Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD

Version 2.0

Adoptées le 7 juillet 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historique des versions

Version 2.0	7 juillet 2021	Adoption des lignes directrices après consultation publique
Version 1.0	2 septembre 2020	Adoption des lignes directrices pour consultation publique

SYNTHÈSE

Les notions de responsable du traitement, de responsable conjoint du traitement et de sous-traitant ont un rôle capital à jouer dans l'application du règlement général sur la protection des données 2016/679 (RGPD), étant donné qu'elles déterminent qui est responsable du respect des différentes règles en matière de protection des données et la manière dont les personnes concernées peuvent exercer leurs droits dans la pratique. Le sens précis de ces notions et les critères relatifs à leur interprétation correcte doivent être suffisamment clairs et cohérents dans l'ensemble de l'Espace économique européen (EEE).

Les notions de responsable du traitement, de responsable conjoint du traitement et de sous-traitant sont des notions *fonctionnelles* en ce qu'elles visent à répartir les responsabilités en fonction des rôles réels joués par les parties et des notions *autonomes* en ce qu'elles doivent être interprétées principalement selon la législation de l'UE en matière de protection des données.

Responsable du traitement

En principe, il n'existe aucune limite au type d'entité susceptible d'assumer le rôle de responsable du traitement, mais, dans la pratique, il s'agit généralement de l'organisation en tant que telle et pas d'une personne au sein de celle-ci (comme le directeur général, un employé ou un membre du conseil d'administration) qui fait office de responsable du traitement.

> Un responsable du traitement est un organisme qui *décide* de certains éléments essentiels du traitement. La responsabilité du traitement peut être définie par la loi ou découler d'une analyse des éléments ou circonstances factuels de l'espèce. Certaines activités de traitement peuvent être considérées comme étant naturellement liées au rôle d'une entité (un employeur vis-à-vis de son personnel, un éditeur envers ses abonnés ou une association à l'égard de ses membres). Très souvent, les clauses contractuelles peuvent aider à identifier le responsable du traitement, bien qu'elles ne soient pas toujours déterminantes.

Un responsable du traitement détermine les finalités et les moyens du traitement, à savoir le *pourquoi* et le *comment* de ce dernier. Le responsable du traitement doit décider à la fois des finalités et des moyens. Toutefois, certains aspects plus pratiques de la mise en œuvre (les «moyens non essentiels») peuvent être laissés à la discrétion du sous-traitant. Il n'est pas nécessaire que le responsable du traitement ait réellement accès aux données faisant l'objet du traitement pour être considéré comme un responsable du traitement.

Responsables conjoints du traitement

Il peut y avoir des responsables conjoints du traitement lorsque plus d'un acteur intervient dans le traitement. Le RGPD introduit des règles spécifiques pour les responsables conjoints du traitement et établit un cadre qui régit leur relation. Le critère essentiel pour qu'il y ait responsabilité conjointe du traitement est la participation conjointe de deux entités ou plus dans la détermination des finalités et des moyens d'une opération de traitement. Une participation conjointe peut prendre la forme d'une *décision commune* prise par deux entités ou plus ou découler de *décisions convergentes* adoptées par deux entités ou plus, lorsque les décisions se complètent et sont nécessaires à la réalisation du traitement de telle sorte qu'elles ont un effet concret sur la détermination des finalités et des moyens du traitement. Un critère important est que le traitement ne serait pas possible sans la participation des deux parties en ce sens que le traitement par chacune des parties est indissociable de celui de l'autre, c'est-à-dire inextricablement lié. La participation conjointe doit englober, d'une part, la détermination des finalités et, de l'autre, la détermination des moyens.

Sous-traitant

Un sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Il existe deux conditions de base pour être considéré comme un sous-traitant: il doit s'agir d'une entité distincte du responsable du traitement et il doit traiter les données à caractère personnel pour le compte du responsable du traitement.

Le sous-traitant ne doit traiter les données que selon les instructions du responsable du traitement. Ces instructions peuvent néanmoins lui laisser une certaine marge d'appréciation quant à la manière de servir au mieux les intérêts du responsable du traitement, en permettant au sous-traitant de choisir les moyens techniques et organisationnels les plus appropriés. Toutefois, un sous-traitant viole le RGPD s'il va au-delà des instructions du responsable du traitement et commence à déterminer ses propres finalités et ses propres moyens de traitement. Il sera alors considéré comme un responsable du traitement pour ce traitement et pourra faire l'objet de sanctions pour avoir outrepassé les instructions du responsable du traitement.

Relation entre le responsable du traitement et le sous-traitant

Un responsable du traitement ne doit recourir qu'à des sous-traitants qui offrent des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences du RGPD. Les éléments à prendre en considération pourraient être 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, les ressources du sous-traitant et son respect d'un code de conduite ou d'un mécanisme de certification approuvés.

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 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.

Relation entre les responsables conjoints du traitement

Les responsables conjoints du traitement définissent de manière transparente, par accord entre eux, leurs obligations respectives aux fins d'assurer le respect des obligations que leur impose le RGPD. La détermination de leurs responsabilités respectives doit notamment porter sur l'exercice des droits des personnes concernées et l'obligation d'information. En outre, la répartition des responsabilités devrait couvrir d'autres obligations incombant au responsable du traitement, notamment en ce qui concerne les principes généraux de la protection des données, la base juridique, les mesures de sécurité, l'obligation de notification des violations de données, les analyses d'impact relatives à la protection des données, le recours à des sous-traitants, les transferts vers des pays tiers et les contacts avec les personnes concernées et les autorités de contrôle.

Chaque responsable conjoint du traitement a le devoir de s'assurer qu'il dispose d'une base juridique pour le traitement et que les données ne sont pas traitées ultérieurement d'une manière incompatible avec les finalités pour lesquelles elles ont été initialement collectées par le responsable du traitement qui partage les données.

Le RGPD ne précise pas la forme juridique de l'accord conclu entre les responsables conjoints du traitement. Par souci de sécurité juridique et afin de garantir la transparence et la responsabilité, le comité européen de la protection des données recommande que cet accord prenne la forme d'un document contraignant, tel qu'un contrat ou un autre acte juridique contraignant en vertu du droit de l'UE ou de l'État membre auquel les responsables du traitement sont soumis.

L'accord reflète dûment les rôles et rapports respectifs des responsables conjoints du traitement à l'égard des personnes concernées et le contenu de l'accord est mis à la disposition de la personne concernée.

Indépendamment des termes de l'accord, les personnes concernées peuvent exercer leurs droits à l'égard et à l'encontre de chacun des responsables conjoints du traitement. Les autorités de contrôle ne sont pas liées par les termes de l'accord que ce soit en ce qui concerne la question de la qualité de responsables conjoints du traitement des parties ou du point de contact désigné.

TABLE DES MATIÈRES

Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point e), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD» ou le «règlement»),

vu l'accord sur l'Espace économique européen et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

considérant que les travaux préparatoires des lignes directrices ont impliqué la collecte des contributions des parties prenantes, tant par écrit qu'à l'occasion d'un événement organisé pour les parties prenantes, afin de recenser les défis les plus urgents;

A ADOPTÉ LES LIGNES DIRECTRICES SUIVANTES

INTRODUCTION

1. Le présent document vise à fournir des orientations sur les notions de responsable du traitement et de sous-traitant fondées sur les règles du RGPD relatives aux définitions visées à l'article 4 et les dispositions relatives aux obligations énoncées dans le chapitre IV. Son objectif principal consiste à clarifier le sens de ces notions, les différents rôles et la répartition des responsabilités entre ces acteurs.

2. La notion de responsable du traitement et son interaction avec celle de sous-traitant ont un rôle capital dans l'application du RGPD, étant donné qu'elles déterminent qui est responsable du respect des différentes règles en matière de protection des données et comment les personnes concernées peuvent exercer leurs droits dans la pratique. Le RGPD énonce clairement le principe de responsabilité, selon lequel le responsable du traitement veille à la conformité avec les principes relatifs au traitement de données à caractère personnel visés à l'article 5 et est en mesure de démontrer cette conformité. En outre, le RGPD introduit des règles plus spécifiques sur le recours au(x) sous-traitant(s) et quelques dispositions sur le traitement de données à caractère personnel s'adressent non seulement aux responsables du traitement, mais aussi aux sous-traitants.

