_swissprivacy.law

Le sous-traitant, entre hantise et maîtrise

Luca D'Errico, le 9 février 2024

La gestion des sous-traitants est un sujet complexe et encore trop souvent négligé par les entreprises. Voici trois moments clés de la gestion des sous-traitants qui permettront d'éviter que les sous-traitants deviennent une hantise.

I. Introduction

Si je devais dire quelle peut être la hantise par excellence d'un responsable du traitement, je dirais sans hésiter la « hantise du sous-traitant ».

Malheureusement, encore trop peu d'entreprises collectant puis partageant des données personnelles réalisent à quel point leurs sous-traitants les rendent vulnérables. Certains dirigeants visionnaires, ne voulant pas trop investir sur le sujet, préfèrent « *se gratter quand ça pique* », lorsque d'autres sont rassurés par l'idée fragile d'avoir signé un contrat dédiant une clause de deux lignes où le sous-traitant s'engage à respecter les exigences légales applicables en matière de protection des données.

Pour ces amateurs de sensations fortes, la question n'est plus de savoir s'ils auront un jour de gros ennuis, mais quand ils y feront face. Pour tous les autres, l'alternative se résume donc à « maîtriser » leurs sous-traitants.

Je propose d'aborder ici brièvement trois moments clés de la gestion des sous-traitants qui, à défaut de réduire le risque à zéro, permettront de prouver à quel point le responsable du traitement a pris ce sujet très au sérieux. Il est important de souligner que les conseils partagés ici sont le fruit de mon expérience personnelle dans le domaine de la gestion des sous-traitants. Dans certaines circonstances, les lois sur la protection des données offrent une certaine marge de manœuvre au responsable du traitement, sans définir forcément les actions à entreprendre. Il peut donc être nécessaire d'adopter une vision plus large afin d'assurer la conformité.

II. Moments clés de la gestion des sous-traitant

A. Inventaire de sous-traitants

Tout responsable du traitement doit impérativement dresser et tenir à jour un inventaire exhaustif des sous-traitants qui interviennent dans ses traitements de données. En fonction de la taille de l'entreprise et des pays dans lesquels elle opère et sous-traite, cet inventaire peut s'avérer aussi difficile à réaliser qu'à maintenir, mais constitue le point de départ inévitable de ce chantier gigantesque.

Une fois les sous-traitants identifiés, il s'agira ensuite d'établir précisément quelles sont les catégories de données personnelles partagées, les finalités qui justifient leur traitement ou encore la façon dont elles sont partagées. Ces éléments d'information essentiels, mais non exhaustifs, participent à la construction de l'outil central permettant de piloter et démontrer la conformité aux exigences légales en matière de protection des données, à savoir le registre des activités de traitement, que le responsable du traitement est tenu de réaliser sous certaines conditions.

La création de ce registre et sa mise à jour sont étroitement liées à la capacité de hiérarchiser les risques pour les personnes concernées (collaborateurs, clients existants ou potentiels, etc.) relatifs aux traitements de données réalisés. Une fois ces risques identifiés et évalués, le responsable du traitement est à même d'implémenter les mesures indispensables pour maîtriser ces risques, qu'elles soient administratives, techniques, managériales ou légales, et ainsi protéger la vie privée des personnes concernées. À défaut d'implémenter lui-même, le délégué à la protection des données peut, à tout le moins, être l'initiateur de cette implémentation.

En toute hypothèse, comment faire cela concrètement ? Grâce à l'efficace outil qu'est l'analyse d'impact relative à la protection des données (AIPD). Lorsqu'elle est réalisée en bonne et due forme et qu'elle implique toutes les parties prenantes, sous-traitants inclus, elle permet de construire un traitement conforme aux exigences légales en matière de protection des données et surtout respectueux de la vie privée des personnes concernées.

La grande question-réflexe récurrente au sujet de l'AIPD est : Sommes-nous vraiment obligés de la réaliser ? Il s'agit là d'une question tendancieuse.

