Approche contractuelle pour une gestion optimale des risques et responsabilités liés au RGPD

Cruquenaire, Alexandre; Lecroart, Elodie

Published in:
DPO news

Publication date:
2021

Document Version
le PDF de l'éditeur

Doctrine

Approche contractuelle pour une gestion optimale des risques et responsabilités liés au RGPD

Introduction

1. La collecte, l'enregistrement, l'utilisation ou encore la transmission de données à caractère personnel doivent se faire en adéquation avec les principes et obligations énoncés par le RGPD.

   Tenu par le principe d'*accountability*, le responsable du traitement doit pouvoir démontrer les mesures prises en vue d'assurer le respect de ces règles dans le cadre de ses activités. Une telle obligation, fondée sur une approche de gestion des risques, doit également tenir compte des différents intervenants prenant part aux activités de traitement.

   En effet, il découle de la nature fonctionnelle des concepts de responsable du traitement, de responsables conjoints, de sous-traitant et de destinataire que ceux-ci ont pour but de délimiter les responsabilités respectives dans la chaîne des opérations de traitement.

2. La présente contribution aborde les relations les plus fréquentes qui peuvent survenir entre les différents acteurs d'activités de traitement de données à caractère personnel. Pour chaque situation, les implications et solutions contractuelles propres seront discutées.

I. Relation entre le responsable du traitement (ou sous-traitant)[1] et le délégué à la protection des données

3. Un délégué à la protection des données (ci-après « DPD ») doit être désigné dans tous les cas prévus à l'article 37 du RGPD[2]. En dehors de ces hypothèses, lorsqu'un DPD est désigné sur une base volontaire, les mêmes conditions et obligations liées à la fonction s'appliquent[3].

   Bien que le RGPD n'impose pas formellement la conclusion d'un contrat entre le DPD et le responsable du traitement ou le sous-traitant, la sécurité juridique préconise de régler contractuellement les principaux aspects de la relation entre les parties.

4. Le DPD doit être choisi en fonction de ses connaissances spécialisées du droit et des pratiques en matière de protection des données. Qu'il s'agisse d'un membre de l'entreprise ou d'un consultant externe, le délégué à la protection des données doit présenter les qualités professionnelles requises pour exercer sa mission, tant au niveau de ses connaissances relatives à la législation en matière de protection des données que de ses acquis dans le domaine d'activité de l'organisme pour lequel il intervient.

   Si le niveau d'expertise requis pour assumer cette fonction n'est pas défini, celui-ci doit s'apprécier en fonction de la complexité des opérations de traitement de données effectuées et de la sensibilité des données traitées[4].

   Dans cette optique, la soumission du DPD à une obligation contractuelle de formation adéquate et régulière peut s'avérer utile. La définition d'un programme de formation et la prise en charge des frais liés doivent être réglées dans le contrat.

5. Lorsque cette fonction n'est pas exercée à temps plein, il convient de déterminer le nombre d'heures que le délégué à la protection des données doit consacrer à sa mission.

   Dans la mesure où certaines obligations[5] du RGPD nécessitent une réaction prompte du responsable du traitement, le délégué à la protection des données doit pouvoir garantir sa disponibilité. Il importe de s'assurer que le DPD est joignable et peut être consulté dans des conditions permettant au responsable de se conformer à ses obligations. Le DPD devrait également être en mesure de désigner une ou plusieurs autre(s) personne(s) habilitée(s) à assurer ses fonctions en cas d'indisponibilité plus ou moins longue. Vu la nécessaire confidentialité des informations liées à la fonction de DPD et les responsabilités éventuelles qui en découlent, le remplacement temporaire du DPD doit faire l'objet d'une procédure claire et être assorti de garanties appropriées. Il convient en effet de préserver non seulement le niveau de compétence, mais également le secret professionnel liés à la fonction[6].

