution de la technique et de la loi. Il devra également parvenir à promouvoir la protection des données auprès des collaborateurs du responsable de traitement.

F. Missions

[Rz 28] L'art. 12b al. 1 OLPD fournit une liste exemplative des tâches du conseiller. Selon cette disposition, il doit notamment contrôler les traitements de données personnelles et proposer des mesures s'il apparait que des prescriptions sur la protection des données ont été violées (let. a), et dresser l'inventaire des traitements effectués par le responsable de traitement mentionné à l'art. 11a al. 3 LPD et le tenir à la disposition du préposé ou des personnes concernées qui en font la demande (let. b). Les tâches du conseiller ne se limitent cependant pas seulement à ces activités et méritent d'être complétées et détaillées.

---

15 Par ex. art. 28 ss du Code civil suisse du 10 décembre 1907 (RS 210) ; art. 3 et 39b de la Loi fédérale sur le contrat d'assurance du 2 avril 1908 (RS 221.229.1) ; art. 328b du CO ; art. 56 ss de la Loi fédérale relative à la recherche sur l'être humain du 30 septembre 2011 (RS 810.30) ; art. 107a et 107b de la Loi fédérale sur l'aviation du 21 décembre 1948 (RS 748.0).

16 Fiche d'information du préposé sur les conseillers (n° 6).

1) Contrôler les traitements

[Rz 29] Corolaire de ses prérogatives quant à l'accès à tous les traitements de données personnelles, le conseiller procède à la surveillance et au contrôle de l'exécution régulière desdits traitements, tant du point de vue technique que juridique. Il lui revient donc de se renseigner sur les traitements, de les identifier et de collecter des informations sur la manière dont les traitements sont exécutés. Pour y parvenir, le conseiller devra entretenir des relations étroites avec les différents départements et services du responsable de traitement (par ex. RH, IT) et être avisé de tout changement relatif à un traitement. Il devra conserver et entretenir la documentation idoine, la trace des recommandations qu'il émet, les informations qui lui sont transmises par les collaborateurs du responsable de traitement, etc.

[Rz 30] Le contrôle des traitements s'étend évidemment à la vérification de l'implémentation, de l'application et du respect de la loi, ainsi que des mesures, procédures et règlements adoptés par le responsable de traitement en matière de protection des données. Le conseiller attachera une importance particulière à vérifier que seules les personnes autorisées accèdent aux données personnelles,[17] que les traitements respectent les finalités annoncées,[18] qu'ils sont proportionnés auxdites finalités,[19] que les données ne sont pas conservées au-delà du délai légal ou déterminé par les circonstances et besoins des traitements, etc. Ces vérifications se feront par la comparaison de la situation de fait avec celle annoncée et enregistrée dans l'inventaire des traitements (cf. *infra* II.F.3).

2) Proposer des mesures

[Rz 31] L'art. 12 al. 1 let. a OLPD précise que le conseiller a pour tâche de proposer des mesures s'il apparait que des prescriptions sur la protection des données ont été violées. La lettre de cette disposition n'est pas opportune, car le conseiller doit pouvoir proposer des mesures même sans qu'aucune violation n'ait été signalée. Par exemple, les collaborateurs du responsable de traitement devraient consulter le conseiller à chaque fois qu'un projet touche la protection des données afin qu'il puisse donner son avis,[20] en particulier si un nouveau traitement de données ou une modification importante d'un traitement actuel sont envisagés.

[Rz 32] La compétence de proposer des mesures est en lien avec la fonction même du conseiller : n'ayant en principe pas un pouvoir décisionnel, la compétence principale du conseiller réside dans sa capacité à analyser une situation et à dresser un éventail de propositions à la direction afin que celle-ci décide quelle mesure devra être adoptée. Le conseiller a néanmoins la compétence d'édicter des instructions à l'attention du responsable de traitement.

[Rz 33] Le terme « mesures » doit être ici compris dans un sens large. Il comprend non seulement les mesures techniques et organisationnelles mentionnées aux art. 8 à 12 OLPD, mais aussi n'importe quel autre moyen licite nécessaire à l'accomplissement des tâches du conseiller et permettant d'assurer la protection des données.

---

17 Art. 9 al. 1 let. g OLPD.

18 Art. 4 al. 3 LPD.

19 Art. 4 al. 2 LPD.

20 Commentaire OLPD (n° 11), n° 7.1.2, p. 15.

[Rz 34] Il faut relever encore que si les mesures proposées par le conseiller ne sont pas suivies, ce dernier ne peut pas en appeler à une autorité supérieure pour contraindre le responsable de traitement. Tout au plus pourra-t-il demander conseil au préposé conformément à l'art. 28 LPD, voire s'adresser à l'autorité de surveillance particulière du domaine d'activité du responsable de traitement (par ex. la Finma pour une banque), ou à une organisation faitière.

3) Inventorier les traitements

[Rz 35] Le conseiller doit encore dresser l'inventaire des traitements effectués par le responsable de traitement et le tenir à la disposition du préposé ou des personnes concernées qui en font la demande (art. 12b al. 1 let. b OLPD). Cela permet de garantir la transparence des traitements qui ne sont plus soumis à déclaration.[21] Il faut cependant préciser que seuls les traitements mentionnés à l'art. 11a al. 3 LPD doivent figurer dans cet inventaire, c'est-à-dire ceux relatifs à des données sensibles ou à des profils de la personnalité, et ceux impliquant des communications régulières de données personnelles à des tiers. A notre avis, il convient d'aller au-delà de l'exigence minimale de l'OLPD et de réaliser un inventaire exhaustif, de manière à pouvoir procéder à une analyse fine des risques relatifs aux traitements.

[Rz 36] Avant de procéder à l'inventaire des traitements, il convient d'identifier ces derniers. Cela peut se faire de différentes manières, mais nous nous limiterons à en détailler une qui permet d'inventorier des traitements existants et mis en œuvre au moyen d'outils informatiques déjà mis en place. Cette méthode se déroule en deux temps. Tout d'abord, il faut établir une liste des logiciels et systèmes informatiques utilisés, puis une fiche d'identification de chacun d'eux (nom, fonctionnalités, données traitées, liste des personnes ou services qui l'utilisent, etc.).[22] Ensuite, il faudra établir une liste des processus métiers actifs chez le responsable de traitement et déterminer quelles sont les activités de traitements exercées par chaque service ou département, et grâce à quels logiciels et systèmes informatiques ces activités sont réalisées. Enfin, le recoupement de ces informations entre elles permettra au conseiller d'avoir un inventaire des traitements complet, incluant les activités de traitement informatisées ou non.

[Rz 37] Hormis l'art. 11a al. 3 LPD, ni la loi, ni l'ordonnance ne donnent de précisions sur le contenu de cet inventaire et sur les indications à fournir relativement aux traitements. Il convient néanmoins de se référer à la liste d'informations à transmettre en cas de demande d'accès au sens de l'art. 8 LPD.[23] Il est également possible de s'inspirer des dispositions sur le registre des traitements que doit tenir le préposé (art. 11a LPD ; art. 3, 16 et 28 OLPD).[24]

---

21 Commentaire OLPD (n° 11), n° 7.1.2, p. 15.

22 Les outils informatiques mis à disposition du responsable de traitement par un partenaire contractuel (par exemple un SaaS ou un service cloud) doivent évidemment faire partie de cette liste. Il en va de même des bases de données et fichiers créés et utilisés de manière locale par les collaborateurs (tableurs, traitement de texte, etc.) grâce à des outils standards de bureautique.

