Le traitement des données personnelles dans un groupe d'entreprises

Contents

1. Contexte

Le Règlement 2016/679[1], dit Règlement Général sur la Protection des Données (RGPD) institue un cadre harmonisé et renforcé de libre circulation des données personnelles sur le territoire de l'Union européenne. En effet, il a pour objectif de redonner aux citoyens le contrôle sur leurs données personnelles, tout en simplifiant l'environnement réglementaire pour les entreprises[2].

Sur ce dernier point par exemple, si votre entreprise est constituée de plusieurs d'entités juridiques distinctes dans divers États membres de l'Union européenne, soit un groupe d'entreprises, il n'est pas besoin de garanties particulières s'agissant de transferts de données personnelles à l'intérieur dudit groupe. Bien entendu, cela concerne uniquement les cas de transferts dans l'espace européen de libre circulation des données personnelles au sens du Chapitre V du RGPD, dont les autres dispositions restent pleinement applicables. En revanche, tout transfert de données hors de l'Union européenne (UE) et de l'Espace Économique Européen (EEE) doit faire l'objet de garanties afin de minimiser les risques pour les personnes concernées[3]. La Suisse étant au bénéfice d'une décision d'adéquation de la Commission européenne au sens de l'art. 45 RGPD, les transferts de données personnelles peuvent être importées (et exportées) sans autres autorisations spécifiques.

Toutefois, qu'en est-il au niveau contractuel dans un contexte de traitement de données dans un groupe d'entreprises ? Est-ce libre ? Faut-il un contrat de sous-traitance de traitement de données personnelles, même entre deux entités d'un même groupe d'entreprises ?

Dans un premier temps, il est nécessaire de rappeler les notions de responsable de traitement (*Data controller*), de sous-traitant (*Data processor*) et celle de responsables conjoints du traitement de données (*Joint controller*). Il convient d'emblée de préciser qu'il ne s'agit pas d'éléments statiques ou définitifs : une entité ou une entreprise peut être à la foi responsable de traitement de données personnelles mais également sous-traitante dans une autre situation. La tenue d'un registre des activités de traitement de données, conformément à l'art. 30 RGPD sera d'une grande aide. Il permet d'établir une cartographie des différents traitements de données personnelles au sein de votre organisation, indiquant notamment les différents acteurs et leurs rôles respectifs lors d'un traitement de données personnelles.

[1] EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679, consulté le 09.01.2018.
[2] Conseil de l'Union européenne, https://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/, consulté le 09.01.2018.
[3] Commission Nationale de l'Informatique et des Libertés https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue, consulté le 16.01.2019.

Vous êtes responsable du traitement si :

- Vous déterminez, seul ou conjointement avec d'autres entités, les finalités et les moyens du traitement de données personnelles considéré. En d'autres termes, vous décidez des tenants et aboutissants du traitement de données personnelles dont vous avez la maîtrise (art 4. al. 7 RGPD)[4].

Vous êtes sous-traitant si :

- Vous traitez les données personnelles uniquement sur instructions du responsable du traitement. Bien que moins autonome que le responsable du traitement, le sous-traitant est tout de même soumis à diverses obligations du RGPD[5]. Les cas les plus fréquents sont la sous-traitance du recrutement, du marketing, de la gestion des systèmes informatiques, ou encore la sous-traitance de la facturation/comptabilité voire le recours à une fiduciaire. Dans ce cas, l'entreprise qui délègue le traitement sera la responsable du traitement et le fournisseur de service sollicité sera considéré comme sous-traitant, n'agissant que sur instructions. En outre, rappelons à toutes fins utiles que le cloud computing peut également s'assimiler à un recours à la sous-traitance[6]. Dans ces situations, un contrat de sous-traitance doit être établi (art 4 al. 8 et 28 ss, Consid. 81 RGPD).