6. La réglementation en vigueur requiert l'implication du DPD sur toutes les questions relatives à la protection des données. Le caractère effectif de cette implication peut faire l'objet d'un examen attentif par l'Autorité de protection des données[7]. Il est donc nécessaire de détailler dans le contrat les missions précises que le DPD doit prendre en charge et le champ d'application de celles-ci. Le RGPD prévoit en effet que c'est le responsable du traitement (ou le sous-traitant) qui doit, notamment, tenir le registre des activités de traitement ou procéder à une analyse d'impact. Si la responsabilité de la mise en œuvre incombe au responsable du traitement, rien n'empêche toutefois de confier, d'une manière plus ou moins large, la réalisation de ces missions au DPD[8]. Il est donc recommandé de clarifier la répartition des rôles dans le contrat afin de prévenir toute discussion ultérieure.

[1] La désignation d'un délégué à la protection des données peut s'imposer, selon les circonstances, soit uniquement au responsable du traitement ou au sous-traitant, soit à chacun d'entre eux.

[2] Conformément à l'article 37, paragraphe 1, un délégué à la protection des données doit être désigné : a) lorsque le traitement est effectué par une autorité publique ou un organisme public ; b) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou c) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

[3] Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant les délégués à la protection des données (DPD)*, WP 243, version révisée et adoptée le 5 avril 2017, p. 7.

[4] *Ibid.*, p. 13.

[5] L'on songe notamment à l'obligation de traiter la demande d'exercice par une personne concernée de ses droits dans les 30 jours à compter de la réception de la demande ou encore au délai de 72 heures à compter de la prise de connaissance d'une violation de données pour notifier l'incident à l'autorité de contrôle si cette violation engendre un risque pour les droits et libertés des personnes concernées.

[6] Sur l'obligation de secret s'imposant au DPD, voy. art. 38, § 5, RGPD. Voy. aussi les *Lignes directrices* précitées, WP243, p. 15.

[7] Voy. APD, Chambre contentieuse, Décision quant au fond, 28 avril 2020, n° 18/2020, disponible à l'adresse : www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf.

[8] Cette faculté d'élargir les missions du DPD est ainsi confirmée par les *Lignes directrices* précitées, WP243, p. 20 (concernant les analyses d'impact) et p. 22 (concernant la tenue du registre des traitements).

Compte tenu du principe d'*accountability*[9], il est en outre conseillé de prévoir que le DPD s'engage à produire, pour toute question qui lui serait soumise ou pour toute réunion à laquelle il serait convié, un compte-rendu ou un avis permettant de démontrer qu'il a été consulté.

Les droits de propriété intellectuelle relatifs à ces rapports et avis, ainsi qu'à tout autre support qui serait produit par le DPD, doivent par ailleurs faire l'objet d'une clause expresse de cession de droits d'auteur au responsable du traitement ou au sous-traitant, et ce, tant pour la durée du contrat que pour la période postérieure à celui-ci. À défaut de clause *ad hoc*, le DPD pourrait contester l'usage postérieur à la fin de la collaboration de certains documents produits par lui durant l'exercice de sa mission. L'on pense en particulier aux modèles de documents qui auraient été spécifiquement réalisés par le DPD afin de répondre aux besoins spécifiques du responsable. Le DPD étant une personne physique, le Code de droit économique exige une preuve écrite de la cession de droits d'auteur, même dans le cadre d'œuvres réalisées sur commande. Dans le cas du DPD, l'on pourrait sans doute s'appuyer sur l'objet du contrat de collaboration afin d'en déduire à tout le moins l'existence d'une licence non exclusive d'exploitation des œuvres réalisées en cours de mission[10]. Il convient toutefois de garder à l'esprit qu'en cas de doute sur la portée des dispositions contractuelles, l'article XI.167 du Code de droit économique prescrit d'interpréter le contrat en faveur du DPD (l'auteur)[11]. Une clause de propriété intellectuelle est donc recommandée afin d'assurer la sécurité juridique.