23 A cet égard, rappelons que le responsable de traitement devra fournir à la personne qui en fait la demande les informations suivantes : l'origine des données, le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, les catégories de participants au traitement et les catégories de destinataires des données.

24 L'art. 3 al. 1 OLPD indique que doivent être déclarés les nom et adresse du responsable de traitement, le nom et la dénomination complète du traitement, la personne auprès de laquelle peut être exercé le droit d'accès, le but du traitement, les catégories de données personnelles traitées, les catégories de destinataires des données, les catégories de participants au traitement, c'est-à-dire les tiers qui sont en droit d'introduire des données dans le traitement ou d'y procéder à des mutations. L'art. 16 al. 1 OLPD contient la même obligation à l'attention des organes fédéraux.

[Rz 38] Voici, à notre avis, le type d'informations que l'inventaire devrait contenir en présence de traitements moyennement complexes, mais incluant des données sensibles : base juridique du traitement, but du traitement, catégories de personnes concernées, catégories de données personnelles, source des données, catégories de destinataires, lien vers le contrat avec un sous-traitant (le cas échéant), localisation des données, noms des pays vers lesquels des données personnelles sont transférées et sur quelle base juridique ces transferts sont effectués (le cas échéant), durée de conservation, fondement légal ou contractuel de cette durée, existence d'un processus de décision automatisé (le cas échéant), nécessité d'une analyse d'impact et lien vers le résultat de l'analyse d'impact (le cas échéant), informations sur un incident de protection des données antérieur (le cas échéant).

[Rz 39] Concernant l'*origine des données*, nous aurons par exemple la personne concernée, un partenaire contractuel, un tiers, des registres publics, des déductions opérées par des analyses, etc. Le *but du traitement* sera celui qui est indiqué lors de la collecte de données, qui est prévu par une loi ou qui ressort des circonstances (art. 4 al. 3 LPD). Ainsi, la récolte de signature pour une initiative ou un référendum, un traitement à but marketing. Les *catégories de données* comprendront par exemple les informations suivantes : adresse postale, numéro AVS, lieu de travail, profession, revenu, famille, santé, nationalité, lieu d'origine, langue, assurance, nom, prénom, fournisseur de prestations, certificats médicaux, rapports médicaux, degré d'occupation, numéro de téléphone, date de naissance, etc. Quant aux *catégories de destinataires*, on y trouvera en particulier la personne concernée elle-même, les assurances, les fournisseurs de prestations médicales, les autorités, le service juridique du responsable de traitement, le service après-vente, les réassureurs, les communes, les offices des poursuites, les offices des faillites, les banques, l'administration cantonale des contributions, une protection juridique, un cabinet d'avocat, etc. Enfin, les collaborateurs du responsable de traitement, les représentants, les mandataires, les sociétés du groupe d'entreprises auquel le responsable de traitement appartient, des secteurs spécifiques du responsable de traitement, etc. sont des *catégories de participants* aux traitements.

[Rz 40] L'inventaire va donc lister tous les traitements de données personnelles mis en œuvre par le responsable de traitement et y inclure les informations énumérées *supra*. En fonction du nombre, de la complexité et de la sensibilité des traitements, cette tâche peut s'avérer titanesque. Il n'en demeure pas moins qu'elle doit être effectuée avec minutie, car cet inventaire sera la base même du travail du conseiller. Ce dernier devra ainsi passer au crible chaque département ou service du responsable de traitement pour obtenir les informations dont il a besoin.

[Rz 41] L'inventaire, qui doit être tenu sous une forme écrite, n'a pas à être réalisé dans un format particulier : il peut aussi bien être tenu au format électronique (par exemple sous la forme d'un tableur ou d'une base de données) qu'au format papier. Le choix de l'outil pour la réalisation de l'inventaire dépendra notamment de la quantité d'informations destinée à être introduite dans ledit inventaire.

4) Autres tâches

[Rz 42] L'OLPD est avare en détail sur les tâches du conseiller et ne liste expressément, à notre avis, que les activités que le conseiller doit impérativement déployer. La pratique permet de compléter le catalogue des tâches du conseiller. Ainsi, à titre d'illustration, nous pouvons sans autre ajouter les activités suivantes, qui peuvent être prévues contractuellement, aux tâches susmentionnées.

[Rz 43] Le conseiller s'assurera que l'approche adoptée par le responsable de traitement est uniforme et cohérente. Cela se fera en particulier par la mise en application d'un code de conduite, d'une **charte** ou d'une réglementation interne de hauts niveaux relatifs à la protection des données et qui a vocation à s'appliquer à tous les collaborateurs du responsable de traitement ou du sous-traitant. Le conseiller maintiendra à jour une **documentation** complète en matière de protection des données pour les collaborateurs et départements du responsable de traitements. Cette documentation contiendra non seulement des guides, instructions, explications, modèles, procédures, référentiels et bonnes pratiques, mais aussi une base de connaissances permettant aux collaborateurs de savoir quelles décisions ont été prises en fonction des circonstances du cas d'espèce.[25] Il assistera le responsable de traitement dans la réalisation des **analyses d'impact** et diligentera des **audits**.[26] Il sera en tout cas l'un des destinataires des rapports d'audit de protection des données s'il ne réalise pas les audits lui-même, puisqu'il doit contrôler les traitements et proposer des mesures. Il s'occupera de la **notification des incidents** – confirmés ou suspectés – de protection des données à la direction (voire aux autorités de contrôle) et participera à leur gestion et résolution.[27] Ces tâches seront en général accomplies en étroite collaboration avec le responsable de la sécurité des systèmes d'information (RSSI), ainsi qu'avec les services et départements concernés. Le conseiller sera le **point de contact direct** avec les clients, collaborateurs et partenaires du responsable de traitement, les autorités, le préposé fédéral et les préposés cantonaux pour toute question relative à la protection des données au sein du responsable de traitement. Il mettra au point (et animera) des formations internes et actions de sensibilisation pour que les collaborateurs et partenaires du responsable de traitement adaptent leurs méthodes de travail et adoptent de bonnes pratiques. La **formation des collaborateurs** travaillant avec des données personnelles, voire sensibles, est indispensable à une bonne gouvernance en matière de données personnelles. Le conseiller procèdera à une **veille légale** et jurisprudentielle si celle-ci n'est pas confiée au service juridique du responsable de traitement.

G. Excursus : le conseiller d'un organe fédéral

[Rz 44] L'art. 31 al. 1 let. a LPD prévoit qu'il échoit au **préposé** d'assister les organes fédéraux (et cantonaux) dans le domaine de la protection des données. L'al. 2 lui permet encore de conseiller les organes de l'administration fédérale, même si la LPD n'est pas applicable. C'est enfin à lui que revient la tâche de surveiller l'application de la LPD par les organes fédéraux.