Vous êtes responsables conjoints du traitement si :

- Vous déterminez conjointement, avec la ou les entités concernée(s) de votre groupe d'entreprises, les finalités et les moyens du traitement de données considéré. La participation de chaque entité dans le processus décisionnel quant aux buts et moyens du traitement de données est fondamentale pour déterminer s'il y a ou non responsables conjoints du traitement. Il n'y a dans ce cas pas besoin de contrat, mais d'une convention qui définit clairement les rôles et responsabilités de chacun[7]. Il est pertinent de préciser à ce stade que la récente jurisprudence de la Cour de Justice de l'Union européenne (CJUE) a donné une acception très large à cette catégorie. Nous y reviendrons (art. 26, Consid. 79 RGPD).

Pour plus de détails, l'ancien Groupe de l'Art. 29 a établi une interprétation fournie à ce sujet, « *Opinion 1/2010 on the concepts of "controller" and "processor"* », apportant tous les éclairages et compléments utiles[8]. Sur la distinction responsable de traitement/sous-traitant, l'Information Commissioner's Office a publié une analyse enrichie de plusieurs exemples[9].

[4] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/, consulté le 15.01.2019.
[5] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/, consulté le 15.01.2019.
[6] Commission Nationale de l'Informatique et des Libertés, https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf, consulté le 15.01.2019.
[7] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/, consulté le 14.01.2019.
[8] EUR-Lex, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, consulté le 14.01.2019.
[9] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/, consulté le 15.01.2019.

2. Discussion

a. Sous-traitant ?

Si l'externalisation d'une fonction de l'entreprise par le biais de fournisseurs de services ne fait, dans la plupart des cas, que peu de doute quant à sa qualification de sous-traitant dans le cadre du RGPD, qu'en est-il dans le contexte d'un groupe d'entreprise ?

Il n'est pas rare qu'un groupe d'entreprises délègue certaines fonctions, comme la gestion des systèmes informatiques (IT), le marketing ou tout autre fonction à l'une ou l'autre entité du groupe. Cela implique bien souvent des transferts et des traitements de données entre deux entités au moins du groupe d'entreprises. Il est clair que tout traitement de données personnelles, à l'intérieur d'un groupe d'entreprises ou non, doit respecter les principes généraux du RGPD, notamment la licéité et la poursuite de finalités déterminées, explicites et légitimes. L'existence d'un groupe d'entreprises ne peut être une fin en soi pour justifier un traitement de données personnelles.

Cependant, la notion de sous-traitant implique d'une part une composante externe à l'entreprise qui est peu évidente dans un groupe d'entreprises, et d'autre part le responsable du traitement de données pourrait être *challengé* sur le choix d'un sous-traitant, surtout si ce dernier devait s'avérer peu fiable en matière de protection des données et de sécurité.

Or, dans un groupe d'entreprises, les entités travaillent bien souvent à un but commun et il n'est pas réellement possible d'effectuer un choix comme on le ferait s'agissant d'un « véritable » sous-traitant. De ce point de vue, la qualification de sous-traitant paraît donc peu adéquate. Dans des lignes directrices rédigées par la *Malta Gaming Authority* sous supervision de *l'Information and Data Protection Commissioner* de Malte, l'analyse semble aller dans ce sens[10].

Le considérant 37 du RGPD n'apporte quant à lui pas de réponse claire et définitive :

« Un groupe d'entreprises devrait couvrir une entreprise qui exerce le contrôle et ses entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres entreprises du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel. Une entreprise qui contrôle le traitement de données à caractère personnel dans des entreprises qui lui sont affiliées devrait être considérée comme formant avec ces dernières un groupe d'entreprises. »

Cela étant, le principe de « *no group privilege* », exigerait non seulement le respect de tous les principes du RGPD, l'assurance d'avoir les garanties de niveau adéquat de protection des données en cas de transferts hors de l'UE et de l'EEE, mais également la mise en place de contrats de sous-traitance entre les différentes entités d'un groupe d'entreprises concerné par un traitement de données personnelles[11].