De la même manière, si le DPD souscrit des licences d'utilisation de certains logiciels ou outils spécifiques en matière de gestion des données et de mise en œuvre des procédures spécifiques de protection des données[12], il convient de prévoir contractuellement qui sera le titulaire effectif de ces licences et, éventuellement, de régler le sort de celles-ci à la fin de la mission. Le DPD devra, le cas échéant, remettre au responsable du traitement ou au sous-traitant tout identifiant ou code d'accès permettant de reprendre la main sur ces logiciels ou outils et les données qu'ils contiennent.

7. Le DPD doit agir en toute indépendance. Il ne peut exercer d'autres tâches qui entraîneraient un conflit d'intérêts. Le DPD doit faire rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant. Si le DPD ne peut recevoir d'instructions quant à la manière d'exercer ses missions, il ne devrait pas pouvoir interrompre ou suspendre ses missions dans l'hypothèse où un désaccord surviendrait entre lui et les décideurs[13]. Son rôle se limite à avertir le responsable du traitement du fait que, selon lui, une activité de traitement est incompatible avec le RGPD, sans qu'il puisse prendre quelque mesure que ce soit visant à empêcher la mise en place de l'activité de traitement. Dans ce cas, pour autant que le désaccord soit bien documenté, le devoir de conseil du DPD serait rempli[14]. Cela pose toutefois la question du statut d'une telle documentation. Elle est certes importante pour la responsabilité propre du DPD dans ses relations avec le responsable du traitement, mais pourrait également constituer un élément d'auto-incrimination du responsable du traitement si ce désaccord figurait dans la documentation officielle d'*accountability* du responsable du traitement à laquelle l'APD peut exiger d'avoir accès[15].

8. Il sera en outre prudent d'anticiper dans le contrat la transition entre le DPD actuel et son successeur. Que le changement survienne en raison d'un licenciement (pour une raison distincte de l'exercice de ses missions de DPD), d'un départ volontaire ou de la fin du contrat de consultance externe, il importe de veiller à l'intégrité et l'accessibilité de la documentation et des outils déployés pour la personne appelée à prendre la relève. Le responsable du traitement doit donc imposer des exigences en termes de format et de classification des documents produits, de modalités de stockage et de transmission au successeur en vue de garantir la continuité des démarches liées à la protection des données. Une procédure de transfert des connaissances permet en principe d'éviter tout risque d'interruption dans les services de support du DPD.

9. Lorsque le DPD est externe, il est recommandé de prévoir une clause de garantie permettant un recours en cas de violation du RGPD qui ferait suite à une faute du DPD. Dans ce cas, le responsable du traitement devrait ajouter une obligation d'assurance, surtout lorsque le DPD offre ses services au travers d'une société unipersonnelle dont la solvabilité pourrait s'avérer insuffisante[16].

[9] Posé à l'article 5, § 2, du RGPD.

[10] À propos de l'incidence de l'objet du contrat sur son interprétation dans ce cas, voy. not. A. CRUQUENAIRE, *L'interprétation des contrats en droit d'auteur*, Bruxelles, Larcier, 2007, pp. 263 et s.

[11] Ce qui implique d'écarter une cession de droits d'auteur en cas de doute sur la portée du contrat à cet égard.

[12] Voy. par exemple le « GDPR Compliance Support Tool » mis à disposition par la Commission nationale pour la protection des données (CNPD) du Grand-duché du Luxembourg qui permet notamment de gérer le registre des traitements d'une organisation. En France, la Commission nationale de l'informatique et des libertés (CNIL) a quant à elle mis à disposition l'outil « PIA » permettant de réaliser une analyse d'impact préalable.

[13] Sur l'articulation de ces contraintes opérationnelles avec la déontologie de l'avocat DPD, voy. F. COTON et J. Fr. HENROTTE, « Everything you always wanted to know about DPO (but were afraid to ask) », *Cah. jur.*, 2017/2, pp. 37-38.