[Rz 45] Il semblerait donc que le conseiller à la protection des données des organes fédéraux ne soit autre que le préposé. Mais l'art. 11a al. 5 let. e LPD permet aussi aux organes fédéraux, à l'instar des personnes privées, de ne pas déclarer leurs traitements, sous réserve qu'ils nomment un conseiller. L'OLPD va cependant plus loin et consacre une disposition particulière au conseiller d'un organe fédéral. En effet, l'art. 23 al. 1 OLPD prévoit que « la Chancellerie fédérale et chaque

25 Par ex. dans quel cas il est possible de transmettre des informations sur un client lorsqu'un tiers les requiert, en fonction de la qualité du tiers et du type d'informations requis.

26 Une analyse d'impact consiste en un processus visant à aider le responsable de traitement à identifier et diminuer les risques relatifs à la protection des données pour un projet particulier. Il s'agit de déterminer quel sera l'impact d'un projet sur la personnalité et les droits fondamentaux des personnes concernées par les traitements nécessaires à la mise en œuvre dudit projet.

27 Ces incidents consistent par exemple en une perte de contrôle sur des données, un accès par des tiers non autorisés ou une mise à disposition non autorisée de données personnelles à des tiers.

département désignent respectivement et au minimum un conseiller à la protection des données ». Là où le secteur privé dispose d'une faculté, la Chancellerie fédérale et les départements fédéraux ont l'obligation de désigner au moins un conseiller.

[Rz 46] Les organes fédéraux doivent d'ailleurs annoncer à leur(s) conseiller(s), dès le début, tout projet de traitement automatisé de données personnelles, afin que les exigences de la protection des données soient immédiatement prises en considération.[28] Ce n'est que si les exigences posées par les art. 12a et 12b OLPD sont respectées que les organes fédéraux seront, à l'instar des personnes privées, déliés de leur obligation de déclarer leurs traitements au préposé.[29]

[Rz 47] Contrairement au conseiller dans le secteur privé, le conseiller d'un organe fédéral n'a en principe pas de tâche de contrôle ou de représentation vers l'extérieur. Toutefois, les organes fédéraux disposent d'une marge de manœuvre pour étendre son cahier des charges et lui confier des tâches de contrôle et de représentation.[30]

III. Dans le projet de LPD révisée

[Rz 48] Le projet de LPD révisée[31] (ci-après : P-LPD) fusionne les dispositions des actuelles LPD et OLPD concernant la fonction de conseiller et les introduit dans la loi. Il n'existait pas de telles dispositions sur le conseiller dans l'avant-projet de loi, mais elles ont été ajoutées suite à la consultation qui a révélé le souhait que le conseiller soit explicitement mentionné dans la LPD révisée.[32]

[Rz 49] L'art. 9 al. 1 P-LPD prévoit ainsi que les responsables de traitement privés (anciennement « maitres de fichier ») peuvent nommer un conseiller à la protection des données. A l'instar du droit actuellement en vigueur, la désignation d'un conseiller n'est pas obligatoire. Elle pourra avoir lieu en tout temps. De nouvelles obligations feront leur apparition pour les responsables de traitement, en échange de la suppression de l'obligation pour le secteur privé de déclarer les traitements des données au préposé.[33]

[Rz 50] L'art. 21 al. 1 P-LPD prévoit que le responsable de traitement doit consulter le préposé préalablement à un traitement de données si l'analyse d'impact (cf. art. 20 P-LPD) révèle que ledit traitement présente un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, dans le cas où le responsable de traitement ne prendrait pas les mesures pour diminuer le risque. L'al. 4 de cette disposition indique que le responsable de traitement peut renoncer à consulter le préposé s'il a impliqué son conseiller à la protection des données dans le processus d'analyse d'impact.[34]

[Rz 51] Pour pouvoir bénéficier de cette possibilité, le conseiller doit exercer sa fonction de manière indépendante et sans recevoir d'instructions du responsable de traitement. Il ne doit pas non plus exercer de tâches incompatibles avec son activité de conseiller. Il doit disposer des

28 Art. 20 al. 2 OLPD.

29 Art. 23 al. 2 OLPD.

30 Commentaire OLPD (n° 11), n° 7.2, p. 15.

31 Loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (Projet), FF 2017 6803.

32 Message, FF 2017 6565 (n° 13), p. 6652.

33 *Ibid.*, pp. 6594 et 6655.

34 *Ibid.*, p. 6680.

connaissances professionnelles nécessaires, être annoncé au préposé et ses coordonnées doivent être publiées. Ces conditions sont cumulatives.[35]

[Rz 52] Le Conseil fédéral règlera dans l'OLPD révisée la désignation des conseillers par les organes fédéraux. Ces derniers seront obligés d'en nommer un, à l'instar du droit actuel. Ils devront également publier ses coordonnées et l'annoncer au préposé.

[Rz 53] Le conseiller veillera au respect des prescriptions de protection des données et prodiguera des conseils en la matière au responsable de traitement. Ce dernier sera toujours seul responsable juridiquement des traitements auxquels il procède. Le message du Conseil fédéral précise que rien n'interdit qu'un conseiller puisse être en même temps responsable de la sécurité des systèmes d'information (RSSI).[36]

[Rz 54] Le projet de LPD révisée n'apporte pas de bouleversement de la fonction de conseiller. Les exigences en vigueur sous l'empire de l'OLPD actuelle seront reprises telles quelles dans la loi. C'est le seul changement d'ordre purement formel qui peut être perçu, sans faire preuve d'une trop grande naïveté, comme une indication d'une certaine importance de la fonction de conseiller, ce d'autant que l'art. 9 P-LPD a été introduit sur la base du résultat de la consultation sur l'avant-projet.[37]

[Rz 55] Par conséquent, ce qui a été dit ci-dessus relativement au droit en vigueur devrait rester applicable sous l'empire de la future LPD.[38]

IV. Dans le RGPD

A. Introduction

[Rz 56] Le Règlement européen sur la protection des données[39] est entré en vigueur le 27 avril 2016 et est applicable depuis le 25 mai 2018. Il remplace la directive européenne 95/46/CE et, par sa nature, est directement applicable dans les Etats membres de l'Union européenne (ci-après : l'UE). Ce texte est une réforme majeure qui vise notamment à redonner du pouvoir aux personnes concernées par des traitements de données personnelles et à mieux les protéger. Dans le secteur privé, le délégué à la protection des données (ci-après : délégué) aura une importance accrue.

[Rz 57] Il faut rappeler ici que la directive 95/46 ne contenait aucune mention du délégué. Le droit national des Etats membres s'est souvent chargé d'indiquer la possibilité de nommer un délégué, comme la France et ses correspondants à la protection des données, plus communément

35 Art. 9 al. 2 P-LPD.

36 FF 2017 6565 (n° 13), p. 6652. Le Message diverge ici de l'avis de l'Office fédéral de la justice sur cette question (cf. *supra* n° II.D) qui indiquait une compatibilité de fonction entre le conseiller et le responsable de la sécurité informatique (dont les fonctions sont différentes du RSSI).

37 Comme l'indique le Message, les milieux économiques ont souhaité que les responsables du traitement qui ont désigné un conseiller puissent bénéficier de certains allègements administratifs (FF 2017 6565 (n° 13), p. 6599).