[10] Malta Gaming Authority, https://www.mga.org.mt/wp-content/uploads/MGA-IDPC-GDPR-Guidelines-May-2018.pdf, consulté le 11.01.2019.
[11] FGVW, https://www.fgvw.de/en/news/archive-2012/company-law-it-intra-group-data-transfer-legal-pitfalls-for-companies, consulté le 14.01.2019.

Selon la Commission Nationale de l'Informatique et des Libertés (CNIL - France) et *l'Office of the Data Protection Commissioner* (ODPC - Irlande), il convient de considérer chaque entreprise d'un groupe comme des entités distinctes et indépendantes. Dans cette conception, un contrat de sous-traitance est nécessaire, du moins dans un concept de précaution et surtout conformément à l'interprétation des autorités de protection des données des États membres, notamment pour s'assurer que la délégation du traitement de données personnelles soit effectué avec diligence et de manière responsable[12].

Il est pertinent de rappeler que ce ne sont pas les contrats qui déterminent les rôles de responsable du traitement, de sous-traitant ou de responsables conjoints du traitement, mais bien les éléments factuels du traitement de données. Les contrats de sous-traitance ou les chartes (ou tout autre type d'accord de coordination) ne peuvent servir à limiter une responsabilité que trahissent les faits. Ainsi, dans une récente jurisprudence, la CNIL a refusé la qualification de sous-traitante à la défenderesse UBER TECHNOLOGIES INC (États-Unis), qui se déclarait sous-traitante d'UBER B.V. (Europe), conformément au contrat qui liait les deux parties. Dans le cas d'espèce, UBER TECHNOLOGIER INC s'est comportée en responsable de traitement et doit donc être qualifiée de responsable conjoint du traitement avec UBER B.V. selon la CNIL[13].

L'analyse précitée de l'autorité française de protection des données a été effectuée sous l'empire dans l'ancienne loi nationale française. Au vu des similitudes avec le RGPD et le besoin d'une certaine continuité, il est fort probable qu'il en sera de même avec le RGPD. Dès lors, cette décision doit servir de piqûre de rappel pour les entreprises : il s'agit en premier lieu de déterminer avec soin le rôle de tous les acteurs d'un traitement de données personnelles, puis de mettre en place toutes les mesures contractuelles et opérationnelles nécessaires. D'une part afin d'éviter toute mauvaise surprise et d'autre part pour démontrer une implémentation cohérente et adéquate des devoirs et obligations posés par le RGPD.

[12] Out-Law.com, https://www.out-law.com/en/articles/2018/june/yahoo-irish-data-watchdog/, consulté le 14.01.2019.
[13] Legifrance, Délibération SAN-2018-011 du 19 décembre 2018, https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037830841&fastReqId=413824161&fastPos=1, consulté le 14.01.2019.

b. Responsables conjoints du traitement ?

Il est tout-à-fait concevable que deux entités d'un groupe d'entreprises soient responsables conjointes du traitement, si chacune d'entre elles est en mesure de décider des moyens et des buts du traitement des données personnelles.

La délibération de la CNIL dans l'affaire UBER, cité ci-dessus, amène à ce sujet des éléments concrets ; rappelons qu'UBER TECHNOLOGIES INC s'est déclarée sous-traitante de UBER B.V. La qualité de responsable du traitement des données personnelles de UBER B.V. n'est pas contestée. Toutefois :

- le service est une application unique conçue aux États-Unis puis adaptée dans d'autres régions du monde
- c'est UBER TECHNOLOGIES INC qui a géré les conséquences de la violation de données sans intervention d'UBER B.V.
- c'est la société UBER TECHNOLOGIES INC qui a communiqué sur cet incident
- c'est également cette dernière qui a rédigé des documents clés relatifs aux traitement des données personnelles, qui est en charge de la formation des nouveaux employés du groupe, qui conclu des contrats avec des sociétés tierces et fournit les outils essentiels au fonctionnement du service.