[14] Sur le devoir de conseil du DPD, voy. A. CRUQUENAIRE et J. Fr. HENROTTE, « Le devoir de conseil dans le Règlement général sur la protection des données : *bis repetita placent ?* », *in Droit, normes et libertés dans le cybermonde – Liber amicorum Yves Poullet*, Bruxelles, Larcier, 2018, pp. 599 et s.

[15] Voy., par exemple, APD, Chambre contentieuse, Décision quant au fond, 15 avril 2020, n° 15/2020, no 112 (sollicitant la communication des décisions internes et des avis du DPD sur le traitement litigieux). Bien que cela déborde notre propos, l'on observera que les limites du principe d'*accountability* doivent être envisagées avec prudence, afin de ne pas heurter le principe fondamental de la présomption d'innocence auquel la jurisprudence de la CEDH lie habituellement le droit de se taire et de ne pas s'auto-incriminer. Le principe d'*accountability* contrarie ces principes liés au droit à un procès équitable ; c'est inévitable. Peut-il pour autant mener l'APD à exiger la communication des échanges « internes » entre le DPD et le responsable du traitement ? Même si le RGPD demeure relativement vague sur la portée du secret professionnel du DPD, il nous semble que celui-ci devrait être considéré comme relevant de l'essence de la fonction et qu'à défaut d'habilitation expresse du législateur pour lever cette confidentialité, l'APD ne devrait pas pouvoir exiger la communication des échanges « internes » couverts par ce secret. En ce sens, voy. F. COTON et J. Fr. HENROTTE, « Everything you always wanted to know about DPO (but were afraid to ask) », *op. cit.*, pp. 37-38. Voy. aussi, par analogie, le raisonnement de la CEDH concernant les exigences requises pour la conformité à la Convention européenne des droits de l'homme de l'obligation pour les avocats de dénoncer les soupçons de blanchiment liés à certaines activités de leurs clients (CEDH, 6 décembre 2012, *Michaud c. France*, req. n° 12323/11). Notons que la réponse à cette question de l'étendue des pouvoirs légalement reconnus à l'APD a une incidence directe sur la licéité des clauses contractuelles qui organiseraient des modalités particulières relatives à ces communications « internes ».

[16] Il n'existe pas d'obligation d'assurance pour les DPD, sauf lorsqu'ils sont avocats (l'assurance de responsabilité civile des barreaux s'appliquant par défaut aux missions de DPD remplies par des avocats).

II. Relation entre le responsable du traitement et le sous-traitant

10. L'article 28, § 3, du RGPD dispose que le recours par le responsable du traitement à un sous-traitant pour effectuer un traitement de données est régi par un contrat ou un autre acte juridique qui lie le sous-traitant à l'égard du responsable du traitement.

    Le législateur a défini certaines mentions devant obligatoirement figurer dans ce contrat ou cet autre acte juridique. Vu les limites de la présente contribution, nous soulignerons seulement certaines questions méritant une attention particulière.

    Il convient tout d'abord d'observer que l'article 28, § 8, du RGPD prévoit qu'une autorité de contrôle peut adopter des clauses contractuelles types. Plusieurs autorités de contrôle ont déjà soumis leurs projets de clauses contractuelles types à l'avis de l'EDPB[17].

11. Le contrat de sous-traitance doit avant tout délimiter avec précision l'objet, la portée du traitement et les finalités poursuivies par celui-ci. Ce n'est qu'en définissant avec précision les contours du traitement faisant l'objet de la sous-traitance que le responsable du traitement pourra, *a contrario*, exclure toute autre utilisation ou transmission à des tiers des données à caractère personnel par le sous-traitant.

12. Le responsable du traitement est légalement tenu de ne recourir qu'à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées permettant d'assurer le respect du RGPD.