3. Il est donc primordial que le sens précis de ces notions et les critères de leur bonne application soient suffisamment clairs et communs dans l'ensemble de l'Union européenne et de l'EEE.

4. Le groupe de travail «Article 29» a publié des orientations sur les notions de «responsable du traitement» et de «sous-traitant» dans son avis 1/2010 (WP 169)[2] afin de fournir des éclaircissements et des exemples concrets concernant ces notions. Depuis l'entrée en vigueur du RGPD, de nombreuses questions ont été soulevées quant à la mesure dans laquelle ce règlement a apporté des changements aux notions de responsable du traitement et de sous-traitant et à leurs rôles respectifs. Ces questions

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[2] Avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16 février 2010, WP 169.

ont notamment porté sur le fond et sur les conséquences de la notion de responsabilité conjointe du traitement (par exemple, au sens de l'article 26 du RGPD) et sur les obligations spécifiques imposées aux sous-traitants par le chapitre IV (par exemple, à l'article 28 du RGPD). Par conséquent, et étant donné qu'il reconnaît que l'application concrète de ces notions doit être clarifiée, le comité européen de la protection des données juge désormais nécessaire de fournir des orientations plus détaillées et plus précises afin de garantir une approche cohérente et harmonisée dans l'ensemble de l'Union et de l'EEE. Les présentes lignes directrices remplacent le précédent avis du groupe de travail «Article 29» sur ces notions (WP 169).

5. Dans la partie I, les présentes lignes directrices examinent les définitions des différentes notions de «responsable du traitement», de «responsables conjoints du traitement», de «sous-traitant» et de «tiers/destinataire». Dans la partie II, des orientations supplémentaires sont données sur les conséquences associées aux différents rôles de responsable du traitement, de responsables conjoints du traitement et de sous-traitant.

PARTIE I – NOTIONS

1 OBSERVATIONS GÉNÉRALES

6. En son article 5, paragraphe 2, le RGPD introduit clairement le principe de responsabilité, à savoir que:

   - le responsable du traitement est *responsable du respect* des principes énoncés au paragraphe 1 dudit article et que
   - le responsable du traitement est en mesure de *démontrer le respect* des principes énoncés au paragraphe 1 dudit article.

   Ce principe a été décrit dans un avis du groupe de travail «Article 29»[3] et ne sera pas examiné en détail ici.

7. L'introduction du principe de responsabilité dans le RGPD et sa mise en avant en tant que principe central avaient pour but de souligner que les responsables du traitement doivent mettre en œuvre des mesures appropriées et effectives et être à même de démontrer la conformité du traitement avec le règlement.[4]

8. Le principe de responsabilité a été précisé à l'article 24, qui dispose que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de **démontrer** que le traitement est effectué conformément au RGPD. Ces mesures sont réexaminées et actualisées si nécessaire. Le principe de responsabilité est également reflété à l'article 28, qui énumère les obligations du responsable du traitement lorsqu'il recrute un sous-traitant.

9. Le principe de responsabilité s'adresse directement au responsable du traitement. Toutefois, certaines règles plus spécifiques s'adressent à la fois aux responsables du traitement et aux sous-traitants; c'est notamment le cas des règles applicables aux autorités de contrôle prévues à l'article 58. Tant les responsables du traitement que les sous-traitants peuvent se voir infliger des amendes en cas de non-respect des obligations imposées par le RGPD qui les concernent et tous deux rendent compte

[3] Avis 3/2010 du groupe de travail «Article 29» sur le principe de responsabilité, adopté le 13 juillet 2010, 00062/10/FR, WP 173.
[4] Considérant 74 du RGPD.

directement aux autorités de contrôle en vertu des obligations de tenir à jour et de fournir les documents appropriés sur demande, de coopérer aux enquêtes et de se conformer aux injonctions administratives. Dans le même temps, il convient de rappeler que les sous-traitants doivent toujours se conformer aux instructions du responsable du traitement et agir uniquement selon celles-ci.

10. Le principe de responsabilité, ainsi que les autres règles plus spécifiques sur la manière de se conformer au RGPD et sur la répartition des responsabilités, impose donc de définir les différents rôles de plusieurs acteurs qui interviennent dans une activité de traitement de données à caractère personnel.

11. À titre d'observation générale concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, il convient de relever que ces notions n'ont pas été modifiées par rapport à la directive 95/46/CE et que, dans l'ensemble, les critères de répartition des différents rôles demeurent inchangés.

12. Les notions de responsable du traitement et de sous-traitant sont des concepts *fonctionnels*: ils visent à répartir les responsabilités en fonction des rôles réels des parties[5]. Cela implique que le statut juridique d'un acteur en tant que «responsable du traitement» ou «sous-traitant» doit, en principe, être déterminé par ses activités réelles dans un cas particulier, plutôt que par la désignation formelle d'un acteur en tant que «responsable du traitement» ou «sous-traitant» (par exemple, dans le cadre d'un contrat)[6]. En d'autres termes, la répartition des rôles devrait généralement résulter d'une analyse des éléments factuels ou des circonstances de l'espèce et, en tant que telle, elle n'est pas négociable.

13. Les notions de «responsable du traitement» et de «sous-traitant» sont également des notions *autonomes* en ce sens que, bien que des sources juridiques externes puissent contribuer à déterminer qui est un responsable du traitement, elles doivent être principalement interprétées conformément à la législation de l'Union en matière de protection des données. La notion de responsable du traitement ne devrait pas être affectée par d'autres concepts – parfois en conflit avec elle ou empiétant sur elle – utilisés dans d'autres domaines du droit, tels que le créateur ou le titulaire d'un droit en matière de propriété intellectuelle ou de droit de la concurrence.

14. L'objectif sous-jacent de l'attribution du rôle de responsable du traitement étant de garantir la responsabilité et la protection effective et complète des données à caractère personnel, la notion de «responsable du traitement» devrait être interprétée de manière suffisamment large, en privilégiant autant que possible une protection effective et complète des personnes concernées[7] de manière à garantir le plein effet de la législation de l'UE en matière de protection des données, à éviter des lacunes et à empêcher le contournement éventuel des règles, tout en ne réduisant pas le rôle du sous-traitant.

[5] Avis 1/2010 du groupe de travail «Article 29», WP 169, p. 9.

[6] Voir aussi les conclusions de l'avocat général Mengozzi dans l'affaire *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:57, point 68 («*Aux fins de la détermination du "responsable du traitement" au sens de la directive 95/46, j'incline à considérer [...] qu'un formalisme excessif permettrait de contourner facilement les dispositions de la directive 95/46 et que, par conséquent, il y a lieu de se fonder sur une analyse plus factuelle que formelle [...]*»).

[7] CJUE, affaire C-131/12, Google Spain SL et Google Inc./Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, arrêt du 13 mai 2014, point 34; CJUE, affaire C-210/16, Wirtschaftsakademie Schleswig-Holstein, arrêt du 5 juin 2018, point 28; CJUE, affaire C-40/17, Fashion ID GmbH & Co.KG/Verbraucherzentrale NRW eV, arrêt du 29 juillet 2019, point 66.

2 DÉFINITION DU RESPONSABLE DU TRAITEMENT

2.1 Définition du responsable du traitement

15. Le responsable du traitement est défini à l'article 4, paragraphe 7, du RGPD comme étant

> «***la personne physique ou morale, l'autorité publique, le service ou un autre organisme*** *qui,* ***seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement****; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être* ***prévus par le droit de l'Union ou par le droit d'un État membre****»*.

16. La définition du «responsable du traitement» se compose de cinq éléments principaux, qui seront analysés séparément dans les présentes lignes directrices. Ces éléments sont les suivants:

- «la personne physique ou morale, l'autorité publique, le service ou un autre organisme»
- «détermine»
- «seul ou conjointement avec d'autres»
- «les finalités et les moyens»
- «du traitement».