Voici comment les Lignes directrices du G29 répondent à cette question :

> *« Le RGPD exige des responsables du traitement qu'ils mettent en œuvre des mesures appropriées pour assurer et être en mesure de démontrer la conformité de leurs opérations avec les dispositions du règlement, en tenant compte notamment « des risques,*

> *dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques » (article 24, paragraphe 1). [...] Conformément à l'approche par les risques préconisée par le RGPD, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Ainsi, une AIPD n'est requise que lorsqu'un type de traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » (article 35, paragraphe 1).*

S'il s'arrête là, le responsable du traitement aura tendance à limiter au maximum la réalisation de cet exercice fondamental qu'est l'AIPD. C'est pourquoi je conseille vivement de lire la réponse complète, qui poursuit en précisant :

> *« Le simple fait que les conditions déclenchant l'obligation d'effectuer une AIPD ne soient pas remplies ne restreint toutefois pas l'exigence générale faite aux responsables du traitement de mettre en œuvre des mesures pour gérer de manière appropriée les risques pour les droits et libertés des personnes concernées. Concrètement, cela signifie que les responsables du traitement sont tenus d'évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement est ''susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques'' ».*

Mon expérience en matière d'AIPD révèle que c'est souvent en effectuant l'AIPD que l'on est capable de discerner avec certitude si un traitement de données personnelles analysé engendre réellement un risque élevé pour les personnes concernées ou pas. En résumé, dans le doute et même si les critères d'obligation ne l'exigent pas, il vaut mieux effectuer l'AIPD. À noter finalement qu'en Suisse, le seuil légal de réalisation d'une AIPD est le même conformément à l'art. 22 LPD. Le PFPDT a eu l'occasion de se déterminer à ce sujet dans le cadre d'un aide-mémoire.

Ce qui précède doit impérativement aider les entreprises à ne pas amalgamer « illicéité » et « insécurité ». La vraie question n'est pas de savoir si c'est légal ou non de se priver d'une AIPD, mais plutôt de s'assurer que le traitement de données n'engendre pas un risque pour les personnes qui nous confient leurs données personnelles. Se limiter strictement aux conditions légales ne suffit pas toujours ; une approche globale de la protection des données, intégrant par exemple les bonnes pratiques de la sécurité de l'information, peut se révéler essentielle

J'ai constaté au fil des ans que beaucoup de responsables du traitement adhèrent à l'exigence de mise en conformité pour les mauvaises raisons. Un peu comme ces conducteurs automobiles qui, au moment de boucler leur ceinture de sécurité, craignent plus l'amende que le pare-brise.

S'assurer que la sous-traitance soit conforme aux exigences légales en matière de protection des données/sécurité de l'information et qu'ils ne nous font courir aucun risque significatif doit être une priorité majeure pour le responsable du traitement. Non par peur d'écoper une sanction pécuniaire quelconque, mais parce que le risque de mettre la clé sous la porte à la prochaine violation de données personnelles est réel. À titre purement indicatif, j'aime citer une statistique publiée par Scott Schober (Expert en cybersécurité et auteur des livres « Hacked Again » et « La cybersécurité est l'affaire de tous »), qui dit que 60 % des PME américaines victimes de piratage ou d'une violation de données ferment leurs portes dans les six mois.

B. Relation contractuelle

Lorsque le responsable du traitement a une image claire et à jour de ses sous-traitants ou lorsqu'il est en passe de s'attacher les services d'un nouveau prestataire, il devient aussi urgent qu'important d'établir une relation contractuelle adéquate.

À sa grande surprise, il découvrira peut-être qu'aucun contrat n'a été signé avec certains sous-traitants à qui il communique des données personnelles depuis de nombreuses années. Ce scénario n'étant pas forcément pire que celui où le responsable du traitement n'a pas clairement donné d'instruction à son sous-traitant.

En tout état de cause, le plus grand soin doit être réservé à l'établissement du contrat. Et ce dernier n'est plus une affaire de juristes uniquement, sans quoi le contrat risque fort de ne pas refléter et couvrir les risques analysés dans l'AIPD, ainsi que les mesures pour y pallier, et la force du contrat s'en trouvera d'autant réduit.

Aussi étrange que cela puisse paraître, un des premiers débats consistera à définir qui revêt quel rôle dans le traitement des données. Cette question aux abords anodine peut parfois donner lieu à des débats enflammés. Dans certains cas, ce qui peut paraître évident au premier coup d'œil méritera d'être nuancé. Sur ce point, la Commission nationale de l'informatique et des libertés (CNIL) prodigue un conseil éclairé :

