_swissprivacy.law

Data Processing Agreement : un outil clé pour encadrer et sécuriser la sous-traitance de données personnelles en pratique

Manon Baur, le 7 octobre 2025

Si les Data Processing Agreements sont indispensables pour encadrer la sous-traitance de données personnelles, la pratique démontre qu'ils sont encore trop souvent incomplets et négligent des points essentiels, exposant ainsi les responsables du traitement et les personnes concernées à des risques pourtant aisément évitables.

I. Introduction

L'externalisation croissante de traitements de données personnelles à des sous-traitants, tant dans le secteur privé que public et en Suisse comme à l'étranger, soulève d'importantes questions de protection des données. Ces transferts – souvent massifs – entraînent en effet une perte de contrôle inhérente, susceptible d'exposer les responsables du traitement et les personnes concernées à des risques accrus. Dans ce contexte, plusieurs remparts juridiques doivent être mis en place par les responsables du traitement, non seulement pour assurer le respect de leurs obligations en vertu du cadre légal, mais aussi pour minimiser au mieux les risques de violation de la sécurité des données ainsi transférées, et, plus globalement, de traitement(s) non conforme(s) aux prescriptions applicables, susceptibles d'engager leur responsabilité.

Dans ce contexte, les accords de sous-traitance, communément désignés par leur appellation anglophone *Data Processing Agreement* ou DPA (et à distinguer des accords conclus entre responsables de traitement, i.e., *Joint Controller Agreement*, ou entre deux sous-traitants) s'imposent comme des outils de conformité, de gestion des risques et de gouvernance clé pour les responsables du traitement. Leur importance est d'ailleurs telle que le fait de recourir, pour le responsable du traitement, intentionnellement à un sous-traitant sans base contractuelle (et hors fondement légal) constitue une violation de son devoir de diligence, passible d'une amende pouvant atteindre CHF 250'000.- (art. 61 let. b LPD).

En pratique toutefois, nombre de responsables du traitement sous-estiment la portée réelle du DPA, souvent relégué au rang de simple annexe contractuelle parmi d'autres, ou signé sur la base de modèles préétablis par le sous-traitant, parfois même rédigés pour plusieurs juridictions à la fois.

La présente contribution a ainsi pour objectif de rappeler l'utilité du DPA, non seulement eu égard au cadre légal, mais également par rapport à l'arborescence contractuelle IT dans laquelle il s'insère (ou, du moins, devrait s'insérer), en mettant l'accent sur 6 points d'attention choisis.

II. Le DPA en quelques mots

A) Ancrage légal et juridique

Conformément à l'art. 9 al. 1 LPD, le traitement de données personnelles peut être confié à un sous-traitant pour autant qu'un contrat ou la loi le prévoie et (i) que seuls sont effectués les traitements que le responsable du traitement est en droit d'effectuer lui-même, et (ii) qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit. Dans ce contexte, le responsable du traitement doit s'assurer que le sous-traitant est en mesure de garantir la sécurité des données (art. 9 al. 2 LPD).

L'art. 8 al. 1 LPD prévoit que tant le responsable du traitement que le sous-traitant doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Les mesures ainsi choisies devront permettre d'éviter toute violation de la sécurité des données, en prenant en compte le type de données traitées, mais également la finalité, la nature, l'étendue et les circonstances du traitement (8 al. 2 LPD et art. 1 al. 2 let. a et b OPDo).

Il sied encore de rappeler que le recours à un sous-traitant en pratique ne décharge pas le responsable du traitement de ses obligations, ni même de sa responsabilité. En effet, c'est bien le responsable du traitement qui demeure le premier responsable, vis-à-vis des personnes dont les données sont traitées, de la protection de leur personnalité (les régimes de limitation, respectivement d'exclusion, de responsabilité internes étant réservés). Le responsable du traitement aura ainsi tout intérêt à choisir son sous-traitant avec soin, de lui donner toutes les instructions nécessaires et d'assurer une surveillance périodique de ce dernier pour garantir une conformité au cadre légal et contractuel.