2.1.1 «La personne physique ou morale, l'autorité publique, le service ou un autre organisme»

17. Le premier élément se rapporte au type d'entité qui peut être responsable du traitement. Selon le RGPD, un responsable du traitement peut être «*une personne physique ou morale, une autorité publique, un service ou un autre organisme*». Cela signifie qu'il n'existe, en principe, pas de limitation quant au type d'entité susceptible d'assumer le rôle de responsable du traitement. Il peut s'agir d'une organisation, mais également d'un individu ou d'un groupe d'individus[8]. Toutefois, dans la pratique, c'est généralement l'organisation en tant que telle, et non une personne au sein de celle-ci (comme le directeur général, un salarié ou un membre du conseil d'administration), qui agit en tant que responsable du traitement au sens du RGPD. S'agissant du traitement de données au sein d'un groupe d'entreprises, il convient d'accorder une attention particulière à la question de savoir si un établissement peut agir comme responsable du traitement ou comme sous-traitant, par exemple lors du traitement de données pour le compte de la société mère.

18. Parfois, des entreprises et des organismes publics chargent une personne particulière de la mise en œuvre du traitement. Même si une personne physique particulière est désignée pour veiller au respect des règles en matière de protection des données, cette personne ne sera pas le responsable du traitement mais agira pour le compte de l'entité juridique (entreprise ou organisme public) qui, en sa qualité de responsable du traitement, sera responsable en dernier ressort en cas de violation des règles. Dans le même ordre d'idées, même si un service particulier ou une unité particulière d'une organisation assume la responsabilité opérationnelle de veiller à la conformité de certaines activités

[8] À titre d'exemple, dans son arrêt dans l'affaire *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, point 75, la Cour de justice a jugé qu'une communauté religieuse de témoins de Jéhovah a agi comme un responsable du traitement conjointement avec ses membres individuels. Arrêt dans l'affaire *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, point 75.

de traitement, cela ne signifie pas pour autant que ce service ou cette unité (plutôt que l'organisation dans son ensemble) devient le responsable du traitement.

Exemple:

Le service marketing de l'entreprise ABC lance une campagne publicitaire en vue de promouvoir les produits d'ABC. Le service marketing décide de la nature de la campagne, des moyens à utiliser (courrier électronique, réseaux sociaux,...), des clients à cibler et des données utilisées pour que la campagne soit la plus efficace possible. Même si le service du marketing a agi en disposant d'une autonomie considérable, l'entreprise ABC sera en principe considérée comme le responsable du traitement, étant donné que la campagne publicitaire est lancée par l'entreprise et a lieu dans le cadre de ses activités commerciales et de ses objectifs.

19. En principe, tout traitement de données à caractère personnel effectué par des employés dans le cadre des activités d'une organisation peut être réputé avoir lieu sous le contrôle de celle-ci[9]. Cependant, dans des circonstances exceptionnelles, il peut arriver qu'un employé décide d'utiliser des données à caractère personnel à ses propres fins, outrepassant ainsi de manière illicite l'autorité qui lui a été confiée (par exemple, pour créer sa propre entreprise ou dans un but similaire). Il incombe donc à l'organisation, en sa qualité de responsable du traitement, de s'assurer qu'il existe des mesures techniques et organisationnelles appropriées, y compris, par exemple, une formation et une information du personnel, pour garantir le respect du RGPD[10].

2.1.2 «Détermine»

20. Le deuxième élément qui définit la notion de responsable du traitement fait référence à l'*influence* du responsable du traitement sur le traitement par l'*exercice d'un pouvoir décisionnel*. Un responsable du traitement est un organisme qui *décide* de certains éléments essentiels du traitement. Cette responsabilité peut être définie par la loi ou découler d'une analyse des éléments ou circonstances factuels de l'espèce. Il convient d'étudier les traitements spécifiques en question et de comprendre qui les détermine en examinant d'abord les questions suivantes: «*pourquoi ce traitement est-il effectué?*» et «*qui a décidé que le traitement devait avoir lieu pour une finalité particulière?*».

Circonstances à l'origine du contrôle

21. La notion de responsable du traitement étant une notion fonctionnelle, elle repose donc sur une **analyse factuelle plutôt que formelle**. Afin de faciliter cette analyse, certaines règles générales et hypothèses pratiques peuvent être utilisées pour guider et simplifier le processus. Dans la plupart des cas, l'«organe qui détermine» peut être aisément et clairement identifié par référence à certaines circonstances juridiques et/ou factuelles dont on peut normalement déduire une «influence», à moins que d'autres éléments n'indiquent le contraire. On distingue deux types de situations: 1) le contrôle découlant de *dispositions légales* et 2) le contrôle découlant d'une *influence factuelle*.

1) *Contrôle découlant de dispositions légales*

22. Dans certains cas, le contrôle peut être déduit d'une compétence juridique explicite, par exemple lorsque le responsable du traitement est désigné ou lorsque les critères spécifiques applicables à sa

[9] Les employés qui ont accès à des données à caractère personnel au sein d'une organisation ne sont généralement pas considérés comme des «responsables du traitement» ou comme des «sous-traitants», mais plutôt comme des «personnes agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant» au sens de l'article 29 du RGPD.
[10] Article 24, paragraphe 1, du RGPD.

nomination sont déterminés par le droit de l'Union ou par le droit national. En effet, l'article 4, paragraphe 7, dispose que «*lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre*». Alors que l'article 4, paragraphe 7, ne fait référence qu'au «responsable du traitement» au singulier, le comité européen de la protection des données est d'avis que le droit de l'Union ou le droit d'un État membre peut aussi désigner plus d'un responsable du traitement, voire des responsables conjoints du traitement.

23. Lorsque le responsable du traitement est spécifiquement identifié par la loi, cette désignation est déterminante pour définir qui agit en tant que responsable du traitement. Cela présuppose que le législateur a désigné comme responsable du traitement l'entité qui est véritablement en mesure d'exercer le contrôle. Dans certains pays, le droit national prévoit que les autorités publiques sont responsables du traitement des données à caractère personnel dans le cadre de leurs fonctions.

24. Toutefois, plus fréquemment, plutôt que de désigner directement le responsable du traitement ou de définir les critères applicables à sa désignation, la législation confiera une mission ou imposera à quelqu'un l'obligation de collecter et de traiter certaines données. Dans ces cas, la finalité du traitement est souvent déterminée par la loi. Le responsable du traitement sera normalement celui désigné par la loi en vue de la réalisation de cette finalité, de cette mission de service public. Ce serait, par exemple, le cas lorsqu'une entité chargée de certaines missions de service public (comme la sécurité sociale) qui ne peuvent être réalisées sans collecter au moins certaines données à caractère personnel, crée une base de données ou un registre afin d'exécuter lesdites missions. En pareil cas, la loi désigne, quoique indirectement, le responsable du traitement. Plus généralement, la loi peut aussi imposer à des entités publiques ou privées l'obligation de conserver ou de fournir certaines données. Ces entités seront alors normalement considérées comme des responsables du traitement pour le traitement nécessaire à l'exécution de cette obligation.

Exemple: dispositions légales

Le droit national du pays A impose aux autorités municipales l'obligation de fournir des prestations sociales, tels que des versements mensuels aux citoyens en fonction de leur situation financière. Pour effectuer ces paiements, les autorités municipales doivent collecter et traiter les données relatives à la situation financière des demandeurs. Bien que la loi ne prévoie pas expressément que les autorités municipales sont les responsables de ce traitement, cela découle implicitement des dispositions légales.

2) *Contrôle découlant d'une influence factuelle*

25. En l'absence de contrôle découlant de dispositions légales, la désignation d'une partie comme responsable du traitement doit être établie en se fondant sur une appréciation des circonstances factuelles dans lesquelles s'inscrit le traitement. Toutes les circonstances factuelles pertinentes doivent être prises en considération pour déterminer si une entité donnée exerce une influence déterminante sur le traitement de données à caractère personnel en question.

26. La nécessité d'une appréciation factuelle signifie également que le rôle du responsable du traitement ne découle pas de la nature de l'entité qui traite les données, mais de ses activités concrètes dans un contexte précis. En d'autres termes, la même entité peut agir à la fois comme responsable du traitement pour certaines opérations de traitement et comme sous-traitant pour d'autres, et la qualité de responsable du traitement ou de sous-traitant doit être appréciée au regard de chaque activité spécifique de traitement de données.