38 Le Message indique d'ailleurs que le P-LPD « reprend largement le droit en vigueur » en ce qui concerne la désignation, les tâches et le statut du conseiller (FF 2017 6565 (n° 13), p. 6652).

39 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE.

appelés « correspondants informatique et liberté », ou CIL.[40] Le CIL français n'avait pas plus de prérogatives que le conseiller.

[Rz 58] A l'inverse, le RGPD consacre au délégué une section entière logée dans le chapitre IV sur le responsable de traitement et le sous-traitant. Cette section témoigne ainsi de l'importance du délégué dans le cadre juridique de la protection des données dans l'UE. Censé faciliter la mise en conformité et le respect des normes, le délégué devient, en partie grâce au RGPD, un acteur central de la protection des données en entreprise, ainsi qu'un intermédiaire entre les différentes parties prenantes, notamment les autorités et les personnes concernées.

B. Bases légales applicables

[Rz 59] Le RGPD contient trois dispositions topiques relatives au délégué. L'art. 37 relatif à la désignation du délégué indique notamment les situations dans lesquelles un délégué doit impérativement être désigné, et les modalités de désignation. L'art. 38 précise la fonction du délégué, son statut. Enfin, l'art. 39 décrit la mission du délégué grâce à un catalogue d'activités minimal. Le considérant 97 vient contextualiser ces trois dispositions.

C. Raison d'être du délégué : garant de la conformité

[Rz 60] Le délégué est l'artisan de la conformité de la personne morale privée aux règles sur la protection des données. Le rôle du délégué est de faciliter la mise en conformité aux nouvelles règles européennes, notamment par l'implémentation d'outils et procédures. Le délégué est l'un des acteurs clés des systèmes de gouvernance des données dans l'entreprise. Du fait que sa désignation peut être obligatoire (cf. *infra*), il est clair que l'UE n'a pas voulu, contrairement à la Suisse, laisser la possibilité aux acteurs économiques de s'autoréguler dans toutes les situations.

D. Désignation

[Rz 61] Le responsable de traitement, selon les traitements de données personnelles auxquels il procède, ou le sous-traitant, peut être contraint de désigner un délégué. Nous traiterons successivement la désignation obligatoire et la désignation facultative.

1) Obligatoire

[Rz 62] L'art. 37 al. 1 RGPD rend obligatoire la désignation d'un délégué si les activités de base du responsable de traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées (let. b), ou si les activités de base du responsable de traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories par-

40 Voir l'art. 22 de la Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. A noter qu'au moment où nous écrivons ces lignes, l'Assemblée nationale procède actuellement à l'adaptation de cette loi dans le cadre du Projet de loi relatif à la protection des données personnelles (JUSC1732261L), disponible sur legifrance.gouv.fr, consulté le 4 mai 2018.

ticulières de données visées à l'art. 9 et de données personnelles relatives à des condamnations pénales et à des infractions visées à l'art. 10 (let. c).

[Rz 63] Cette disposition s'applique tant aux responsables de traitement qu'aux sous-traitants. Ces derniers doivent donc désigner un délégué, même si le responsable de traitement en a désigné un de son côté, pour autant que les critères de désignation de l'art. 37 al. 1 RGPD soient remplis pour les sous-traitants. Un sous-traitant n'est cependant pas tenu de désigner un délégué si seul le responsable de traitement y est contraint.

[Rz 64] Nonobstant l'art. 37 al. 1 RGPD, le droit national d'un Etat membre peut prévoir d'autres situations dans lesquelles la désignation d'un délégué est obligatoire.[41]

a. Activités de base d'un responsable de traitement

[Rz 65] Il convient d'abord de relever que, dans le secteur privé, la **notion d'activités de base** doit être comprise comme les activités principales du responsable de traitement ou du sous-traitant et ne concerne pas le traitement des données personnelles en tant qu'activité auxiliaire.[42] En d'autres termes, les activités principales sont celles que le responsable de traitement déploie pour atteindre ses buts (statutaires, économiques, politiques, etc.). Par exemple, le but d'une banque est de fournir des services financiers ; le but d'un assureur est de fournir des couvertures d'assurance. Ces deux activités nécessitent de traiter des données personnelles, voire sensibles, pour qu'elles soient poursuivies. Ainsi, comme le traitement de ces données est lié à l'activité principale, il relèvera donc de l'activité de base du responsable de traitement. En revanche, le traitement de données induit dans chaque entreprise par le recrutement de nouveaux employés, le paiement de leur salaire, par la présence d'un support informatique ne relève pas de l'activité de base puisque, bien que le traitement de données soit indispensable, ces activités doivent être considérées comme auxiliaires.[43]

[Rz 66] Une fois les activités de base définies, il faut déterminer si elles répondent à l'un des deux critères suivants : traiter des données personnelles dans un but de suivi régulier et systématique à grande échelle, ou traiter à grande échelle des catégories particulières de données personnelles et des données personnelles relatives à des condamnations pénales et à des infractions.

b. En cas de traitement à grande échelle de catégories particulières de données ou de données personnelles relatives à des condamnations pénales et à des infractions

[Rz 67] Ce cas de figure est explicite. Le traitement à grande échelle a été défini ci-dessus, nous n'y reviendrons pas. Nous préciserons cependant que les catégories particulières de données visées ici sont celles énumérées à l'art. 9 RGPD. Elles comprennent les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins

41 Art. 37 al. 4 RGPD.

42 Consid. 97 RGPD.

43 Comité européen sur la protection des données (ci-après : CEDP), Lignes directrices concernant les délégués à la protection des données (DPD), adoptées le 13 décembre 2016, révisées le 5 avril 2017, p. 8 (ci-après : CEPD DPD).

d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.[44]

[Rz 68] Quant à la notion de données personnelles relatives à des condamnations pénales et à des infractions qui figure à l'art. 37 al. 1 let. c RGPD, elle inclut les mesures de sureté connexes mentionnées à l'art. 10 RGPD. Ces mesures connexes peuvent relever du droit administratif, du droit pénal ainsi que du droit civil. Ainsi, les mesures prises sur la base de l'art. 28b du Code civil suisse (CC) sont considérées comme des mesures de sureté connexes au sens du RGPD.

c. En cas de suivi régulier et systématique à grande échelle

[Rz 69] Le RGPD ne donne pas de définition de la notion de « **suivi régulier et systématique** », tout au plus dispose-t-on d'un large catalogue de possibilités de « suivi du comportement » au considérant 24 dont on peut s'inspirer sans en faire une application par analogie.[45] Le tracking et le monitoring sur internet sont clairement visés ici, mais le RGPD ne se limite pas seulement au monde numérique puisqu'il inclut toutes les formes de suivi, qu'il soit réalisé en ligne ou hors ligne. Un exemple typique de suivi (en ligne et hors ligne) serait l'analyse comportementale à des fins de publicité ciblée.

