**Aide-mémoire relatif au modèle de contrat de sous-traitance de données personnelles**

A teneur de l’article 29 alinéa 1 de la Loi sur l’information, la protection des données et l’archivage, modifiée le 16.03.2023 (ci-après : nLIPDA), il est donné au responsable du traitement la possibilité de sous-traiter le traitement de données personnelles, pour autant que la loi ou un contrat écrit le prévoie.

Au regard de la pratique, il est rare qu’une base légale prévoie une telle possibilité. Il est ainsi nécessaire qu’un contrat soit conclu entre les parties. La conclusion d’un contrat est également recommandée lorsque la sous-traitance est autorisée par la loi afin de s’assurer du respect des règles de protection des données par le sous-traitant. Il est précisé que le responsable du traitement qui sous-traite demeure toujours responsable du respect de la LIPDA vis-à-vis de la personne concernée, ce également pour les agissements des sous-traitants.

Le présent document constitue uniquement une aide à la compréhension du modèle de « contrat de sous-traitance » proposé aux communes valaisannes, notamment pour les parties qui nécessitent d’être complétées par les parties. Il ne saurait dès lors être exhaustif.

Questions préalables à l’établissement du contrat :

1. Des données personnelles, sensibles ou non (selon la définition des alinéas 3 et 7 de l’article 3 nLIPDA), seront-elles sous-traitées ?
2. Non, aucune donnée personnelle ne sera traitée. La nLIPDA n’est par conséquent pas applicable. Il n’est ainsi pas nécessaire de disposer d’un contrat sous l’angle de la protection des données. Il est néanmoins recommandé, voir obligatoire, de disposer d’un contrat pour les autres questions juridiques.
3. Oui, des données personnelles au sens de la nLIPDA seront traitées. Dans ce cas, passer au point 2.
4. Existe-t-il un contrat écrit avec le partenaire contractuel ? Dans la majorité des cas, il devrait être répondu par l’affirmative à cette question. L’article 29 alinéa 1 nLIPDA prévoit d’ailleurs que tout contrat avec un sous-traitant devra être passé sous la forme écrite. Il s’agit cependant généralement de conditions générales du sous-traitant ou de simples bons de commandes. Dans ce cas, nous recommandons de vous assurer que le contrat conclu avec le sous-traitant respecte les minimaux requis par l’article 29 alinéa 1 nLIPDA. Il vous est également possible de proposer à votre sous-traitant de contracter au moyen du modèle de contrat de sous-traitance remis en annexe, et qui est présenté ci-après.

Contenu du modèle de contrat de sous-traitance :

1. Accord principal : Le modèle de contrat de sous-traitance vient en appui de l’accord principal conclu entre les parties en ce qui concerne le traitement des données personnelles. C’est ainsi un outil qui s’ajoute au contrat principal conclu entre les parties. Il doit donc y être fait référence dans le préambule déjà.
2. Application du RGPD : Dans la plupart des cas, seule la LIPDA sera applicable au traitement des données. Toutefois, il se peut que le Règlement général européen de protection des données (ci-après : RGPD) soit applicable dans certains cas.

Pour ce faire, il y a lieu de déterminer si le RGPD s’applique, notamment en prenant connaissance de son article 3[[1]](#footnote-1). Il faut alors examiner les circonstances concrètes du traitement de la sous-traitance envisagée. Ainsi, les clauses du contrat surlignées en lien avec le RGPD pourront être supprimées dans la mesure où ce règlement ne trouverait pas application.