    Une telle obligation implique, pour le responsable du traitement, d'effectuer au préalable une analyse du niveau de risque qu'engendrent les activités de traitement envisagées et, en conséquence, de faire entrer dans le champ contractuel les exigences en matière de sécurité auxquelles doit répondre le sous-traitant pour y répondre.

    Une énumération précise des mesures de sécurité qui doivent être prises par le sous-traitant présente l'avantage d'avoir un engagement ferme sur la mise en œuvre de ces mesures. L'inconvénient d'un détail des mesures réside dans la nécessité de modifier les documents contractuels lorsque les mesures sont modifiées, alors que l'évolutivité devrait être de l'essence même de telles mesures. Il nous semble donc peu réaliste d'exiger une énumération détaillée des mesures de sécurité. Comme l'indique l'EDPB, tout est fonction des circonstances, la description contractuelle pouvant aller de l'énumération détaillée des mesures à une simple description des objectifs minimaux de sécurité à atteindre par le sous-traitant[18]. Cette énumération doit aller de pair avec la possibilité pour le responsable du traitement d'auditer la mise en œuvre de ces mesures ou encore de les réévaluer. Le contrat doit donc régler les modalités d'une telle évaluation/adaptation.

    Lorsque le sous-traitant est appelé à fournir un outil de traitement des données, il importe de s'assurer que celui-ci intègre les principes de *privacy by design* et de *privacy by default*.

    En fonction du profil du sous-traitant, le contrat peut également prévoir une obligation de conseil quant au choix des mesures appropriées à adopter compte tenu de l'état de la technique et du niveau de risque. Tel est notamment le cas lorsque le sous-traitant met à disposition un outil de traitement de données standard incorporant des mesures de sécurisation.

    L'on soulignera en outre que le responsable est souvent placé dans des circonstances où il n'a aucune marge de manœuvre, face à des prestataires de services de grande taille qui refusent toute négociation sur leurs conditions générales de sous-traitance RGPD. L'approche d'analyse de risques portée par le RGPD trouve là un terrain d'application particulier, le responsable étant confronté au dilemme entre accepter des conditions contractuelles de collaboration non satisfaisantes (vu l'absence de marge de négociation), et devoir renoncer aux services (vu l'absence d'alternative sur le marché) alors que les services concernés sont essentiels aux activités du responsable. Cette situation n'est pas rare, notamment lorsque l'on est en présence d'opérateurs hyper spécialisés qui se savent plus ou moins incontournables dans leur secteur. À cet égard, il nous semble qu'une application raisonnable du RGPD, s'agissant d'évaluer une éventuelle entorse à ses règles, devrait considérer la situation du marché (existe-t-il des alternatives réelles ?) et le caractère plus ou moins important de l'outil litigieux par rapport aux activités du responsable du traitement[19].

    Sur le plan des principes, la responsabilité première demeure toutefois celle du responsable du traitement. L'analyse des risques et l'implication des dirigeants de l'entreprise dans la décision de choix d'un sous-traitant sont par conséquent des étapes préalables essentielles dans l'organisation interne du responsable du traitement, afin que les choix posés soient pleinement assumés.

13. Outre les aspects de sécurité, le contrat doit également définir les attentes du responsable du traitement envers le sous-traitant en ce qui concerne le devoir d'assistance et de collaboration de ce dernier.

    En fonction de l'implication du sous-traitant dans le traitement de données à caractère personnel, le responsable du traitement peut également solliciter davantage d'implication du sous-traitant dans les tâches de réalisation d'une analyse d'impact ou de gestion des demandes des personnes concernées.

    Prenons le cas d'un hôpital privé qui fait appel à un prestataire spécialisé dans la fourniture de licences de logiciel de gestion de dossier patient. Il est plus que probable que l'hôpital aspirera à un degré d'assistance élevé du prestataire, le cas échéant en collaboration avec le DPD, en cas de demande formulée par l'autorité

[17] L'EDPB a notamment déjà rendu un avis sur les projets proposés par les autorités de contrôle du Danemark (avis n° 14/2019) et de la Slovénie (avis n° 17/2020) ; ces avis sont disponibles sur le site de l'EDPB. L'autorité de contrôle française (la CNIL) propose également des exemples de clauses dans l'attente de l'adoption des clauses types.