[Rz 70] Le CEPD a proposé une interprétation des termes « régulier » et « systématique ». Le suivi est régulier s'il est effectué en continu ou à intervalles particuliers pendant une certaine période, s'il est récurrent ou se répète à échéances fixes, ou s'il est réalisé de manière constante ou périodique. Le suivi est systématique s'il est effectué conformément à un système ou à une stratégie, ou s'il est préétabli, organisé ou méthodique, ou s'il a lieu dans le cadre d'un programme général de collecte de données.[46]

[Rz 71] Constituent ainsi un suivi régulier et systématique :

- l'exploitation d'un réseau de télécommunications ou la fourniture de services de télécommunications ;
- les activités de marketing basées sur des données ;
- le profilage et la notation d'individus à des fins d'évaluation des risques ;
- la géolocalisation ;
- les programmes de fidélité et la publicité comportementale ;
- la surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables ;
- les dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc.[47]

---

44 Art. 9 al. 1 RGPD. A noter qu'une définition des données génétiques, biométriques et des données concernant la santé est fournie à l'art. 4 ch. 13 à 15 RGPD.

45 « [...] Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données [personnelles] qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit. » (consid. 24 relatif à l'application extraterritoriale du RGPD).

46 CEPD DPD (n° 43), p. 10 ss.

47 CEPD DPD (n° 43), p. 11.

[Rz 72] L'expression « **à grande échelle** » de l'art. 37 al. 1 let. b RGPD n'est pas non plus définie dans le règlement, mais le consid. 91 donne quelques éclaircissements.[48] Elle devrait être interprétée selon plusieurs critères, en particulier le volume de données traité, la durée du traitement, le nombre de personnes concernées par le traitement, l'étendue géographique de ce dernier. Le CEPD illustre la notion « à grande échelle » par le traitement de données :

- des patients d'un hôpital, des clients d'une banque ou d'une assurance dans le cadre de leurs activités usuelles ;
- de voyage des passagers (suivi des titres de transport) ;
- de géolocalisation en temps réel des clients d'une chaine de restauration rapide (traitement à des fins statistiques) ;
- personnelles via l'utilisation d'un moteur de recherche qui traite les données à des fins de publicité ciblée ;
- par un fournisseur de services de téléphonie ou internet et relatives au contenu, au trafic et à la localisation.

[Rz 73] Un traitement à grande échelle n'est pas réalisé dans la situation d'un médecin ou d'un avocat exerçant leur activité à titre individuel.[49]

2) Facultative

[Rz 74] En dehors des situations mentionnées *supra*, la désignation d'un délégué est facultative dans le secteur privé, à moins que le droit de l'UE ou celui d'un Etat membre ne l'exige.[50] Il convient de rappeler ici qu'une société ayant son siège en Suisse et qui n'a pas d'établissement dans l'UE n'est soumise au RGPD qu'aux conditions de l'art. 3 al. 2 RGPD, c'est-à-dire si ses activités de traitement de données personnelles sont liées à l'offre de biens ou de services à des personnes se trouvant sur le territoire de l'UE, qu'un paiement soit exigé ou non desdites personnes (let. a),[51] ou si lesdites activités sont liées au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE (let. b). En revanche, tout traitement de données personnelles qui a lieu dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'UE devrait être effectué conformément au règlement, que le traitement lui-même ait lieu ou non dans l'UE.[52]

---

48 Une opération de traitement à grande échelle vise à traiter un volume considérable de données personnelles au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, notamment pour les droits et libertés des personnes concernées (extrait du consid. 91 RGPD relatif aux analyses d'impact).

49 CEPD DPD (n° 43), p. 25.

50 Art. 37 al. 4 RGPD.

51 Afin de déterminer si un responsable de traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'UE, il y a lieu d'établir s'il est clair que le responsable de traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs Etats membres de l'UE. Alors que la simple accessibilité du site internet du responsable de traitement, d'un sous-traitant ou d'un intermédiaire dans l'UE, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable de traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs Etats membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'UE, peuvent indiquer clairement que le responsable de traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'UE (Extraits du consid. 23 RGPD).

52 Consid. 22 RGPD.

3) Formalités de désignation

[Rz 75] Les coordonnées du délégué doivent être communiquées à l'autorité de contrôle européenne et publiées (par ex. sur le site web du responsable de traitement et du sous-traitant).[53] Le RGPD requiert en outre que les coordonnées du délégué soient incluses dans les informations à fournir aux personnes concernées.[54] Ces coordonnées devront également être communiquées à une autorité de contrôle européenne en cas de violation de données personnelles[55] et en cas de consultation de ladite autorité.[56]

[Rz 76] A l'instar de ce que prévoit la LPD pour le conseiller, le délégué peut être un membre du personnel du responsable de traitement ou du sous-traitant, ou remplir ses missions sur la base d'un contrat de service.[57] Ce qui a été dit *supra* à ce sujet concernant le conseiller en droit suisse devrait donc s'appliquer *mutatis mutandis* au délégué. A noter enfin que selon l'art. 37 al. 2 RGPD, un groupe d'entreprises peut désigner un seul délégué à condition qu'un délégué soit facilement joignable à partir de chaque lieu d'établissement.

[Rz 77] Le CEPD indique que le délégué devrait idéalement se trouver dans l'UE, même si le responsable de traitement ou le sous-traitant ne s'y trouve pas. Si le responsable de traitement ou le sous-traitant n'a pas d'établissement dans l'UE, le CEPD concède que le délégué pourra mener ses activités plus efficacement hors de l'UE.[58] Un conseiller exerçant en Suisse ne devrait ainsi pas être délocalisé dans l'UE du simple fait que le responsable de traitement est soumis au RGPD.

53 Art. 37 al. 7 RGPD. Pour une entreprise suisse soumise au RGPD, il convient, à notre avis et pour des raisons pratiques, de communiquer les coordonnées du délégué à l'autorité de contrôle de l'Etat membre dans lequel le représentant de l'entreprise suisse a été désigné en vertu de l'art. 27 RGPD.