1. Sous-traitant ultérieur : La sous-traitance ultérieure de second niveau est autorisée par la nLIPDA, et peut ainsi être prévue contractuellement, avec l’accord du responsable du traitement. Ainsi, il est prévu dans le modèle annexé que le sous-traitant de premier niveau peut sous-traiter ultérieurement (second niveau) uniquement avec l’accord écrit, y compris la forme électronique, du responsable du traitement. L’Annexe 3 devra être complétée à ces fins. Par ailleurs, le sous-traitant ultérieur (second niveau) ne pourra pas lui-même sous-traiter le traitement de données personnelles, la nLIPDA ne le permettant pas.
2. Communication transfrontière de Données personnelles : Le chiffre 7 du modèle annexé prévoit la communication transfrontière de Données personnelles. Quand bien même la communication de Données personnelles à l’étranger n’est pas formellement interdite par la nLIPDA, l’article 25 prévoit un certain nombre de règles à respecter. Il y aura ainsi lieu de déterminer le lieu de traitement des données personnelles transmises au sous-traitant, et de choisir l’option de traitement en Suisse ou également à l’étranger, en respect des principes énumérés dans le modèle. Par ailleurs, les données personnelles soumises au secret de fonction doivent être traitées en Suisse. En effet, une communication à l’étranger de données protégées par le secret de fonction pourrait revêtir une violation du secret de fonction, soit une violation de l’article 320 CP. Ainsi, dans un cas de traitement de données personnelles soumises au secret de fonction à l’étranger, il y aura lieu de prévoir un chiffrement des données réalisé en Suisse, et la clef de chiffrement devra être détenue par le Responsable du traitement. Dans l’éventualité où la clef serait détenue par le sous-traitant, il y aura lieu de prévoir des règles strictes sur l’interdiction de transmettre la clé à l’étranger, afin d’éviter que les données ne puissent être déchiffrées.
3. Annexe 1, description des parties et du traitement : Dans le cadre de l’annexe 1, il y aura lieu de définir précisément qui sont les parties (responsable du traitement et sous-traitant), les noms, fonction et coordonnées des personnes de contact de chaque partie, ainsi que les activités en rapport avec les données transférées au titre du contrat. La seconde partie de cette annexe prévoit la description du traitement, qui doit être complétée par les parties. Ceci comprend notamment les catégories de données personnelles transférées, la fréquence des transferts, la nature du traitement par le   
   sous-traitant et la durée de conservation des données. En cas de transfert à des   
   sous-traitants ultérieurs, ces informations devront également être complétées.
4. Annexe 2, mesures techniques et organisationnelles, y compris les mesures techniques et organisationnelles visant à garantir la sécurité des données : Dans ce cadre, il y aura lieu de décrire en termes spécifiques les mesures techniques et organisationnelles mises en œuvre par l’importateur de données, soit en l’espèce le sous-traitant. Des exemples sont listés à l’annexe 2 et il y a lieu de garder ceux qui sont applicables, ainsi que d’ajouter d’autres éventuelles mesures si existantes. En cas de transferts vers des sous-traitants ultérieurs, il y a lieu de décrire les mesures techniques et organisationnelles que le   
   sous-traitant ultérieur doit prendre.
5. Annexe 3 : Liste des sous-traitants ultérieurs. Cette liste doit être complétée avec les coordonnées des sous-traitants ultérieurs. Elle doit être mise à jour dès qu’un nouveau sous-traitant ultérieur est autorisé par le responsable du traitement.
6. Annexe 4 : Clauses contractuelles types (transfert de responsable du traitement à sous-traitant). Cette annexe doit être complétée uniquement lorsque des données personnelles sont transférées vers un Etat qui n’assure pas un niveau de protection adéquat au sens de l’article 25 nLIPDA, par exemple les Etats-Unis. Les clauses 17 et 18 de cette annexe devront être complétées si le RGPD trouve application.

Par ailleurs, l’Annexe I de l’Annexe 4 devra être complétée uniquement pour ce qui concerne la lettre C, à savoir l’autorité de contrôle compétente en application de la clause 13 de l’Annexe 4. Les lettres A et B sont déjà complétée par le biais de l’Annexe 1.A et 1.B vues ci-avant. Les Annexes II et III de l’Annexe 4 sont déjà complétées par les Annexes 2 et 3 vues ci-avant.

1. Article 3 RGPD – Champ d’application territorial

   1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

   2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

   a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

   b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

   3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public. [↑](#footnote-ref-1)