[18] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, version 1.0, 2 septembre 2020, n° 124 (voy. aussi no 123, soulignant que le niveau de détails est à considérer comme suffisant lorsqu'il permet au responsable de se conformer à son obligation d'accountability quant au choix d'un sous-traitant présentant les garanties appropriées).

[19] En cas d'outil fourni par un sous-traitant en position dominante, et même si cela ne s'inscrit pas totalement dans la logique du RGPD, l'on pourrait en effet considérer que le manquement du sous-traitant est plus grave que celui du responsable. En pareille circonstance, il est d'ailleurs peu probable que les conditions générales de sous-traitance comportent une clause de garantie en cas de violation du RGPD imputable à un manquement du sous-traitant à ses obligations de sécurité.

de contrôle, une personne concernée ou encore lors de la réalisation d'une analyse d'impact préalable[20].

À l'inverse, le responsable du traitement devrait pouvoir exiger un niveau d'assistance moins élevé en ce qui concerne un prestataire qui fournirait une solution d'archivage standard.

14. En termes de responsabilité, le contrat de sous-traitance peut organiser une répartition de la responsabilité consécutive à une violation du RGPD, mais sans que cela porte atteinte à la réparation intégrale (et *in solidum*) due à la personne concernée[21]. Il est donc conseillé d'user de cette faculté pour opérer les aménagements utiles entre les parties, notamment lorsque le sous-traitant assume des charges qui ne lui incombent pas obligatoirement selon le RGPD[22].

15. La survenance d'une brèche de sécurité dans les outils ou les infrastructures du sous-traitant constitue un autre point délicat. Rappelons qu'en cas de survenance d'une violation de données entraînant un risque pour les droits et libertés des personnes, le responsable du traitement doit en principe avertir l'autorité de contrôle dans les 72 heures de la prise de connaissance de l'incident. Diverses informations devront être fournies à l'autorité de contrôle, afin que celle-ci évalue le niveau de risque de l'incident. Ces informations ne sont parfois connues que du sous-traitant. Le sous-traitant devra donc fournir tous les renseignements utiles au responsable du traitement. Le sous-traitant devrait également être lié par l'obligation de prendre toutes les mesures appropriées visant à limiter les conséquences préjudiciables de la violation de données, conformément aux instructions éventuelles du responsable.

    Une faculté d'audit spécifique en cas de brèche de sécurité est très utile pour permettre au responsable de rétablir un niveau de sécurité satisfaisant. Cet audit, qui peut être réalisé par un auditeur externe, sera l'occasion de déterminer si la violation de données est due à un manquement du sous-traitant à son obligation de mettre en œuvre les mesures de sécurité appropriées. Le coût de l'audit ainsi que des sanctions spécifiques pourront être mis à la charge du sous-traitant si une faute du sous-traitant est identifiée.

16. S'agissant des possibilités d'audit ou de contrôle, indépendamment d'une brèche de sécurité, celles-ci devront être expressément prévues. La régularité et le coût de ces opérations devront être négociés avec le sous-traitant. Ce dernier pourra, dans tous les cas, imposer une obligation de confidentialité à la personne responsable de l'audit ou du contrôle, afin notamment de préserver les secrets d'affaires.

17. La question du recours à des sous-traitants de second rang doit faire l'objet d'une attention particulière. Si la pratique est autorisée, le responsable du traitement devra toutefois veiller à obtenir du sous-traitant principal que celui-ci ne fasse pas appel à un sous-traitant de second rang situé en dehors de l'Union européenne, dans un pays qui ne présenterait pas des garanties équivalentes en termes de protection des données. L'arrêt *Schrems II*[23], prononcé le 16 juillet 2020 par la Cour de justice de l'Union européenne, a rappelé l'importance de cette question par rapport aux sous-traitants exposés à la législation américaine sur le renseignement[24] ou sur la procédure pénale[25].