27. Dans la pratique, certaines activités de traitement peuvent être considérées comme étant naturellement associées au rôle ou aux activités d'une entité, ce qui implique finalement des responsabilités en termes de protection des données. Cela peut être dû à des dispositions légales plus générales ou à une pratique juridique établie dans différents domaines (droit civil, droit commercial, droit du travail, etc.). Dans ce cas, les rôles traditionnels existants et l'expertise professionnelle impliquant normalement une certaine responsabilité contribueront à identifier le responsable du traitement, par exemple: un employeur à l'égard du traitement de données à caractère personnel de son personnel, un éditeur traitant les données à caractère personnel de ses abonnés ou une association traitant les données à caractère personnel de ses membres ou de ses contributeurs. Lorsqu'une entité procède au traitement de données à caractère personnel dans le cadre de son interaction avec ses propres employés, clients ou membres, c'est généralement elle qui déterminera les finalités et les moyens du traitement et agira donc comme responsable du traitement au sens du RGPD.

Exemple: cabinets d'avocats

L'entreprise ABC mandate un cabinet d'avocats pour la représenter dans un litige. Pour mener à bien cette mission, le cabinet d'avocats doit traiter les données à caractère personnel relatives à l'affaire. Les raisons qui régissent le traitement des données à caractère personnel sont le mandat du cabinet d'avocats de représenter son client en justice. Ce mandat ne vise toutefois pas spécifiquement le traitement de données à caractère personnel. Le cabinet d'avocats agit avec un degré considérable d'indépendance, par exemple pour décider quelles informations doivent être utilisées et comment et l'entreprise cliente n'a pas donné d'instructions concernant le traitement des données à caractère personnel. Le traitement effectué par le cabinet d'avocats pour remplir sa mission de représentant légal de l'entreprise est donc lié au rôle fonctionnel du cabinet, de sorte que celui-ci doit être considéré comme étant le responsable de ce traitement.

Exemple: opérateurs de télécommunications[11]

La fourniture d'un service de communications électroniques, tel qu'un service de courrier électronique, implique le traitement de données à caractère personnel. Le fournisseur de ces services sera normalement considéré comme le responsable du traitement des données à caractère personnel nécessaires au fonctionnement du service proprement dit (par exemple, les données relatives au trafic et à la facturation). Si l'unique but et rôle du fournisseur de services sont de permettre la transmission de messages électroniques, le fournisseur ne sera pas considéré comme le responsable du traitement des données à caractère personnel contenues dans le message proprement dit. Normalement, en ce qui concerne les données à caractère personnel contenues dans le message, le responsable du traitement sera la personne dont émane le message et non le fournisseur du service de transmission.

28. Très souvent, un examen des clauses contractuelles liant les différentes parties concernées peut faciliter la détermination de la ou des parties agissant en qualité de responsable du traitement. Même si un contrat ne précise pas qui est le responsable du traitement, il peut contenir suffisamment d'éléments pour déduire qui exerce un rôle décisionnel en ce qui concerne les finalités et les moyens du traitement. Il peut également arriver que le contrat mentionne explicitement l'identité du responsable du traitement. S'il n'existe aucune raison de douter que cela reflète fidèlement la réalité, rien ne s'oppose à ce que les termes du contrat soient respectés. Toutefois, les clauses contractuelles

[11] Le comité européen de la protection des données estime que cet exemple, qui figurait précédemment au considérant 47 de la directive 95/46/CE, reste pertinent dans le cadre du RGPD.

ne sont pas toujours déterminantes, étant donné que cela permettrait aux parties de répartir la responsabilité comme elles l'entendent. Il n'est possible ni de devenir responsable du traitement ni d'échapper aux obligations du responsable du traitement simplement en formulant le contrat d'une certaine manière alors que les circonstances factuelles indiquent autre chose.

29. Si une partie décide pourquoi et comment des données à caractère personnel sont traitées, cette partie sera responsable du traitement, quand bien même le contrat indique qu'il s'agit d'un sous-traitant. De même, ce n'est pas parce qu'un contrat commercial utilise le terme «sous-traitant» qu'une entité doit être considérée comme un sous-traitant au sens de la législation en matière de protection des données[12].

30. Conformément à l'approche factuelle, le terme «détermine» signifie que l'entité qui exerce effectivement une influence déterminante sur les finalités et les moyens du traitement est le responsable du traitement. Normalement, un accord de sous-traitance établit qui est la partie qui détermine (responsable du traitement) et qui est la partie qui reçoit les instructions (sous-traitant). Même si le sous-traitant propose un service précisément défini au préalable, le responsable du traitement doit recevoir une description détaillée du service et prendre la décision finale d'approuver activement la manière dont le traitement est effectué et demander des changements, le cas échéant. Par ailleurs, le sous-traitant ne peut pas modifier, à un stade ultérieur, les éléments essentiels du traitement sans le consentement du responsable du traitement.

Exemple: service standardisé de stockage en nuage

Un important fournisseur d'espace de stockage en nuage offre à ses clients la possibilité de stocker de grands volumes de données à caractère personnel. Le service est totalement standardisé, les clients n'ayant que peu ou pas de possibilité de le personnaliser. Les conditions contractuelles sont fixées et rédigées unilatéralement par le fournisseur des services informatiques en nuage et sont soumises au client selon le principe «à prendre ou à laisser». L'entreprise X décide de recourir au fournisseur de services informatiques en nuage pour stocker les données à caractère personnel de ses clients. L'entreprise X sera toujours considérée comme responsable du traitement, étant donné qu'elle a décidé de faire appel à ce fournisseur particulier de services de stockage en nuage pour traiter des données à caractère personnel pour ses finalités. Dans la mesure où le fournisseur de services en nuage ne traite pas les données à caractère personnel à ses propres fins et conserve les données uniquement pour le compte de ses clients et selon les instructions, ce fournisseur sera considéré comme un sous-traitant.

2.1.3 «Seul ou conjointement avec d'autres»

31. L'article 4, paragraphe 7, reconnaît que les «finalités et les moyens» du traitement peuvent être déterminés par plus d'un acteur. Il précise que le responsable du traitement est l'acteur qui, «seul ou conjointement avec d'autres», détermine les finalités et les moyens du traitement. Cela signifie que plusieurs entités différentes peuvent être responsables du même traitement, chacune d'entre elles étant alors soumise aux dispositions applicables en matière de protection des données. En conséquence, une organisation peut toujours être responsable du traitement, même si elle ne prend pas toutes les décisions concernant les finalités et les moyens. Les critères applicables à la

[12] Voir, par exemple, groupe de travail «Article 29», avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), adopté le 22 novembre 2006, WP 128, p. 11.

responsabilité conjointe et la mesure dans laquelle deux ou plusieurs acteurs exercent conjointement le contrôle peuvent revêtir différentes formes, comme on le verra plus avant[13].

2.1.4 «Les finalités et les moyens»

32. Le quatrième élément de la définition du responsable du traitement concerne l'objet de son influence, à savoir la détermination des «finalités et des moyens» du traitement. Il constitue la partie substantielle de la notion de responsable du traitement, c'est-à-dire ce qu'une partie devrait déterminer pour être considérée comme un responsable du traitement.

33. Les dictionnaires définissent la «finalité» comme «un résultat attendu qui est prévu ou qui oriente les actions planifiées» et les «moyens» comme «la manière dont un résultat est obtenu ou un objectif est atteint».

34. Le RGPD dispose que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités. La détermination des «finalités» du traitement et des «moyens» pour les atteindre revêt donc une importance particulière.

35. La détermination des finalités et des moyens revient à décider respectivement du «pourquoi» et du «comment» du traitement:[14] pour une opération de traitement particulière, le responsable du traitement est l'acteur qui a déterminé la *raison* pour laquelle le traitement a lieu (c'est-à-dire «à quelles fins» ou «pourquoi») et *comment* cet objectif sera atteint (c'est-à-dire quels moyens doivent être mis en œuvre pour atteindre l'objectif). Une personne physique ou morale qui exerce cette influence sur le traitement de données à caractère personnel participe ainsi à la détermination des finalités et des moyens du traitement en question, conformément à la définition énoncée à l'article 4, paragraphe 7, du RGPD[15].