54 Art. 13 al. 1 let. b et art. 14 al. let. b RGPD.

55 Art. 33 al. 3 let. b RGPD ; cf. art. 4 ch. 12 RGPD pour une définition de la violation des données personnelles.

56 Art. 34 al. 3 let. d RGPD.

57 Art. 37 al. 6 RGPD.

58 CEPD DPD (n° 43) , p. 26.

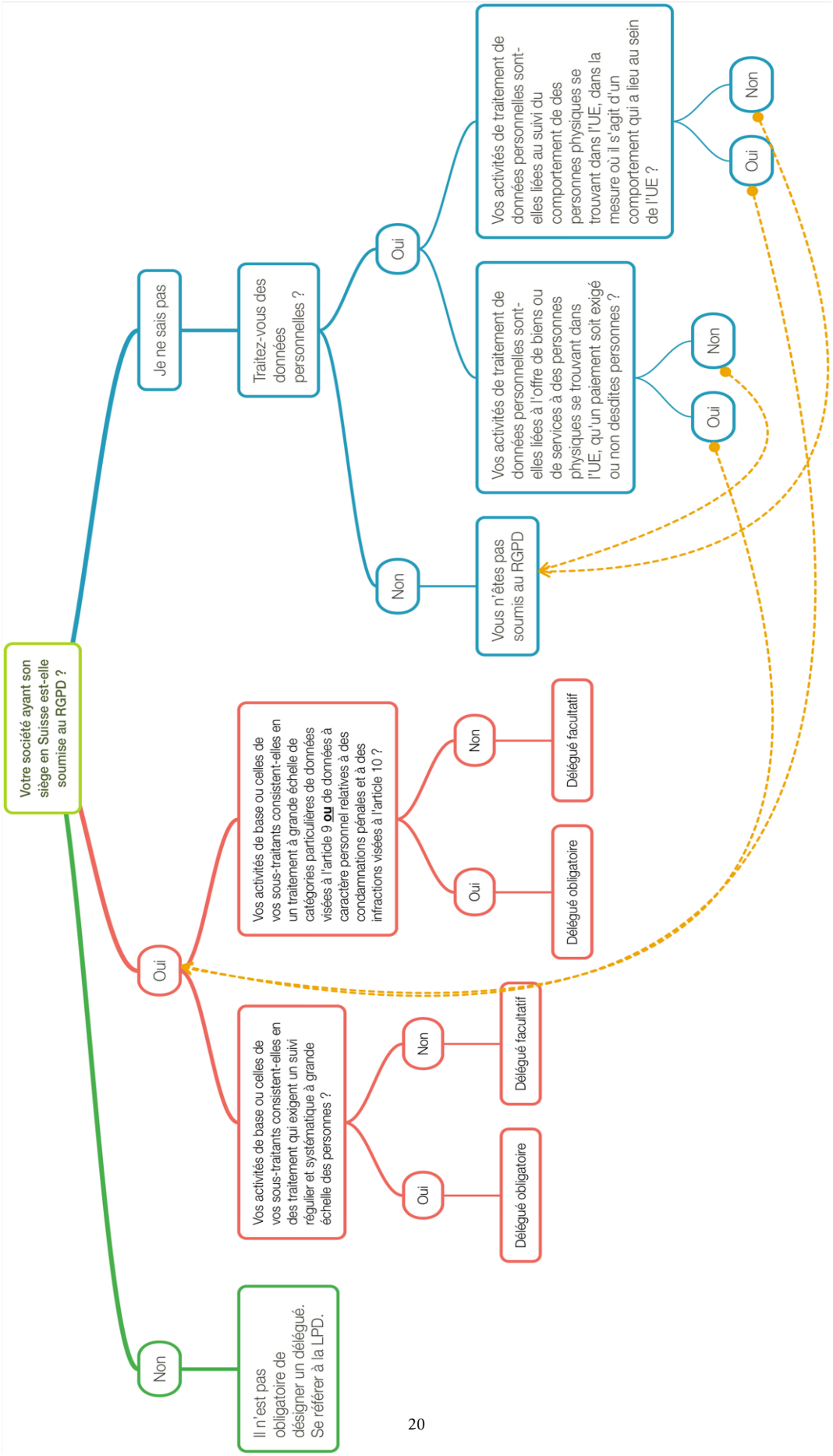
Votre société ayant son siège en Suisse est-elle soumise au RGPD ?
Oui
Non
Il n'est pas obligatoire de désigner un délégué. Se référer à la LPD.
Vos activités de base ou celles de vos sous-traitants consistent-elles en des traitement qui exigent un suivi régulier et systématique à grande échelle des personnes ?
Oui
Non
Délégué obligatoire
Délégué facultatif
Vos activités de base ou celles de vos sous-traitants consistent-elles en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ?
Oui
Non
Délégué obligatoire
Délégué facultatif
Je ne sais pas
Traitez-vous des données personnelles ?
Oui
Non
Vous n'êtes pas soumis au RGPD
Vos activités de traitement de données personnelles sont-elles liées à l'offre de biens ou de services à des personnes physiques se trouvant dans l'UE, qu'un paiement soit exigé ou non desdites personnes ?
Oui
Non
Vos activités de traitement de données personnelles sont-elles liées au suivi du comportement de des personnes physiques se trouvant dans l'UE, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE ?
Oui
Non

Schéma décisionnel pour la désignation d'un délégué (adapté de celui mis à disposition par l'International Association of Privacy Professionals).

E. Fonction et statut

[Rz 78] Le délégué doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles.[59] Le caractère approprié de l'**association du délégué** aux questions relatives à la protection des données dépendra de l'organisation interne du responsable de traitement ou du sous-traitant. Il devra faire partie des groupes de travail, comités de pilotage et autres réunions ayant à un moment donné à aborder une question de protection des données. L'indication « en temps utile » fait ici référence à l'obligation pour le responsable de traitement ou le sous-traitant de prendre en compte les problématiques de protection des données dès la conception (*privacy by design*).[60] Le délégué doit d'ailleurs être consulté lorsqu'une analyse d'impact est diligentée par le responsable de traitement ou le sous-traitant.[61] L'opinion du délégué doit être prise en compte dans l'analyse des risques et de la conformité. Si elle n'est pas suivie, il faut en documenter les raisons.[62] En cas de violation de données personnelles, le délégué doit être immédiatement prévenu et consulté puisqu'il est le point de contact pour l'autorité de contrôle compétente, laquelle devra, en principe, être notifiée.[63]

[Rz 79] L'art. 38 al. 3 RGPD indique que le responsable du traitement et le sous-traitant veillent à ce que le délégué ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le consid. 97 ajoute que cette exigence reste valable que le délégué soit ou non un employé du responsable du traitement ou du sous-traitant. Personne ne peut exiger du délégué qu'il traite une problématique dans un sens plutôt que dans un autre. L'**indépendance du délégué** est cependant limitée par son champ d'activité, lequel est fixé à *minima* par l'art. 39 RGPD, mais peut être étendu ou précisé par le responsable de traitement ou le sous-traitant. L'une des garanties de l'indépendance du délégué consiste en son droit de rapporter directement au niveau le plus élevé de la direction du responsable de traitement ou du sous-traitant (qui peut être, par exemple, la direction générale ou le comité).[64]

[Rz 80] Le délégué n'a pas l'interdiction d'exercer d'autres tâches.[65] Il peut donc exercer ses fonctions de délégué à temps partiel, pour autant que les autres tâches n'entrainent pas de **conflit d'intérêts** ni ne mettent à mal son indépendance et son accès aux ressources. Il ne peut donc pas exercer une autre fonction dont l'une des tâches consisterait à prendre des décisions quant à des traitements de données personnelles. Le CEPD estime que les fonctions suivantes sont en principe incompatibles avec la fonction de délégué : directeur général, directeur opérationnel, direc-

59 Art. 38 al. 1 RGPD.

60 Les problématiques de protection des données doivent être prises en compte tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, grâce à des mesures techniques et organisationnelles appropriées qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires (Extraits de l'art. 25 al. 1 RGPD).

61 Art. 35 al. 2 RGPD.

62 Déduit de l'art. 5 al. 2 RGPD. Le responsable de traitement est responsable de la licéité des traitements et des principes de protection des données, et est en mesure de démontrer que ceux-ci sont respectés.