B) Portée et insertion contractuelle

En pratique, les situations de sous-traitance de tâches fondamentales au fonctionnement d'une organisation sont fréquentes, notamment lorsque leur maintien en interne s'avère trop onéreux. Tel est le cas, par exemple, de certaines fonctions propres aux ressources humaines, souvent gérées via des plateformes ou applications externalisées auprès de presta-

taires, d'ailleurs parfois établis à l'étranger. Il en va par exemple ainsi de logiciels permettant l'enregistrement du temps de travail, le suivi des absences et des vacances, la gestion des déclarations sociales ou encore la vérification des références et l'exécution de *background checks.* Ceux-ci impliquent le transfert d'un volume particulièrement important de données personnelles, y compris sensibles, telles que les informations relatives à la santé des employé ou encore aux antécédents pénaux.

Dans d'autres configurations, la sous-traitance constituera un préalable nécessaire à l'exercice même de l'activité du responsable du traitement – notamment, lorsqu'une plate-forme tierce, fournie par un prestataire, est indispensable au déroulement des opérations quotidiennes d'une entité, par exemple dans le domaine bancaire ou en matière de gestion de fortune.

Appréhender pleinement la portée pratique d'un DPA implique encore de saisir la place qu'il occupe dans l'architecture contractuelle IT de la structure concernée. Un DPA n'existe en effet que rarement de manière autonome : il est, en principe, conclu parallèlement à un contrat-cadre de services — généralement désigné sous les appellations anglophones de *Services Agreement* ou *Master Agreement* — ou en constitue directement une annexe. Par rapport à ce contrat-cadre, qui définira les conditions générales de la sous-traitance, le DPA se concentrera spécifiquement sur l'encadrement du traitement des données personnelles par le prestataire de service. Le DPA s'insérera ainsi souvent aux côtés d'autres instruments contractuels complétant le contrat-cadre précité : un contrat *Software-as-a-Service* (SaaS), qui régit les conditions d'utilisation d'un logiciel en mode SaaS (accès, licences, sécurité, support), ainsi que, par exemple, un *Service Level Agreement* (SLA), qui fixe quant à lui les engagements en matière de performance et de disponibilité dudit service.

Dans certains cas, le DPA est directement intégré aux conditions générales du sous-traitant. Il n'est pas rare non plus de rencontrer des *Global DPA*, conçus pour s'appliquer à des traitements dans plusieurs juridictions, avec seulement quelques adaptations locales. Cette approche comporte certains risques : outre les difficultés de négociation qu'elle peut engendrer, elle ne garantit pas toujours une protection optimale des intérêts du responsable du traitement (et des personnes concernées), dans la mesure où le *benchmark* choisi pourrait ne pas être des plus adaptés au droit suisse .

Compte tenu de cette arborescence contractuelle complexe, il est essentiel d'identifier clairement le rôle et la portée de chacun de ces instruments. Or, l'expérience démontre un certain laxisme de la part de nombreux responsables du traitement (et sous-traitants !) sur ce point,

ce qui se traduit en pratique par des redites, des doublons, voire même des contradictions entre documents, sources de difficultés d'interprétation supplémentaires pourtant aisément évitables.

Enfin, et contrairement au droit européen, le droit suisse ne prescrit ni forme particulière ni contenu minimal obligatoire pour un DPA, hormis – indirectement – au travers des obligations définies à l'art. 9 LPD précité. En conséquence, et notamment lorsqu'un sous-traitant est établi dans l'Union européenne – ce qui est fréquent, les clauses types issues du droit européen tendent à être reprises dans le contexte helvétique, moyennant certaines adaptations. Quoi qu'il en soit, le contenu d'un DPA, bien qu'ajustable au cas par cas, repose en pratique sur un socle commun de dispositions essentielles, garantissant la conformité aux prescriptions applicables et la protection renforcée des intérêts du responsable du traitement (et des personnes concernées).