Ces éléments factuels permettent de constater le rôle central d'UBER TECHNOLOGIES INC dans la détermination des finalités et moyens de traitement des données personnelles. UBER TECHNOLOGIES INC doit donc être conjointement qualifiée de responsable du traitement avec UBER B.V., nonobstant la construction contractuelle entre les deux entités.

De plus, dans deux jurisprudences en 2018, la CJUE a fortement étendu la portée de la notion de responsables conjoints du traitement de données.

- Dans sa décision du 5 juin 2018, la CJUE a admis que les administrateurs d'une page Facebook sont conjointement responsables du traitement de données personnelles avec Facebook. Cette interprétation trouve son fondement dans le fait que les administrateurs des pages Facebook puissent notamment paramétrer l'audience cible puis obtenir des rapports d'audience, même s'ils sont au demeurant anonymisés[14].
- Le 10 juillet 2018, la CJUE a statué qu'une communauté religieuse pouvait être considérée responsable conjointe du traitement avec les membres de la congrégation. Ces derniers, par l'activité de prédication porte-à-porte, collectent des données personnelles. Le fait que cette forme d'action, essentielle pour cette communauté, soit organisée, coordonnée et encouragée par ladite communauté est suffisant pour aboutir à une responsabilité conjointe du traitement, même si les données collectées ne sont pas partagées dans cette communauté[15].

[14] EUR-Lex, http://curia.europa.eu/juris/celex.jsf?celex=62016CJ0210&lang1=en&type=TXT&ancre=, consulté le 15.01.2019.
[15] EUR-Lex, http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0025&lang1=en&type=TXT&ancre=, consulté le 15.01.2019.

Il faut donc retenir de ces deux arrêts que quiconque tire directement ou indirectement un bénéfice du traitement de données ou exerce une quelconque influence sur le traitement de données pour son propre compte doit être considéré responsable conjoint du traitement avec l'autre partie en cause. Cette interprétation large est discutable, car elle a pour conséquence, entre autres, de réduire significativement la portée de la notion de sous-traitant[16].

Ces deux jugements ont été pris sous l'empire de la Directive 95/46/CE[17] désormais abrogée au profit du RGPD. Cependant, étant donné les similitudes et l'approche basée d'un point de vue de protection des personnes concernées par le traitement de données personnelle de la part de la CJUE, il est fort probable que cette interprétation subsiste dans le cadre du RGPD.

Du point de vue des personnes dont on traite les données personnelles, cette interprétation est positive : ils peuvent exercer leurs droits auprès de chacun des responsables de traitements, au contraire d'une configuration de type responsable de traitement/sous-traitant, dans laquelle la personne concernée ne peut s'adresser véritablement qu'au responsable du traitement, s'agissant de l'exercice des droits conférés par le RGPD.

Pour les responsables du traitement en revanche, il deviendra dans ce cas fort complexe de différencier avec certitude les cas de sous-traitance des cas de responsabilités conjointes d'un traitement de données, qui plus est dans le cadre de groupe d'entreprises. Afin d'éclaircir cela, les entreprises doivent sérieusement envisager la tenue d'un registre des activités de traitement de données, un « *role-check* » des parties en cause puis la mise en place de contrats de sous-traitance ou cas échéant de conventions entre responsables conjoints du traitement.

[16] Lexology, https://www.lexology.com/library/detail.aspx?g=77ddd905-24e9-445f-be42-7d014c38f549, consulté le 15.01.2019.
[17] EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046, consulté le 15.01.2019.