« *Le donneur d'ordre et le prestataire de service définissent chacun leur rôle sur la base de la*

réglementation applicable (articles 4.7, 4.8 et 28.10 du RGPD), en menant l'analyse ensemble, afin de pouvoir ensuite s'accorder sur leurs obligations respectives. Cela vaut également pour les cas de sous-traitance n'impliquant qu'un accès ponctuel aux données personnelles (telles que les opérations de maintenance). Attention, cela ne signifie pas que les parties peuvent « choisir » ensemble la qualification qui les arrange. Cette clarification est essentielle pour assurer la sécurité juridique des deux parties au contrat. »

Une fois les rôles bien définis, il s'agit d'établir un contrat clair contenant l'objet, la durée, le but du traitement, tout comme les catégories de données personnelles et les catégories de personnes concernées. Tous ces éléments définissent le cadre du traitement pour le sous-traitant. Il faut souligner que, contrairement au droit suisse (art. 9 LPD), l'art. 28 RGPD prescrit un nombre de points élémentaires qui doit figurer au sein d'un contrat de sous-traitance.

Dans les faits, le but du traitement des données personnelles correspondra généralement à la mission du sous-traitant pour autant que celle-ci soit expressément définie.

Sur ce point, il convient d'être attentifs sur les possibles évolutions des services fournis par un prestataire. En effet, il n'est pas rare qu'après quelque temps le contrat ne reflète plus entièrement ce qui avait été défini lors de sa signature. De nouvelles opérations de traitement, non prévues initialement, exigeront potentiellement que le contrat soit revu afin d'y inclure les nouvelles instructions du responsable du traitement et/ou qu'une nouvelle AIPD soit menée afin d'évaluer les risques d'un nouveau traitement pour les personnes concernées.

Un autre énorme piège consiste à sous-évaluer la question des sous-traitants du sous-traitant. En droit européen (art. 28 RGPD), le sous-traitant ne peut recruter un autre sous-traitant que sur autorisation écrite du responsable du traitement ; en droit suisse, l'autorisation ne requiert pas la forme écrite (art. 9 al. 3 LPD). Concrètement, le sous-traitant avec qui nous choisissons de collaborer doit établir une liste de ses propres sous-traitants auxquels il recourt. Cette dernière devra être intégrée dans le registre des activités de traitement que le sous-traitant doit tenir et mettre à jour en sa qualité de prestataires de services traitant des données personnelles pour le compte d'un responsable du traitement. Ce point est particulièrement important dans le cadre d'une demande de droit d'accès (cf. www.swissprivacy.law/218).

Il ne s'agit pas là d'un nouveau tracas administratif aussi perçu régulièrement comme un frein pour l'avancement du projet. Sous-estimer cette gestion en cascade des sous-traitants, c'est se réveiller un matin et découvrir peut-être que l'un des sous-traitants de notre sous-

traitant, dont nous ignorions jusque-là l'existence, a subi une violation de la sécurité des données personnelles sous-traitées, car aucune des mesures de sécurité convenues avec notre sous-traitant n'a été répercutée à son propre sous-traitant.

Le responsable du traitement ne pourra que s'en prendre à lui-même et assumer la responsabilité de cette absence de maîtrise du sujet. Il n'existe pas d'autre alternative pour lui que d'encadrer rigoureusement toutes les parties prenantes, sans exception, et de donner les instructions claires sur la façon de traiter ses données personnelles et de s'assurer des mesures mises en place dans le cadre d'audits.

Lors de cette gestion, un des casse-têtes consistera à localiser les données personnelles. Une totale transparence de l'entier de la chaîne des sous-traitants sera nécessaire. Ceux-ci devront s'engager à lister formellement les pays dans lesquels nos données seront traitées. Pour illustrer la complexité du sujet, dans le contexte de l'Union européenne, la simple consultation de données personnelles par un helpdesk du sous-traitant dans un pays tiers doit être considérée comme un transfert des données dans ledit pays (art. 28 et 44 du RGPD). Ainsi, les transferts de données personnelles doivent régulièrement être encadrés par des mécanismes de protection des données, tels que les clauses contractuelles types, les règles contraignantes d'entreprise, ou d'autres mécanismes approuvés, pour garantir un niveau adéquat de protection des données. Ces mécanismes juridiques de protection des données doivent pouvoir s'appuyer sur des outils techniques de « cartographie ou mappage des données », afin d'être capables de tracer et suivre les flux d'information dans l'organisation durant tout le cycle de vie des données.

Je terminerai d'effleurer ce thème vaste et complexe de la relation contractuelle avec le sous-traitant, en rappelant que le contrat doit impérativement contenir les exigences du responsable du traitement vis-à-vis du sous-traitant en matière de protection des données et de sécurité de l'information. Le contrat est en réalité le lieu de rencontre entre les experts métiers, légaux et de sécurité de l'information.