III. Points d'attention essentiels à la négociation d'un DPA

La présente section vise à identifier six points d'intérêt souvent négligés en pratique par le responsable du traitement et les prestataires de services, qu'il est vivement recommandé de négocier avec rigueur lors de la conclusion d'un DPA. Il convient toutefois de rappeler qu'un DPA limité aux seuls éléments présentés ci-dessous ne saurait être considéré comme exhaustif. D'autres dispositions devront en effet être intégrées afin de garantir la conformité aux exigences de la LPD ainsi qu'aux meilleures pratiques propres à chaque secteur d'activité (bancaire, gestion de fortune, institutions de santé, etc.).

A) Instructions du responsable du traitement et garanties du sous-traitant

Il importe de définir avec précision les instructions générales de conduite imposées par le responsable du traitement, ainsi que les obligations et garanties d'exécution du sous-traitant. Cette clarté facilite la détermination des responsabilités en cas de litige. Lorsque le sous-traitant propose un DPA pré-rédigé, il est essentiel de veiller à ce que les clauses limitant ou excluant sa responsabilité – souvent particulièrement larges, notamment dans les contrats émanant d'entités américaines selon la tradition du common law – soient ajustées pour être conformes au droit suisse, en particulier aux art. 99 ss CO, et ainsi protéger au mieux les intérêts du responsable du traitement et des personnes concernées.

En particulier, il conviendra de veiller à ce que les limitations de responsabilité ne s'appliquent pas en cas de violations contractuelles majeures. Cela inclut notamment les incidents de sécurité, les violations de données, les atteintes à la confidentialité, ainsi que tout

usage, divulgation ou destruction non autorisés des données imputables au sous-traitant, au vu de la sensibilité des données externalisées et des enjeux associés (qui devront être définis au cas par cas).

B) Sécurité des données

Le principe de sécurité des données, énoncé à plusieurs reprises dans la LPD et l'OPDo, doit être concrétisé par des mesures techniques et organisationnelles claires. La collaboration avec des spécialistes IT est souvent nécessaire pour définir des exigences adaptées et faciliter le dialogue dans ce contexte, celui-ci pouvant parfois s'avérer technique. A noter qu'en pratique, il est quelque peu regrettable que certains DPA se limitent à rappeler ce principe général sans spécifier les mesures concrètes mises en œuvre (ce qui ne semble en outre guère conforme à la volonté du législateur).

Il pourra ainsi être question de mesures de pseudonymisation et de chiffrement des données, de contrôles d'accès et d'identifications des utilisateurs, de la protection de la transmission et du stockage, ou encore de la tenue de journaux d'évènements. Le responsable du traitement veillera ainsi systématiquement à s'enquérir des mesures de sécurité en place auprès du sous-traitant (idéalement déjà au stade de la due diligence).

À cet égard, le fait, pour un sous-traitant, de renvoyer dans son DPA à une certification (par ex. ISO 27001 ou SOC 2 Type II, toutes deux largement reconnues à l'échelle internationale) constitue un indice utile à prendre en compte, dans la mesure où ces standards passent en revue un grand nombre d'exigences de sécurité (par exemple, 93 mesures pour la certification ISO 27001). Toutefois, de telles références ne sauraient être considérées à elles seules comme suffisantes : d'une part, parce que leur validité est limitée dans le temps et suppose un suivi régulier et des audits de renouvellement ; d'autre part, parce que leur portée est souvent restreinte à certains processus ou départements d'une entreprise seulement. En outre, il convient de noter que les certifications ISO reflètent essentiellement l'état des contrôles à un instant donné, sans nécessairement évaluer leur efficacité sur la durée. À cet égard, des rapports d'assurance tels que ceux établis selon les normes ISAE ou SOC® offrent généralement une évaluation plus complète, en ce qu'ils permettent de tester l'efficacité opérationnelle des contrôles sur une période donnée. Certains critiques reprochent en outre à la certification ISO 27001 de favoriser une approche trop centrée sur la conformité documentaire, au détriment d'améliorations concrètes de la sécurité.

Ces certifications demeurent néanmoins des indicateurs précieux, à compléter cas échéant dans le DPA par des clauses contractuelles spécifiques engageant le sous-traitant à maintenir

sa ou ses certifications et à appliquer les mesures de sécurité à l'ensemble des processus pertinents identifiés par les parties.