63 Art. 33 RGPD ; cf. *infra* n° IV.G.4.

64 Art. 38 al. 3 *in fine* RGPD.

65 Art. 38 al. 6 RGPD.

teur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique, ainsi que des rôles à des niveaux hiérarchiquement inférieurs. Un conflit d'intérêts peut aussi survenir pour un délégué externe qui serait amené à représenter en justice le responsable de traitement ou le sous-traitant dans un dossier relatif à la protection des données.[66]

[Rz 81] Le délégué ne doit pas être désigné puis oublié. Le responsable de traitement et le sous-traitant doivent l'aider à exercer ses missions, notamment en lui fournissant les **ressources** nécessaires, en lui donnant un **accès complet aux données** personnelles et aux opérations de traitement, et en lui permettant d'entretenir ses connaissances spécialisées.[67]

[Rz 82] Relativement aux ressources, qui dépendent des traitements de données réalisés, de la présence de données sensibles, de la taille du responsable de traitement ou du sous-traitant, le délégué devra bénéficier du temps et du personnel nécessaires pour mener à bien ses missions. Le responsable de traitement ou le sous-traitant doit lui offrir son soutien, notamment par un sponsoring issu de la direction générale et du management qui permettra au délégué, par exemple, d'obtenir des autres départements et services les informations et ressources dont il a besoin. Afin de maintenir son niveau de connaissances professionnelles, le délégué devra bénéficier d'opportunités de formation continue.

[Rz 83] Quant à l'accès aux données et aux traitements, nous renvoyons ici à ce qui a été dit pour le conseiller. Dès lors que le délégué aura la tâche de réaliser ou de participer à la réalisation du registre des traitements de données personnelles, il est indispensable qu'il ait accès aux données personnelles et aux traitements, au moins sur demande.[68]

[Rz 84] Le délégué n'a pas de pouvoir de **décision** à proprement parler. Son rôle est d'informer, de conseiller et de veiller au respect des règles de protection des données. Lui octroyer un pouvoir décisionnel entrerait potentiellement en contradiction avec son indépendance et avec l'absence de responsabilité du délégué en cas de violation du RGPD, puisque le garant de la conformité est le responsable de traitement.[69]

[Rz 85] Le RGPD interdit au responsable de traitement ou au sous-traitant de relever le délégué de ses fonctions ou de le pénaliser en raison de l'exercice de ses missions.[70] Cette exigence vient renforcer l'indépendance du délégué. En revanche, il n'est pas interdit de sanctionner un délégué pour d'autres motifs.[71] Il convient de relever ici qu'un conflit normatif pourrait surgir dans le cas d'un délégué externe avec l'art. 404 al. 1 du Code des obligations (CO), lequel stipule qu'un mandat peut être révoqué ou répudié en tout temps.

66 CEPD DPD, p. 19.

67 Art. 38 al. 2 RGPD.

68 Art. 30 RGPD ; cf. *supra* n° II.D.

69 Art. 24 al. 1 RGPD.

70 Art. 38 2e phrase RGPD.

71 Cf. note 14.

F. Connaissances professionnelles

[Rz 86] Selon l'art. 37 al. 5 RGPD, le délégué est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'art. 39 RGPD.

[Rz 87] Le consid. 97 RGPD précise que, dans le secteur privé, le niveau de connaissances spécialisées requis devrait être déterminé notamment en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données personnelles traitées par le responsable du traitement ou le sous-traitant. Cela signifie par exemple qu'en cas de traitement régulier ou important de données sensibles, ou en cas d'activités de profilage ou impliquant des décisions automatisées, le délégué devrait disposer de connaissances pointues.

[Rz 88] Le CEPD ajoute qu'il est nécessaire que le délégué dispose d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD.[72] Dès lors, une formation juridique semble indispensable à un délégué. A l'inverse, de bonnes connaissances des technologies (de l'information) apparaissent comme suffisantes, à l'instar de celles relatives aux besoins en matière de sécurité des données. La connaissance du secteur d'activité et de l'organisation du responsable de traitement est seulement « utile », selon le CEPD.[73]

[Rz 89] Pour le surplus, ce qui a été expliqué *supra* (n° II.E) concernant le conseiller peut s'appliquer *mutatis mutandis* au délégué. Ce dernier, s'il est désigné par une société ayant son siège en Suisse, devra disposer de connaissances approfondies tant en droit suisse qu'en droit européen de la protection des données, ainsi que dans les droits nationaux des pays d'implantation d'éventuelles succursales ou filiales.

G. Missions

[Rz 90] En préambule, il faut rappeler que le délégué doit tenir compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.[74] Cela signifie concrètement que le délégué devrait se concentrer sur les opérations impliquant des risques élevés pour les droits et libertés des personnes (par ex. traitements de données sensibles, communications à des tiers), sans toutefois négliger les opérations présentant un risque moins élevé.

1) Informer et conseiller

[Rz 91] Le rôle principal du délégué est d'informer et de conseiller le responsable de traitement ou le sous-traitant sur tous les aspects relatifs à la protection des données, en particulier les obligations qui découlent de la réglementation européenne ou nationale applicable.[75] En d'autres termes, il lui revient notamment de sensibiliser les collaborateurs du responsable de traitement

72 CEPD DPD (n° 43), p. 14.

73 *Ibid*.

74 Art. 39 al. 2 RGPD.

75 Art. 39 al. 1 let. a RGPD.

ou du sous-traitant, de les former, de participer aux groupes de travail et autres comités dans lesquels des problématiques de protection des données sont abordées.

2) Contrôler

[Rz 92] En plus de sa fonction de conseil, le délégué a la charge de contrôler le respect (et non pas de faire respecter) des dispositions légales et règlementaires des droits européen et national relatifs à la protection des données, ainsi que les dispositions internes du responsable de traitement ou du sous-traitant. Il a notamment la possibilité de diligenter des audits afin de s'assurer que les règles sont suivies.[76]

[Rz 93] Plus généralement, le délégué pourra collecter des informations auprès des différents services impliqués dans des traitements de données personnelles (ce qui lui servira notamment dans le cadre du maintien du registre ; cf. art. 30 RGPD). Une fois nanti de ces informations, il lui reviendra d'émettre des recommandations ou de proposer des mesures, le cas échéant.

[Rz 94] Il convient ici de rappeler que le délégué n'est pas responsable en cas de non-respect du RGPD : son rôle se borne à contrôler les activités de traitement dont la mise en conformité échoit au responsable de traitement ou au sous-traitant.

3) Vérifier l'exécution des analyses d'impact

[Rz 95] Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données personnelles.[77] Cette exigence a sa source dans le principe de *privacy by design*.[78] Il revient donc au responsable de traitement ou au sous-traitant, et non au délégué, de diligenter des analyses d'impact.

[Rz 96] Alors que le délégué doit, sur demande, dispenser des conseils en ce qui concerne les analyses d'impact et vérifier l'exécution de ces dernières,[79] le responsable du traitement a l'obligation de demander conseil au délégué lorsqu'il effectue une analyse d'impact.[80] Il nous semble ici plus logique de considérer que le délégué doit fournir conseil et assistance lors de la réalisation des analyses d'impact, et ce, dès qu'il a connaissance de la volonté du responsable de traitement ou du sous-traitant de réaliser de telles analyses ou si des interrogations apparaissent quant à la pertinence de l'exécution d'une analyse d'impact.