18. La fin du contrat devra faire l'objet de dispositions contractuelles spécifiques. Outre l'obligation pour le sous-traitant de cesser immédiatement le traitement des données à caractère personnel impliquées dans le contrat, la convention devra également prévoir l'obligation de remettre au responsable du traitement (ou à toute personne désignée par lui) ou de supprimer toute copie des données dont le sous-traitant disposerait encore. Des modalités concrètes en termes de transfert des données (format du fichier, délai du transfert, documentation de l'outil intégrant les données) peuvent être utiles. La documentation attestant de la conformité aux exigences contractuelles et aux obligations spécifiques du sous-traitant devrait également être fournie. Cet aspect est important, car il convient de ne pas négliger l'hypothèse d'une plainte et/ou d'un incident, lié(s) aux activités du sous-traitant, qui surviendrai(en)t après la fin de la relation contractuelle. Il est recommandé de prévoir une assistance post-contractuelle dans un tel cas, mais, au-delà, le transfert préalable d'une documentation de conformité permet de conforter la position du responsable par rapport au principe d'*accountability*.

III. Relation entre le sous-traitant et le sous-traitant de second rang

19. La définition des obligations contractuelles imposées au sous-traitant de second rang par le sous-traitant principal dépendra essentiellement du contrat conclu entre le responsable du traitement et le sous-traitant principal. De façon évidente, ce dernier souhaitera se couvrir conformément au principe du « back-to-back » qui consiste à répercuter les engagements et responsabilités contractés à l'égard du responsable du traitement sur le sous-traitant de second rang.

    La question des délais est à cet égard déterminante. Rappelons que le responsable du traitement peut imposer au sous-traitant principal de réagir dans des délais très courts. S'il dépend du sous-traitant de second rang pour respecter cette obligation, le sous-traitant principal devra avoir la garantie que l'assistance de son propre sous-traitant interviendra en temps utile tout en prévoyant une marge nécessaire pour assurer le suivi auprès du responsable du traitement.

[20] L'assistance du sous-traitant sera notamment requise pour décrire les mesures de sécurité mises en place à travers l'outil logiciel.

[21] K. Rosier et A. Delforge, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant », *in Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, p. 677, n° 21.

[22] L'article 82, § 2, se référant en effet à une absence de responsabilité à l'égard de la personne concernée lorsque l'on est au-delà des obligations spécifiquement mises à la charge du sous-traitant par le RGPD. Dans ce cas, il est particulièrement important de régler la question d'une éventuelle prise en charge dans les rapports entre intervenants aux opérations de traitement.

[23] ,Aff. C-311/18, *Data Protection Commissioner c. Maximillian Schrems et Facebook Ireland*, 16 juillet 2020.

[24] En particulier le Foreign Intelligence and Surveillance Act (FISA), qui offre au gouvernement américain de très larges pouvoirs afin d'exiger de prestataires informatiques américains (ou de leurs filiales européennes) l'accès aux informations intéressant la sécurité nationale américaine ou la conduite des affaires étrangères des États-Unis. Sur la portée large du pouvoir en découlant, voy. not. l'étude du Parlement européen, *Fighting cybercrime and protecting privacy in the cloud*, octobre 2012, p. 34 (disponible à l'adresse : www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf). Voy. aussi S. J. Guick, « FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security », *Harvard National Security Journal*, 2010, vol. 1, pp. 88-143.

[25] Les procédures relatives au *law enforcement*. À propos du Cloud Act, voy. A. Cassart, « Premières réflexions sur le Cloud Act : contexte, mécanismes et articulations avec le RGPD », *R.D.T.I.*, 2018/4, n° 73, p. 51.

