Fiche pratique n° 4: Sous-traitance: choix, forme et fond du contrat

Tout traitement de données à caractère personnel effectué par un sous-traitant doit être régi par un contrat ou un autre acte juridique établi par écrit, y compris sous forme électronique, et contraignant. Le responsable du traitement et le sous-traitant peuvent choisir de négocier leur propre contrat, y compris tous les éléments obligatoires, ou de se fonder en tout ou en partie sur des clauses contractuelles types. Le RGPD énumère à l'article 28 les éléments qui doivent figurer dans l'accord de traitement. L'accord de traitement ne devrait toutefois pas simplement reproduire les dispositions du RGPD; il devrait inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord.

1.1 Choix du sous-traitant

Le responsable du traitement est tenu de faire appel «uniquement à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées» de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée37. Le responsable du traitement est donc chargé d'évaluer le caractère suffisant des garanties fournies par le sous-traitant et devrait être en mesure de démontrer qu'il a pris sérieusement en considération tous les éléments visés dans le RGPD.

L'appréciation par le responsable du traitement du caractère suffisant des garanties est une forme d'évaluation des risques, qui dépendra grandement du type de traitement qui est confié au sous-traitant, et doit être effectuée au cas par cas, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Les éléments suivants devraient être pris en considération par le responsable du traitement afin d'évaluer le caractère suffisant des garanties: les connaissances spécialisées du sous-traitant (par exemple, l'expertise technique en ce qui concerne les mesures de sécurité et les violations de données); la fiabilité du sous-traitant et ses ressources. La réputation du sous-traitant sur le marché peut également constituer un facteur pertinent à prendre en considération par les responsables du traitement. Le responsable du traitement devrait, à une fréquence adéquate, vérifier les garanties du sous-traitant, y compris au moyen d'audits et d'inspections, le cas échéant.

1.2 Forme du contrat ou d'un autre acte juridique

Tout traitement de données à caractère personnel par un sous-traitant doit être régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, conclu entre le responsable du traitement et le sous-traitant, comme l'exige l'article 28, paragraphe 3, du RGPD.

Afin d'éviter de rencontrer des difficultés pour démontrer que le contrat ou un autre acte juridique est effectivement en vigueur, le comité européen de la protection des données recommande de s'assurer que les signatures nécessaires y figurent, conformément au droit applicable (par exemple, le droit des contrats).

Étant donné que le RGPD établit une obligation claire de conclure un contrat écrit, lorsqu'aucun autre acte juridique pertinent n'est en vigueur, son absence constitue une violation du RGPD. Tant le responsable du traitement que le sous-traitant sont chargés de veiller à ce qu'un contrat ou un autre acte juridique régisse le traitement.

Afin de se conformer à l'obligation de conclure un contrat, le responsable du traitement et le sous-traitant peuvent choisir de négocier leur propre contrat, y compris tous les éléments obligatoires, ou de se fonder en tout ou en partie sur des clauses contractuelles types pour ce qui concerne les obligations au titre de l'article 28.

Un accord entre le responsable du traitement et le sous-traitant doit respecter les exigences de l'article 28 du RGPD afin d'assurer que le sous-traitant traite des données à caractère personnel conformément aux dispositions du RGPD. Un tel accord devrait tenir compte des responsabilités spécifiques des responsables du traitement et des sous-traitants. Bien que l'article 28 dresse une liste des éléments qui doivent être abordés dans tout contrat régissant la relation entre les responsables du traitement et les sous-traitants, il laisse aux parties une certaine latitude pour négocier ces contrats.

1.3 Contenu du contrat ou d'un autre acte juridique

Tandis que les éléments visés à l'article 28 du règlement constituent le contenu essentiel du contrat, ce dernier devrait permettre au responsable du traitement et au sous-traitant de clarifier davantage la manière dont ces éléments essentiels seront mis en œuvre en recourant à des instructions détaillées. Par conséquent, l'accord de traitement ne devrait pas se contenter de reproduire les dispositions du RGPD; il devrait inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord.

Dans le même temps, le contrat devrait tenir compte « des tâches et responsabilités spécifiques du sous-traitant dans le cadre du traitement à effectuer et du risque pour les droits et libertés de la personne concernée ». D'une manière générale, le contrat entre les parties devrait être rédigé en tenant compte de l'activité de traitement des données spécifique. Par exemple, il n'est pas nécessaire d'imposer des protections et des procédures particulièrement strictes à un sous-traitant chargé d'une activité de traitement dont les risques ne sont que mineurs. En effet, bien que chaque sous-traitant doive respecter les exigences fixées par le règlement, les mesures et procédures devraient être adaptées à la situation spécifique. En tout état de cause, tous les éléments de l'article 28, paragraphe 3, doivent être couverts par le contrat.

S'agissant du contenu obligatoire du contrat ou d'un autre acte juridique, le comité européen de la protection des données interprète l'article 28, paragraphe 3, en ce sens qu'il doit exposer:

l'objet du traitement (par exemple, des enregistrements de vidéosurveillance des personnes entrant et sortant d'une installation de haute sécurité). Bien que l'objet du traitement soit un concept vaste, il doit être formulé de manière suffisamment précise pour que l'objet principal du traitement soit clair;

la durée du traitement: la période précise, ou les critères utilisés pour la déterminer, devrait être précisée; par exemple, il pourrait être fait référence à la durée de l'accord de traitement;

la nature du traitement; le type d'opérations effectuées dans le cadre du traitement (par exemple: «tournage d'un film», «enregistrement», «archivage d'images», etc.) et la finalité du traitement (par exemple, la détection d'une entrée illégale). Cette description devrait être aussi complète que possible, selon l'activité de traitement concernée, de manière à permettre à des parties extérieures (par exemple, des autorités de contrôle) de comprendre le contenu et les risques du traitement confié au sous-traitant;

le type de données à caractère personnel: celui-ci devrait être précisé de la manière la plus détaillée possible (par exemple, des images vidéo de personnes entrant et sortant de l'installation). Il ne serait pas approprié de se contenter d'indiquer qu'il s'agit de «données à caractère personnel au sens de l'article 4, paragraphe 1, du RGPD» ou de «catégories particulières de données à caractère personnel au sens de l'article 9». Dans le cas de catégories particulières de données, le contrat ou l'acte juridique devrait à tout le moins préciser quels types de données sont concernés, par exemple «informations concernant des dossiers médicaux» ou «informations indiquant si la personne concernée est membre d'un syndicat»;

les catégories de personnes concernées: celles-ci devraient également être mentionnées de façon assez précise (par exemple, «visiteurs», «employés», «services de livraison», etc.);

les obligations et les droits du responsable du traitement: les droits du responsable du traitement sont examinés plus en détail dans les sections suivantes (par exemple, en ce qui concerne le droit du responsable du traitement de mener des inspections et des audits). S'agissant des obligations du responsable du traitement, on peut citer comme exemples l'obligation du responsable du traitement de fournir au sous-traitant les données mentionnées dans le contrat, de fournir et de documenter toute instruction relative au traitement de données par le sous-traitant, de veiller, avant et pendant le traitement, au respect des obligations énoncées dans le RGPD par le sous-traitant, de superviser le traitement, y compris en menant des audits et des inspections avec le sous-traitant.