36. Le responsable du traitement doit décider à la fois des finalités et des moyens du traitement, comme indiqué plus haut. Par conséquent, le responsable du traitement ne peut pas se limiter à déterminer uniquement la finalité. Il doit également prendre des décisions concernant les moyens du traitement. À l'inverse, la partie qui agit comme sous-traitant ne peut jamais déterminer la finalité du traitement.

37. Dans la pratique, si un responsable du traitement recrute un sous-traitant pour effectuer le traitement pour son compte, cela veut souvent dire que le sous-traitant sera en mesure de prendre lui-même certaines décisions quant à la manière d'effectuer le traitement. Le comité européen de la protection des données reconnaît que le sous-traitant peut disposer d'une certaine marge de manœuvre lui permettant de prendre certaines décisions concernant le traitement. Dans cette optique, il convient de fournir des orientations sur le **degré d'influence** que devrait impliquer la qualification d'une entité comme responsable du traitement sur le «pourquoi» et le «comment» du traitement, ainsi que sur la mesure dans laquelle un sous-traitant peut prendre ses propres décisions.

38. Lorsqu'une entité détermine clairement les finalités et les moyens, en confiant à une autre entité des activités de traitement correspondant à l'exécution de ses instructions précises, la situation est simple et il ne fait aucun doute que la seconde entité doit être considérée comme un sous-traitant et la première comme le responsable du traitement.

---

[13] Voir partie I, section 3 («Définition des responsables conjoints du traitement»).

[14] Voir aussi les conclusions de l'avocat général Bot dans l'affaire *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, point 46.

[15] Arrêt dans l'affaire *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, point 68.

Moyens essentiels ou non essentiels

39. La question est de savoir où tracer la frontière entre les décisions qui sont réservées au responsable du traitement et celles qui peuvent être laissées à la discrétion du sous-traitant. Il est évident que les décisions relatives à la finalité du traitement doivent toujours incomber au responsable du traitement.

40. En ce qui concerne la détermination des moyens, une distinction peut être faite entre les moyens essentiels et non essentiels. Traditionnellement, les «moyens essentiels» sont intrinsèquement réservés au responsable du traitement. Si les moyens non essentiels peuvent également être déterminés par le sous-traitant, les moyens essentiels doivent être décidés par le responsable du traitement. On entend par «moyens essentiels» ceux qui sont étroitement liés à la finalité et à la portée du traitement, tels que le type de données à caractère personnel qui sont traitées («*quelles données sont traitées?*»), la durée du traitement («*pendant combien de temps sont-elles traitées?*»), les catégories de destinataires («*qui aura accès aux données?*») et les catégories de personnes concernées («*à qui appartiennent les données à caractère personnel traitées?*»). Outre la finalité du traitement, les moyens essentiels sont aussi étroitement liés à la question de savoir si le traitement est licite, nécessaire et proportionné. Les «moyens non essentiels» concernent des aspects plus pratiques de la mise en œuvre, tels que le choix d'un type particulier de matériel ou de logiciel ou les mesures de sécurité concrètes qui peuvent être laissées à la discrétion du sous-traitant.

Exemple: administration des salaires

L'employeur A fait appel à une autre entreprise pour administrer le paiement de salaires de ses employés. L'employeur A donne des instructions claires concernant les personnes à payer, les montants, la date, la banque, la durée de conservation des données, les données à communiquer à l'administration fiscale, etc. Dans ce cas, le traitement des données est effectué pour la finalité de l'entreprise A, à savoir le paiement des salaires à ses employés, et l'administrateur des salaires ne peut utiliser les données pour aucune finalité propre. La manière dont l'administrateur des salaires doit effectuer le traitement est, en substance, clairement et strictement définie. Néanmoins, l'administrateur des salaires peut arrêter certaines modalités du traitement, telles que le logiciel à utiliser, la manière de donner accès aux données au sein de son organisation, etc. Cela ne modifie pas son rôle de sous-traitant, tant que l'administration ne va pas à l'encontre ou au-delà des instructions données par l'entreprise A.

Exemple: paiements bancaires

Dans le cadre des instructions données par l'employeur A, l'administrateur des salaires transmet des informations à la banque B de sorte qu'elle puisse procéder au paiement effectif des employés de l'employeur A. Cette activité inclut le traitement de données à caractère personnel par la banque B, qu'elle effectue aux fins de l'exercice d'une activité bancaire. Dans le cadre de cette activité, la banque décide, sans en référer à l'employeur A, des données qui doivent être traitées pour fournir le service, de la durée de conservation des données, etc. L'employeur A n'a aucune influence sur la finalité et les moyens du traitement des données par la banque B. La banque B doit donc être considérée comme le responsable de ce traitement et la transmission des données à caractère personnel par l'administrateur des salaires doit être considérée comme une communication d'informations entre deux responsables du traitement, de l'employeur A à la banque B.

Exemple: comptables

L'employeur A engage également le cabinet comptable C afin qu'il effectue des audits de sa comptabilité et transfère des données sur les transactions financières (y compris des données à caractère personnel) à C. Le cabinet comptable C traite ces données sans instructions détaillées de A. Le cabinet comptable C décide seul, conformément aux dispositions légales réglementant les activités d'audit réalisées par C, que les données qu'il collecte ne seront traitées qu'aux fins de l'audit de A et il détermine les données dont il a besoin, les catégories de personnes qui doivent être enregistrées, la durée de conservation des données et les moyens techniques à utiliser. Dans ces conditions, le cabinet comptable C doit être considéré comme un responsable du traitement à part entière lorsqu'il fournit ses services d'audit à A. Cependant, cette appréciation peut varier en fonction des instructions données par A. Si la législation n'impose pas d'obligations spécifiques au cabinet comptable et que l'entreprise cliente fournit des instructions très détaillées sur le traitement, le cabinet comptable agit effectivement comme un sous-traitant. Une distinction pourrait être établie entre le cas où, conformément à la législation réglementant cette profession, le traitement est réalisé dans le cadre de l'activité de base du cabinet comptable et le cas où le traitement est une tâche auxiliaire plus restreinte, réalisée dans le cadre de l'activité de l'entreprise cliente.

Exemple: services d'hébergement

L'employeur A fait appel au service d'hébergement H pour stocker des données cryptées sur ses serveurs. Le service d'hébergement H ne détermine pas si les données qu'il héberge sont des données à caractère personnel et ne procède à aucun autre traitement que le stockage sur ses serveurs. Le stockage étant un exemple d'activité de traitement de données à caractère personnel, le service d'hébergement H traite des données à caractère personnel pour le compte de l'employeur A et est donc un sous-traitant. L'employeur A doit fournir à H les instructions nécessaires et un accord de traitement de données conforme à l'article 28 doit être conclu, imposant à H de mettre en œuvre des mesures de sécurité techniques et organisationnelles. H doit aider A à faire en sorte que les mesures de sécurité nécessaires soient prises et lui notifie toute violation de données à caractère personnel.

41. Bien que les décisions relatives à des moyens non essentiels puissent être laissées à la discrétion du sous-traitant, le responsable du traitement doit toujours stipuler certains éléments dans l'accord de sous-traitance, tels que, en ce qui concerne l'exigence de sécurité, l'instruction de prendre toutes les mesures requises conformément à l'article 32 du RGPD. L'accord doit également indiquer que le sous-traitant doit aider le responsable du traitement à garantir le respect de l'article 32, par exemple. En tout état de cause, le responsable du traitement reste responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que le traitement est effectué conformément au règlement (article 24) et être en mesure de le démontrer. Ce faisant, le responsable du traitement doit tenir compte de la nature, de l'étendue, du contexte et des finalités du traitement ainsi que des risques qu'il comporte pour les droits et les libertés des personnes physiques. C'est la raison pour laquelle le responsable du traitement doit être pleinement informé des moyens utilisés, de sorte qu'il puisse prendre une décision éclairée à cet égard. Pour que le responsable du traitement soit à même de démontrer la licéité du traitement, il est recommandé de préciser, à tout le moins, les mesures techniques et organisationnelles nécessaires dans le contrat ou dans tout autre instrument juridiquement contraignant conclu entre le responsable du traitement et le sous-traitant.