20. En prévision de l'hypothèse dans laquelle sa responsabilité se verrait engagée du fait du sous-traitant de second rang, le sous-traitant principal devrait prévoir une obligation de garantie dans le chef du sous-traitant de second rang. Cette obligation de garantie peut être assortie d'une obligation de souscrire une assurance et d'en apporter la preuve.

IV. Relation entre responsables du traitement

21. Deux hypothèses peuvent impliquer une relation entre responsables du traitement.

22. Le premier cas de figure survient lorsque deux responsables du traitement définissent conjointement les finalités et les moyens du traitement, agissant en tant que responsables conjoints du traitement. Cette hypothèse doit, selon le RGPD, être encadrée par un accord visant à refléter leurs rôles respectifs et à procéder à une répartition des responsabilités[26]. L'objectif poursuivi par le législateur européen est de veiller à ce que, dans le cadre d'opérations de traitement complexes, l'exercice des droits de la personne concernée ne soit pas rendu plus difficile en raison du nombre d'intervenants dans le traitement[27].

23. Le deuxième cas de figure concerne le transfert de données à caractère personnel d'un responsable du traitement vers un autre responsable, qui les traitera ensuite pour ses finalités propres.

Contrairement au schéma de la sous-traitance, la portée du contrat de transfert de données d'un responsable du traitement vers un autre responsable du traitement ne sera pas limitée aux seules finalités de traitement définies par le responsable du traitement-exportateur. Bien au contraire, le responsable du traitement-importateur souhaitera pouvoir utiliser les données à caractère personnel pour ses finalités propres.

Cependant, ces finalités devront être précisées dans le cadre du contrat conclu entre les deux responsables, dès lors qu'elles constitueront la pierre angulaire des engagements respectifs des parties. En effet, le responsable-importateur des données doit fonder le traitement qu'il entend effectuer sur un des fondements juridiques prévus à l'article 6, § 1er, du RGPD. Si ce traitement repose sur le consentement des personnes concernées, il devra exiger du responsable-exportateur que ce dernier ait bien obtenu les autorisations nécessaires directement auprès de ces personnes.

Le responsable du traitement-importateur des données devra lui s'engager à traiter les données à caractère personnel qui lui sont communiquées pour les seules finalités détaillées dans le contrat. À défaut, sa responsabilité devra pouvoir être engagée dans le cadre d'une clause de garantie d'éviction pour tout dommage subi par le responsable du traitement-exportateur en lien avec cette utilisation non autorisée[28].

Les parties devront également s'accorder sur les mesures de sécurité applicables au transfert de données afin de déterminer quelles dispositions devront être mises en place et qui supportera les coûts d'un tel dispositif de sécurité.

Conclusion

24. Notre rapide survol de la diversité des obligations des intervenants qui peuvent prendre part à un traitement de données à caractère personnel montre, de façon assez évidente, que les interactions entre les protagonistes concernés ne peuvent faire l'économie de dispositions contractuelles spécifiques. Ici encore, le contrat constitue un outil privilégié de gestion des risques.

Loin d'épuiser le sujet, la présente contribution a mis en lumière certains éléments clés de cette nécessaire contractualisation de la mise en œuvre du RGPD.

■ *Élodie Lecroart*
Avocate au barreau de Namur (Lexing)

■ *Alexandre Cruquenaire*
Avocat au barreau de Namur (Lexing),
Chargé de cours invité UNamur (CRIDS)

[26] Art. 26 RGPD.

[27] Une analyse plus fouillée déborde le cadre de notre contribution. Pour plus d'informations, voy. EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, *op. cit.*, pp. 40 et s.

[28] L'on pense notamment au transfert des données à des tiers ou encore à l'utilisation des données à des fins de marketing direct alors que les personnes concernées n'ont pas donné leur accord pour un tel traitement et qu'aucun lien contractuel n'existe entre la personne concernée et le responsable du traitement importateur des données.