C) Incident de sécurité

Souvent négligé, ce volet est pourtant crucial. Le responsable du traitement demeure pleinement responsable de la protection des données personnelles traitées, et doit pouvoir respecter ses obligations de notification auprès du Préposé fédéral en cas d'incident de sécurité. Il est donc impératif de définir un délai clair de notification d'un tel incident au responsable du traitement par le sous-traitant, mais également, dans ce contexte, le contenu minimal de cette notification ainsi que les modalités de coopération entre les parties.

En établissant précisément le processus d'escalade à respecter, le responsable du traitement veillera en outre à s'appuyer sur le Guide sur la notification des violations de sécurité des données établi par le PFPDT et à respecter – lorsque pertinent – les nombreuses obligations d'annonce qui sont aujourd'hui les siennes, notamment en cas de cyberattaques (voir notamment La nouvelle obligation d'annonce des cyberattaques – swissprivacy.law).

Il conviendra enfin de prévoir que le sous-traitant ne saurait procéder à une annonce sans consultation préalable du responsable du traitement.

D) Droit d'audit et de vérification

La sous-traitance induisant de facto une perte de contrôle du responsable du traitement sur les données, il est indispensable de veiller à l'intégration d'un droit d'audit clair et explicite au bénéfice de ce dernier dans le DPA. S'il arrive que les sous-traitants refusent d'abord d'intégrer un tel droit, il est vivement recommandé de tout de même le négocier (en en limitant cas échéant la portée afin d'en faciliter l'acceptation).

E) Transfert à l'étranger

Il est également impératif que le responsable du traitement identifie clairement la localisation de ses sous-traitants – un point qui ne fait pas encore l'objet d'un réflexe systématique en pratique. Toute chaîne de transfert transfrontalier doit en effet être documentée et encadrée par des garanties appropriées, notamment en ce qui concerne l'hébergement des données dans des environnements cloud.

F) Sort des données à l'issue des rapports contractuels

Si les principes de restitution ou de destruction des données à l'issue des rapports contractuels sont en général prévus, leur mise en œuvre détaillée l'est moins, ce qui peut conduire à des situations regrettables en pratique, par exemple si le sous-traitant procède à la destruction de l'intégralité des données en sa possession sans que le responsable du traitement n'ait pu en récupérer une copie en amont. Il est par conséquent vivement recommandé de préciser explicitement dans le contrat les modalités de traitement des données en fin de relation contractuelle, incluant les conditions de restitution ou de destruction des données, les délais applicables, la possibilité, pour le responsable du traitement, de récupérer les données avant toute suppression ainsi que l'obligation, pour le sous-traitant, de confirmer par écrit que ces opérations ont bien été effectuées, tout en identifiant les données devant être conservées en vertu d'obligations légales ou réglementaires.

IV. Conclusion

Souvent perçu à tort comme une simple formalité, le DPA constitue en réalité le document de référence pour la protection des données dans un contexte de sous-traitance. Il est ainsi impératif de l'adapter aux spécificités du cas d'espèce et aux bonnes pratiques sectorielles, afin d'encadrer efficacement la relation contractuelle et de minimiser les risques pour le responsable du traitement et les personnes concernées. Lors des processus de *due diligence*, l'analyse approfondie du DPA – ou, en son absence, la vérification des mesures de sécurité mises en œuvre par le sous-traitant – sera indispensable pour le responsable du traitement soucieux de se conformer à ses obligations et d'éviter toute mise en cause de sa responsabilité. Enfin, et à l'instar de tout contrat, un DPA n'est pleinement efficace que s'il est suivi dans les faits, ce qui implique la mise en place de mécanismes de contrôle rigoureux auprès du prestataire.

Proposition de citation : Manon Baur, Data Processing Agreement : un outil clé pour encadrer et sécuriser la sous-traitance de données personnelles en pratique, 7 octobre 2025 *in* www.swissprivacy.law/377