Exemple: centre d'appels

L'entreprise X décide de sous-traiter une partie de ses services à la clientèle à un centre d'appels. Le centre d'appels reçoit des données identifiables sur les achats des clients ainsi que des coordonnées de contact. Il utilise son propre logiciel et sa propre infrastructure informatique pour gérer les données à caractère personnel concernant les clients de l'entreprise X. L'entreprise X signe un accord de sous-traitance avec le fournisseur du centre d'appels conformément à l'article 28 du RGPD, après avoir vérifié que les mesures de sécurité techniques et organisationnelles proposées par le centre d'appels sont appropriées au regard des risques en cause et que le centre d'appels ne traitera les données à caractère personnel que pour les finalités de l'entreprise X et selon ses instructions. L'entreprise X ne fournit aucune autre instruction au centre d'appels quant au logiciel spécifique à utiliser et aucune instruction détaillée sur les mesures de sécurité spécifiques à mettre en œuvre. Dans cet exemple, l'entreprise X reste le responsable du traitement, malgré le fait que le centre d'appels a déterminé certains moyens non essentiels du traitement.

2.1.5 «Du traitement»

42. Les finalités et les moyens déterminés par le responsable du traitement doivent concerner le «traitement de données à caractère personnel». L'article 4, paragraphe 2, du RGPD définit le traitement de données à caractère personnel comme étant «*toute opération ou ensemble d'opérations appliquées à des données ou des ensembles de données à caractère personnel*». En conséquence, la notion de responsable du traitement peut être associée à une seule opération ou à plusieurs opérations de traitement. Dans la pratique, cela peut signifier que le contrôle exercé par une entité particulière peut s'étendre à l'ensemble du traitement en cause, mais qu'il peut aussi se limiter à une étape particulière du traitement[16].

43. Dans la pratique, le traitement de données à caractère personnel impliquant plusieurs acteurs peut être subdivisé en plusieurs opérations de traitement plus petites dont on pourrait considérer que chaque acteur détermine la finalité et les moyens individuellement. D'autre part, une séquence ou un ensemble d'opérations de traitement impliquant plusieurs acteurs peuvent aussi avoir lieu pour la ou les mêmes finalités, auquel cas il est possible que le traitement fasse intervenir un ou plusieurs responsables conjoints du traitement. En d'autres termes, il est possible qu'au niveau «micro», les différentes opérations de traitement de la chaîne semblent dissociées, chacune d'entre elles pouvant avoir une finalité différente. Toutefois, il convient de vérifier à nouveau si au niveau «macro», ces opérations de traitement ne devraient pas être considérées comme un «ensemble d'opérations» poursuivant un objectif conjoint et utilisant des moyens définis conjointement.

44. Quiconque décide de traiter des données doit examiner si elles comprennent des données à caractère personnel et, dans l'affirmative, quelles sont les obligations prévues par le RGPD. Un acteur sera considéré comme un «responsable du traitement», même s'il ne cible pas délibérément des données à caractère personnel en tant que telles ou s'il a estimé à tort qu'il ne traite pas des données à caractère personnel.

[16] Arrêt dans l'affaire *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, point 74: «*Il s'ensuit, ainsi que l'a relevé, en substance, M. l'avocat général [...], qu'une personne physique ou morale apparaît uniquement pouvoir être responsable, au sens de l'article 2, sous d), de la directive 95/46, conjointement avec d'autres, des opérations de traitement de données à caractère personnel dont elle détermine conjointement les finalités et les moyens. En revanche [...], cette personne physique ou morale ne saurait être considérée comme étant responsable, au sens de ladite disposition, des opérations antérieures ou postérieures de la chaîne de traitement dont elle ne détermine ni les finalités ni les moyens».*

45. Il n'est pas nécessaire que le responsable du traitement ait réellement accès aux données faisant l'objet du traitement[17]. Une entité qui sous-traite une activité de traitement et, ce faisant, a une influence déterminante sur la finalité et les moyens (essentiels) du traitement (par exemple en adaptant les paramètres d'un service de manière à ce qu'il influence le choix des personnes dont les données seront traitées), doit être considérée comme le responsable du traitement, même si elle n'aura jamais réellement accès aux données.

Exemple: étude de marché 1

L'entreprise ABC souhaite savoir quels sont les types de consommateurs les plus susceptibles d'être intéressés par ses produits et fait appel à un prestataire de services, XYZ, pour obtenir les informations pertinentes.

L'entreprise ABC donne des instructions à XYZ concernant le type d'informations qui l'intéresse et fournit une liste de questions à poser aux participants à l'étude de marché.

L'entreprise ABC ne reçoit de XYZ que des informations statistiques (par exemple, l'identification des tendances des consommateurs par région) et n'a pas accès aux données à caractère personnel proprement dites. Néanmoins, l'entreprise ABC a décidé que le traitement devait avoir lieu, qu'il est effectué pour sa finalité et son activité et elle a fourni à XYZ des instructions détaillées sur les informations à collecter. L'entreprise ABC doit donc toujours être considérée comme le responsable du traitement de données à caractère personnel destiné à fournir les informations qu'elle a demandées. XYZ ne peut traiter les données que pour la finalité déterminée par l'entreprise ABC et selon ses instructions détaillées et doit donc être considérée comme un sous-traitant.

Exemple: étude de marché 2

L'entreprise ABC souhaite savoir quels sont les types de consommateurs les plus susceptibles d'être intéressés par ses produits. Le prestataire de services XYZ est un bureau d'études de marché qui a recueilli des informations sur les intérêts des consommateurs au moyen de divers questionnaires portant sur un large éventail de produits et de services. Le prestataire de services XYZ a collecté et analysé ces données de manière indépendante, selon sa propre méthodologie, sans recevoir aucune instruction de l'entreprise ABC. Pour répondre à la demande de l'entreprise ABC, le prestataire de services XYZ va générer des informations statistiques, mais sans recevoir aucune autre instruction quant aux données à caractère personnel qu'il devrait traiter ou à la manière de générer ces statistiques. Dans cet exemple, le prestataire de services XYZ agit comme responsable unique du traitement en traitant des données à caractère personnel à des fins d'étude de marché et en déterminant en toute indépendance les moyens pour ce faire. L'entreprise ABC n'a ni rôle ni responsabilité spécifique au titre de la législation sur la protection des données en ce qui concerne ces activités de traitement, étant donné qu'elle reçoit des statistiques anonymisées et n'intervient pas dans la détermination des finalités et des moyens du traitement.

[17] Arrêt dans l'affaire *Wirtschaftsakademie*, C--201/16, ECLI:EU:C:2018:388, point 38.

3 DÉFINITION DES RESPONSABLES CONJOINTS DU TRAITEMENT

3.1 Définition des responsables conjoints du traitement

46. Il peut y avoir des responsables conjoints du traitement lorsque plus d'un acteur intervient dans le traitement.

47. Bien que ce concept ne soit pas nouveau et qu'il figurât déjà dans la directive 95/46/CE, le RGPD, en son article 26, introduit des règles spécifiques pour les responsables conjoints du traitement et établit un cadre pour régir leurs relations. En outre, la Cour de justice de l'Union européenne (CJUE) a apporté des éclaircissements sur cette notion et ses conséquences dans des arrêts récents[18].

48. Comme expliqué plus en détail dans la partie II, section 2, la qualification de responsables conjoints du traitement aura principalement des conséquences sur la répartition des obligations concernant le respect des règles en matière de protection des données et, notamment, les droits des personnes.

49. Dans cette perspective, la section suivante vise à fournir des orientations sur la notion de responsables conjoints du traitement au sens du RGPD et de la jurisprudence de la CJUE afin d'aider les entités à déterminer dans quels cas elles peuvent agir en tant que responsables conjoints du traitement et à appliquer le concept dans la pratique.

3.2 Existence d'une responsabilité conjointe

3.2.1 Considérations générales

50. La définition du responsable du traitement énoncée à l'article 4, paragraphe 7, du RGPD constitue le point de départ pour déterminer l'existence d'une responsabilité conjointe. Les observations contenues dans la présente section sont donc directement liées à celles de la section consacrée à la notion de responsable du traitement et les complètent. Par conséquent, l'appréciation de la responsabilité conjointe devrait refléter celle de la responsabilité «unique» exposée plus haut.