Si la communication entre les juristes défendant les intérêts du responsable du traitement et du sous-traitant peut s'avérer difficile, elle est complexifiée par l'irruption dans la discussion de celui qui est en charge des questions liées à la sécurité de l'information.

Car il s'agit maintenant de traduire en « clauses » les mesures techniques et organisationnelles de sécurité identifiées dans l'AIPD afin de juguler les risques analysés pour un traitement de données que nous allons confier, tout ou partie, à notre sous-traitant.

La négociation du contrat n'est donc pas une affaire de juristes uniquement, mais le carrefour de compétences pointues spécifiques où à ce stade le responsable du traitement devra s'assurer, cas échéant clairement indiquer, quelles sont les mesures techniques et organisationnelles de sécurité que le sous-traitant doit implémenter afin d'offrir des garanties suffisantes en matière de sécurité, c'est-à-dire en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité de l'information, en l'occurrence des données personnelles. Les échanges peuvent être parfois cocasses pour les uns et les autres. Le délégué à la protection des données jouera dans tout cela un rôle de facilitateur, aidant les parties à se comprendre.

La précision avec laquelle établir une relation contractuelle avec un sous-traitant passe donc par la capacité à tisser les liens essentiels entre le registre des activités de traitement et l'AIPD.

C. Audits des sous-traitants

Une fois la relation contractuelle clairement établie, il ne faut pas imaginer que le devoir du responsable du traitement s'arrête là. L'aphorisme antinomique scandant que « *la confiance n'exclut pas le contrôle* » s'applique ici. Le contrat de sous-traitance spécifiera sans ambiguïté que le sous-traitant devra mettre à la disposition du responsable du traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. Ce qui précède n'est pas théorique.

En réalité, cette clause d'audit est plus simple à écrire qu'à mettre en œuvre. Rares sont les entreprises qui ne froncent pas les sourcils lorsque le responsable du traitement annonce vouloir vérifier, lors d'un audit de son délégué à la protection des données, que le traitement de données personnelles confié respecte bien le contrat et/ou la loi. Pour avoir réalisé de nombreux audits, je peux affirmer que la plupart des sous-traitants m'indiquent en introduction que jamais un de leurs clients n'est venu vérifier quoi que ce soit, sous-entendant peut-être que nous n'avons pas confiance en eux. Ainsi, c'est souvent dans un climat de méfiance que ces audits démarrent.

À défaut d'être des visites de courtoisie, ces audits doivent permettre de surveiller activement et concrètement, au moyen d'évidences, que le sous-traitant respecte la loi et ses engagements contractuels en faveur du responsable du traitement dans la même mesure qu'il le fait pour lui-même. À l'issue de ces audits, des recommandations plus ou moins contraignantes doivent être formulées et des actions concrètes peuvent être exigées dans des

délais raisonnables. La vie privée des personnes nous ayant confié leurs données en dépend. Cette étape est absolument essentielle pour le responsable du traitement qui doit respecter le principe « *d'accountability* », issu des art. 5 et 24 du RGPD, et qui désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Ce principe d'accountability entraîne deux tâches distinctes pour le responsable du traitement. La première, à priori, consiste à s'assurer de la conformité du traitement des données personnelles. La deuxième, à posteriori, consiste à justifier de cette conformité auprès des autorités de contrôle.

III. Conclusion

Connaître parfaitement ses sous-traitants et les traitements de données que nous leur confions, établir des contrats clairs contenant toutes les instructions sur la façon de traiter nos données personnelles, et enfin vérifier que le sous-traitant respecte bien notre contrat et la loi applicable sont les trois phases essentielles d'une gestion sérieuse des sous-traitants.

La maîtrise de ce sujet est le résultat d'une approche holistique d'un sujet complexe, résultat bâti sur des compétences pluridisciplinaires. Il va de soi que cette maîtrise nécessite des investissements humains et financiers conséquents. Toutefois, ces derniers seront souvent largement inférieurs aux frais engendrés par la première défaillance d'un sous-traitant. Il vaut donc mieux bâtir sa conviction sur la compréhension des enjeux plutôt que sur une expérience traumatisante.

Proposition de citation : Luca D'Errico, Le sous-traitant, entre hantise et maîtrise, 9 février 2024 *in* www.swissprivacy.law/282