[Rz 97] Le CEPD précise que le responsable de traitement (ou le sous-traitant) demande conseil au délégué notamment sur les éléments suivants :

- la méthodologie à suivre lors de la réalisation d'une analyse d'impact ;
- la question de savoir s'il convient d'effectuer l'analyse d'impact en interne ou de la sous-traiter ;

76 Art. 39 al. 1 let. b RGPD ; consid. 97 *in fine* RGPD.

77 Art. 35 al. 1 RGPD.

78 Art. 25 al. 1 RGPD.

79 Art. 39 al. 1 let. c RGPD.

80 Art. 35 al. 2 RGPD.

- les mesures (y compris des mesures techniques et organisationnelles) à appliquer pour atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées ;
- la question de savoir si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes au RGPD.[81]

[Rz 98] L'analyse d'impact contiendra au moins les éléments suivants :

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données personnelles et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.[82]

4) Coopérer avec l'autorité de contrôle

[Rz 99] Le délégué doit coopérer avec l'autorité de contrôle et faire office de point de contact pour celle-ci sur les questions relatives au traitement (y compris concernant la consultation préalable lorsqu'une analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque), et mener des consultations, le cas échéant, sur tout autre sujet.[83]

[Rz 100] Cette collaboration a pour but de faciliter le dialogue entre le responsable de traitement ou le sous-traitant et l'autorité de contrôle, et de permettre à celle-ci d'obtenir rapidement les informations qu'elle requiert. Il convient de préciser ici que même si le délégué est soumis à une obligation de garder le secret ou de confidentialité, il conserve le droit de prendre contact avec l'autorité de contrôle, par exemple pour lui demander son opinion, ou pour la consulter sur tout autre sujet.[84]

[Rz 101] Bien qu'il incombe au responsable de traitement de notifier l'autorité de contrôle européenne en cas de violation de données personnelles,[85] dans les faits cette tâche sera généralement exécutée par le délégué. Ainsi, une fois la violation découverte, le délégué aura un délai de 72 heures pour notifier l'autorité de contrôle. Toutes les informations relatives à la violation n'ont pas à être transmises dans les 72 heures, seule la notification avec les premiers éléments connus doit intervenir dans ce délai.[86] Le délégué du sous-traitant du responsable de traitement devra,

81 CEPD DPD (n° 43), pp. 20–21.

82 Art. 35 al. 7 RGPD.

83 Art. 39 al. 1 let. d et e RGPD ; art. 36 RGPD.

84 CEPD DPD (n° 43), p. 21.

85 Art. 33 al. 1 et 3 RGPD.

86 « [...] dès que le responsable du traitement apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'il le notifie à l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, 72 heures au plus tard après en avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que la violation en question engendre un risque pour les droits et libertés des

dans les meilleurs délais, notifier à ce dernier toute violation.[87] Le responsable de traitement aura alors 72 heures pour notifier l'autorité de contrôle européenne « choisie ».[88]

[Rz 102] Pour un responsable de traitement sis en Suisse et soumis au RGPD en vertu de l'art. 3 al. 2 RGPD, un représentant devra être nommé dans l'UE.[89] Cette nomination n'est pas obligatoire si le traitement de données est occasionnel, n'implique pas un traitement à grande échelle de catégories particulières de données personnelles ou le traitement de données relatives à des condamnations pénales et à des infractions, ou est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement, ou si le responsable du traitement est une autorité publique ou un organisme public.[90] Le représentant n'agira que comme point de contact dans l'UE entre le responsable de traitement (ou le sous-traitant) et les autorités de contrôle et les personnes concernées. Il devra être annoncé par écrit auprès de l'autorité de contrôle. Malgré la teneur de l'art. 27 al. 3 RGPD, un seul représentant doit être nommé dans l'un des Etats membres de l'UE. Idéalement, le représentant se trouvera dans l'Etat membre où se trouvent la majorité des personnes concernées.

H. Excursus : le délégué d'une autorité suisse

[Rz 103] Selon l'art. 37 al. 1 let. a RGPD, si un traitement de données est effectué par une autorité publique ou un organisme public (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle), cette autorité ou cet organisme public a l'obligation de désigner un délégué.[91] Un seul délégué peut être désigné par plusieurs autorités ou organismes différents, tant que les considérations relatives aux ressources et à l'indépendance sont respectées.

[Rz 104] Le RGPD voit son champ d'application dépasser les frontières de l'UE aux conditions de l'art. 3 al. 2, mais il est complexe de déterminer s'il s'applique ou a vocation à s'appliquer aux autorités publiques ou organismes publics d'Etats non membres de l'UE. Des questions liées à la souveraineté et à l'immunité des Etats étrangers peuvent surgir.[92]

[Rz 105] Il est recommandé aux autorités et organismes publics suisses (à l'échelon fédéral, cantonal et communal) de se renseigner à ce sujet, en particulier dans le cas où ils considèreraient que leurs activités relevant du droit privé pourraient être soumises au RGPD.

---

personnes physiques. Si une telle notification ne peut avoir lieu dans ce délai de 72 heures, la notification devrait être assortie des motifs du retard et des informations peuvent être fournies de manière échelonnée sans autre retard indu » (Extrait du consid. 85 RGPD).

87 Art. 33 al. 2 RGPD.

88 Voir note 53.

89 Art. 4 ch. 17, art. 27 RGPD.

90 Extrait du consid. 80 RGPD ; art. 27 al. 1 et 2 RGPD.

91 Les notions d'autorité publique ou d'organisme public ne sont pas définies dans le RGPD et relèvent du droit national.

92 Sur la conception du Tribunal fédéral relativement à l'immunité de juridiction et d'exécution d'un Etat étranger, voir les ATF 120 II 400 et ATF 124 III 382.

V. Conclusion

[Rz 106] En Suisse comme dans l'UE, le conseiller/délégué est le copilote de la conformité à la protection des données ; le responsable de traitement reste le pilote, mais a besoin du copilote pour diriger son avion, le faire traverser les turbulences et le faire atterrir en douceur.

[Rz 107] Nous l'avons vu, les fonctions de conseiller et de délégué sont très similaires, tant en ce qui concerne leur statut, les connaissances professionnelles minimales exigées, et leur mission. Cependant, alors qu'un délégué devra obligatoirement être désigné dans certaines situations, le droit suisse actuel laisse aux responsables de traitement privés la faculté de décider s'ils souhaitent désigner un conseiller. La révision de la LPD ne devrait rien changer à cet égard. Cet élément, ainsi que la différence notable de densité normative, permettent de constater que le RGPD consacre la fonction de délégué comme un élément essentiel permettant au responsable de traitement de démontrer sa conformité. Rien de tel en droit suisse, ce qui découle notamment de l'absence d'obligation pour les responsables de traitement de démontrer leur conformité.

[Rz 108] Il nous semblerait judicieux que la future LPD se calque sur le RGPD et rende obligatoire la désignation d'un conseiller lorsqu'un responsable de traitement (ou un sous-traitant) traite de grandes quantités de données sensibles, ou procède à des traitements qui pourraient porter une atteinte grave aux droits et libertés des personnes physiques concernées.

François Charlet, Master en droit, criminalité et sécurité des technologies de l'information, Data Protection Officer.

Les opinions exprimées ici n'engagent que l'auteur. Les problématiques exposées sont une compilation d'exemples et ne reflètent pas l'expérience personnelle de l'auteur.