51. L'article 26 du RGPD, qui reprend la définition de l'article 4, paragraphe 7, de ce même règlement, dispose que «*[l]orsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement*». De manière générale, il existe une responsabilité conjointe pour une activité de traitement spécifique lorsque différentes parties déterminent *conjointement* les finalités et les moyens de cette activité de traitement. Dès lors, pour apprécier l'existence de responsables conjoints du traitement, il convient d'examiner si la détermination des finalités et des moyens qui caractérisent un responsable du traitement est décidée par plus d'une partie. Le terme «conjointement» doit être interprété comme signifiant «ensemble» ou «pas seul», sous différentes formes et combinaisons, comme expliqué ci-après.

52. La responsabilité conjointe du traitement devrait être appréciée sur la base d'une analyse factuelle plutôt que formelle de l'influence réelle exercée sur les finalités et les moyens du traitement. Toutes

[18] Voir, notamment, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu/Jehovan todistajat – uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV (*C-40/17). Il est à noter que bien que ces arrêts aient été rendus par la CJUE et portent sur l'interprétation de la notion de «responsables conjoints du traitement» au titre de la directive 95/46/CE, ils restent valides dans le cadre du RGPD, étant donné que les éléments déterminant cette notion dans le RGPD sont les mêmes que dans la directive.

les dispositions existantes ou envisagées devraient être examinées au regard des circonstances factuelles de la relation entre les parties. Un critère purement formel ne serait pas suffisant pour au moins deux raisons: dans certains cas, la désignation formelle d'un responsable conjoint du traitement – prévue par exemple par la loi ou dans un contrat – serait absente; dans d'autres cas, il se peut que la désignation formelle ne reflète pas la réalité des accords, en confiant formellement le rôle de responsable du traitement à une entité qui n'est, en fait, pas en mesure de «déterminer» les finalités et les moyens du traitement.

53. Tous les traitements impliquant plusieurs entités ne donnent pas lieu à une responsabilité conjointe du traitement. Le critère essentiel pour qu'il y ait responsabilité conjointe du traitement est **la participation conjointe de deux entités ou plus dans la détermination des finalités et des moyens** d'un traitement. Plus précisément, la participation conjointe doit englober, d'une part, la détermination des finalités et, de l'autre, la détermination des moyens. Si chacun de ces éléments est déterminé par toutes les entités concernées, celles-ci devraient être considérées comme des responsables conjoints du traitement en question.

3.2.2 Appréciation de la participation conjointe

54. Une participation conjointe à la détermination des finalités et des moyens implique que plus d'une entité exerce une influence déterminante sur la question de savoir si et comment le traitement a lieu. Dans la pratique, une participation conjointe peut revêtir plusieurs formes. Par exemple, la participation conjointe peut prendre la forme d'une **décision commune** prise par deux entités ou plus ou découler de **décisions convergentes** adoptées par deux entités ou plus au sujet des finalités et des moyens essentiels du traitement.

55. Une participation conjointe résultant d'une *décision commune* signifie que les parties décident ensemble, et suppose une intention commune, conformément à l'acception la plus courant du terme «conjointement» mentionné à l'article 26 du RGPD.

Le cas d'une participation conjointe due à des *décisions convergentes* résulte plus particulièrement de la jurisprudence de la CJUE relative à la notion de responsables conjoints du traitement. Des décisions peuvent être considérées comme convergentes au regard des finalités et des moyens **dès lors qu'elles se complètent et sont nécessaires à la réalisation du traitement de sorte qu'elles ont un effet concret sur la détermination des finalités et des moyens du traitement**. Il convient de souligner que la notion de décisions convergentes doit être examinée par rapport aux finalités et aux moyens du traitement et non au regard d'autres aspects de la relation commerciale qui lie les parties[19]. Ainsi, un critère important pour identifier des décisions convergentes dans ce contexte est **le fait que le traitement ne serait pas possible sans la participation des deux parties à la détermination des finalités et des moyens, en ce sens que le traitement par chacune des parties est indissociable de celui de l'autre, c'est-à-dire inextricablement lié**. La situation de responsables conjoints du traitement agissant sur le fondement de décisions convergentes doit toutefois être distinguée de celle d'un sous-traitant, étant donné que ce dernier, bien qu'il participe à l'exécution d'un traitement, ne traite pas les données à ses propres fins, mais effectue le traitement pour le compte du responsable du traitement.

56. Le fait que l'une des parties n'a pas accès aux données à caractère personnel traitées ne suffit pas à exclure une responsabilité conjointe du traitement[20]. À titre d'exemple, dans l'affaire *Jehovah's Witnesses*, la CJUE a estimé qu'une communauté religieuse doit être considérée comme étant

[19] En effet, tous les accords commerciaux impliquent des décisions convergentes dans le cadre du processus aboutissant à la conclusion de l'accord.
[20] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, point 38.

responsable, conjointement avec ses membres prédicateurs, des traitements de données à caractère personnel effectués par ces derniers dans le cadre d'une activité de prédication de porte-à-porte[21]. La CJUE a considéré qu'il n'était pas nécessaire que ladite communauté ait accès aux données ou qu'il devait être établi qu'elle avait donné à ses membres des lignes directrices écrites ou des consignes relativement à ces traitements[22]. La communauté religieuse a participé à la détermination des finalités et des moyens en organisant et en coordonnant les activités de ses membres, ce qui a contribué à la réalisation de l'objectif de la communauté des témoins de Jéhovah[23]. En outre, la communauté avait, de manière générale, connaissance du fait que de tels traitements avaient lieu aux fins de la diffusion de sa foi[24].

57. Il importe également de souligner, comme l'a précisé la CJUE, qu'une entité sera considérée comme un responsable conjoint du traitement avec la ou les autres entités uniquement à l'égard des opérations de traitement pour lesquelles elle détermine, conjointement avec d'autres, les moyens et les finalités dudit traitement, notamment en cas de décisions convergentes. Si l'une de ces entités décide seule des finalités et des moyens des opérations antérieures ou postérieures de la chaîne de traitement, cette entité doit être considérée comme le seul responsable de ce traitement antérieur ou postérieur[25].

58. L'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, la CJUE a précisé que ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce.

3.2.2.1 Finalité(s) déterminée(s) conjointement

59. Il y a responsabilité conjointe du traitement lorsque des entités impliquées dans le même traitement effectuent le traitement à des fins définies conjointement. Tel sera le cas lorsque les entités concernées traitent les données à des fins identiques ou communes.

60. En outre, si les entités ne poursuivent pas la même finalité de traitement, selon la jurisprudence, une responsabilité conjointe du traitement peut également être établie lorsque les entités concernées poursuivent des finalités étroitement liées ou complémentaires. Tel peut être le cas, par exemple, lorsqu'un même traitement apporte un avantage mutuel, à condition que chacune des entités concernées participe à la détermination des finalités et des moyens du traitement pertinent. Toutefois, la notion d'avantage mutuel n'est pas déterminante et ne peut être qu'une indication. Dans l'arrêt *Fashion ID*, par exemple, la CJUE a précisé que l'exploitant d'un site Internet participe à la détermination des finalités (et des moyens) du traitement en intégrant un plug-in social dans un site Internet afin d'optimiser la publicité pour ses produits en les rendant plus visibles sur le réseau social. La CJUE a jugé que les opérations de traitement en cause étaient effectuées dans l'intérêt économique tant de l'exploitant du site Internet que du fournisseur du plug-in social[26].

---

[21] Arrêt dans l'affaire *Témoins de Jéhovah*, C-25/17, ECLI:EU:C:2018:551, point 75.
[22] Ibidem.
[23] Ibidem, point 71.
[24] Ibidem.
[25] Arrêt dans l'affaire *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, point 74: «*En revanche, et sans préjudice d'une éventuelle responsabilité civile prévue par le droit national à cet égard, cette personne physique ou morale ne saurait être considérée comme étant responsable, au sens de ladite disposition, des opérations antérieures ou postérieures de la chaîne de traitement dont elle ne détermine ni les finalités ni les moyens*».
[26] Arrêt dans l'affaire *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, point 80.