3. Recommandations

Sur la base des éléments théoriques et pratiques exposés ci-dessus, il convient d'apporter une ébauche de solution en plusieurs étapes :

1. ***Identification, cartographie et inventaire***

   Afin de pouvoir comprendre et qualifier la situation des traitements de données dans un groupe d'entreprises, il est d'abord nécessaire d'identifier les acteurs/entités concernées par un traitement de données personnelles. Dans cette optique, un inventaire des activités de traitement de données est un outil performant : il permet de cartographier et d'identifier les données personnelles traitées, les bases légales, les motifs justificatifs, les responsables du traitement, les éventuels sous-traitants et les mesures techniques et organisationnelles en place. Une attention particulière doit être portées aux traitements de données sensibles (art. 9 RGPD) et les traitements susceptibles de faire l'objet d'un transfert de données personnelles hors de l'UE ou de l'EEE (art. 44 ss RPGD). En outre, il peut être utile de schématiser les transferts de données entre les diverses entités pour obtenir une vue d'ensemble claire dans un environnement complexe.

2. ***Définition des rôles et des responsabilités***

   Sur la base du travail effectué à l'étape 1, il faut ensuite déterminer qui est responsable du traitement et qui en est le sous-traitant, ou cas échéant, s'il y a responsabilité conjointe du traitement de données. Cela permettra d'implémenter le type d'accord adéquat entre les entités du groupe d'entreprises concernées afin de formaliser le cadre de la relation.

3. ***Formaliser***

   Si le résultat de l'analyse conclu à un relation responsable de traitement/sous-traitant :

   - Établir un contrat de sous-traitance qui lie l'entité sous-traitante à l'égard de l'entité responsable du traitement, en définissant l'objet, la durée, la nature et la finalité du traitement, le type de données et les catégories de personnes concernées ainsi que les obligations et responsabilités respectives des deux parties (art. 28 al. 3 RGPD).
   - En cas de configuration complexe avec plusieurs entités parfois responsables parfois sous-traitantes, comme c'est parfois le cas dans un contexte de groupe d'entreprises, l'établissement d'un contrat de sous-traitance multilatéral unique est souhaitable. En effet, un document unique incluant tous les acteurs en définissant clairement les incombances de chacune des parties est plus efficient qu'une myriade de contrats de sous-traitance.

   Si les éléments soulevés indiquent la présence d'une responsabilité conjointe du traitement de données personnelles, une convention entre les responsables conjoints du traitement doit être

ratifiée. Cette convention définira clairement leurs obligations respectives. Il faudra en outre mettre à disposition des personnes concernées les informations essentielles sur cette convention (art. 26 RGPD, Consid. 79). Ce document contiendra :

- Définition et délimitation des activités de traitement pour lesquelles les parties sont responsables conjointement.
- Définition des responsabilités de chacune des parties en cause, notamment celle d'appliquer les dispositions du RGPD ou de tout autre règle de protection des données, en insistant particulièrement sur la mise en place de mesures techniques et organisationnelles suffisantes.
- Limitation/exclusion de responsabilité envers les autres responsables de traitement en cas de violations ne relevant pas des obligations stipulées dans l'accord.
- L'assurance que toutes les parties soient en mesure de répondre aux demandes des personnes concernées, notamment en désignant un point de contact.

4. ***Implémentation, suivi, contrôles***

   Une fois le cadre contractuel mis en place, il s'agira d'implémenter concrètement les éléments soulevés, par l'adoption de procédures, guides ou autres bonnes pratiques en matière de protection des données. Un suivi de la situation permettra d'assurer le bon respect des prescriptions du RGPD par toutes les parties et diminuera le risque d'incident. Selon le besoin et sur une approche basée sur les risques, des contrôles ponctuels, sous forme d'audits, de mises à disposition d'inventaires de traitement ou encore tests d'intrusion peuvent être effectués pour assurer un niveau de protection adéquat.

Nicolas Savoy

L'implémentation du RGPD est une tâche complexe qui demande un effort d'introspection significatif pour les entreprises et implique un changement radical de paradigme dans l'approche de la protection des données personnelles. L'équipe de Redstone Consulting se tient à votre disposition pour vous accompagner dans se processus et vous aider à atteindre un niveau de maturité optimal en matière de protection des données.
Plus d'informations sur www.redstoneconsulting.ch