61. De même, comme l'a fait observer la CJUE dans l'arrêt *Wirtschaftsakademie*, le traitement de données à caractère personnel au moyen de statistiques établies à partir des visites sur une page fan visent à permettre, d'une part, à Facebook d'améliorer son système de publicité qu'il diffuse à travers son réseau et, d'autre part, à l'administrateur de la page fan d'obtenir des statistiques à des fins de gestion de la promotion de son activité[27]. Dans cette affaire, chaque entité poursuit son propre intérêt, mais les deux parties participent à la détermination des finalités (et des moyens) du traitement des données à caractère personnel des visiteurs de la page fan[28].

62. À cet égard, il importe de souligner que la simple existence d'un avantage mutuel (par exemple commercial) découlant d'une activité de traitement ne donne pas lieu à une responsabilité conjointe de ce traitement. Si l'entité impliquée dans le traitement ne poursuit aucune finalité propre dans le cadre du traitement, mais est simplement rémunérée pour les services rendus, elle agit comme sous-traitant plutôt que comme responsable conjoint du traitement.

3.2.2.2 Moyens déterminés conjointement

63. La responsabilité conjointe du traitement exige également que deux entités ou plus aient exercé une influence sur les moyens du traitement. Cela ne signifie pas que, pour qu'il existe une responsabilité conjointe du traitement, chaque entité concernée doive dans tous les cas déterminer tous les moyens du traitement. En effet, comme l'a précisé la CJUE, différentes entités peuvent intervenir à des étapes différentes du traitement et à des degrés divers. Par conséquent, différents responsables conjoints du traitement peuvent définir les moyens de celui-ci dans une mesure variable, en fonction de celui qui est effectivement en mesure de le faire.

64. Il se peut également que l'une des entités concernées fournisse les moyens du traitement et les mette à disposition pour les activités de traitement de données à caractère personnel effectuées par d'autres entités. L'entité qui décide d'utiliser ces moyens pour que des données à caractère personnel puissent être traitées pour une finalité particulière participe également à la détermination des moyens du traitement.

65. Ce scénario peut notamment se produire dans le cas de plateformes, d'outils standardisés ou d'autres infrastructures qui permettent aux parties de traiter les mêmes données à caractère personnel et qui ont été créés d'une certaine façon par l'une des parties pour être utilisés par d'autres parties, qui peuvent aussi décider de la manière de les créer[29]. L'utilisation d'un système technique existant n'exclut pas une responsabilité conjointe du traitement lorsque les utilisateurs du système peuvent décider du traitement de données à caractère personnel à effectuer dans ce contexte.

66. À titre d'exemple, la CJUE a jugé, dans l'arrêt *Wirtschaftsakademie*, qu'en procédant au paramétrage en fonction de son audience cible ainsi que des objectifs de gestion et de promotion de ses activités, l'administrateur d'une page fan sur Facebook doit être considéré comme participant à la détermination des moyens du traitement de données à caractère personnel relatives aux visiteurs de sa page fan.

67. En outre, le choix d'une entité d'utiliser pour ses propres finalités un outil ou un autre système mis au point par une autre entité, qui permet le traitement de données à caractère personnel, équivaudra probablement à une décision conjointe sur les moyens dudit traitement par ces entités. C'est ce qui

[27] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, point 34.
[28] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, point 39.
[29] Le fournisseur du système peut être un responsable conjoint du traitement si les critères susmentionnés sont remplis, c'est-à-dire si le fournisseur participe à la détermination des finalités et des moyens. À défaut, le fournisseur devrait être considéré comme un sous-traitant.

ressort de l'affaire *Fashion ID*, dans laquelle la CJUE a conclu qu'en insérant sur son site Internet le bouton «j'aime» de Facebook mis à la disposition des gestionnaires de sites Internet par Facebook, Fashion ID avait influé de manière déterminante sur la collecte et la transmission des données à caractère personnel des visiteurs dudit site au profit de Facebook et avait donc déterminé conjointement avec Facebook les moyens de ce traitement[30].

68. Il est important de souligner que **l'utilisation d'un système commun ou d'une infrastructure commune de traitement des données ne conduira pas dans tous les cas à considérer les parties concernées comme des responsables conjoints du traitement**, en particulier lorsque le traitement qu'elles effectuent peut être dissocié et pourrait être effectué par une partie sans l'intervention de l'autre ou lorsque le fournisseur est un sous-traitant qui ne poursuit aucune finalité propre (l'existence d'un simple avantage commercial pour les parties concernées ne suffit pas à considérer celui-ci comme une finalité du traitement).

Exemple: agence de voyages

Une agence de voyages envoie des données à caractère personnel de ses clients à une compagnie aérienne et à une chaîne d'hôtels afin de réserver un voyage à forfait. La compagnie aérienne et l'hôtel confirment la disponibilité des sièges et des chambres demandés. L'agence de voyages émet les documents de voyage et les bons pour ses clients. Chacun des acteurs traite les données pour mener à bien ses propres activités et utilise ses propres moyens. Dans ce cas, l'agence de voyages, la compagnie aérienne et l'hôtel sont trois responsables du traitement différents, qui traitent les données à des fins séparées qui leur sont propres, et il n'y a pas de responsabilité conjointe du traitement.

L'agence de voyages, la chaîne d'hôtels et la compagnie aérienne décident ensuite de participer conjointement à la création d'une plateforme commune sur internet dans le but commun de proposer des voyages à forfait. Elles conviennent des moyens essentiels à utiliser, tels que les données qui seront conservées, comment les réservations seront attribuées et confirmées et qui pourra avoir accès aux informations stockées. En outre, elles décident de partager les données de leurs clients afin de mener des actions de marketing conjointes. Dans ce cas, l'agence de voyages, la compagnie aérienne et la chaîne hôtelière déterminent conjointement pourquoi et comment les données à caractère personnel de leurs clients respectifs sont traitées et elles seront donc les responsables conjoints du traitement pour les opérations de traitement relatives à la plateforme commune de réservation en ligne et les actions de marketing conjointes. Toutefois, chacune d'elles conserverait un contrôle exclusif sur d'autres activités de traitement extérieures à la plateforme commune en ligne.

Exemple: projet de recherche mené par des instituts de recherche

Plusieurs instituts de recherche décident de participer à un projet de recherche spécifique conjoint et d'utiliser à cet effet la plateforme existante de l'un des instituts participants. Chaque institut introduit dans la plateforme les données à caractère personnel qu'il détient déjà aux fins de la recherche conjointe et utilise les données fournies par d'autres par l'intermédiaire de la plateforme pour mener à bien la recherche. Dans ce cas, tous les instituts sont considérés comme des responsables conjoints du traitement des données à caractère personnel qui est effectué en stockant et en divulguant des informations à partir de cette plateforme, puisqu'ils ont décidé ensemble de la finalité du traitement et des moyens à utiliser (la plateforme existante). Chacun des instituts est toutefois un responsable

[30] Arrêt dans l'affaire Fashion ID, C-40/17, ECLI:EU:C:2018:1039, point 79.

distinct pour tout autre traitement susceptible d'être effectué en dehors de la plateforme pour leurs finalités respectives.

Exemple: opération de marketing

Les entreprises A et B ont lancé un produit co-brandé C et veulent organiser un événement pour promouvoir ce produit. À cet effet, elles décident de partager les données issues de leurs bases de données de clients et de clients potentiels respectives et établissent la liste des invités à l'événement sur cette base. Elles conviennent également des modalités d'envoi des invitations à l'événement, de la manière de recueillir des retours d'informations pendant celui-ci et des actions commerciales de suivi. Les entreprises A et B peuvent être considérées comme des responsables conjoints du traitement des données à caractère personnel liées à l'organisation de l'événement promotionnel, étant donné qu'elles décident ensemble de la finalité et des moyens essentiels déterminés conjointement, applicables au traitement des données dans ce contexte.

Exemple: essais cliniques[31]

Un prestataire de soins (le chercheur) et une université (le promoteur) décident de lancer ensemble un essai clinique ayant la même finalité. Ils collaborent à la rédaction du protocole de l'étude (à savoir la finalité, la méthodologie/conception de l'étude, les données à collecter, les critères d'inclusion et d'exclusion des sujets, la réutilisation de la base de données, le cas échéant, etc.). Ils peuvent être considérés comme des responsables conjoints du traitement pour cet essai clinique étant donné qu'ils déterminent et conviennent ensemble de la même finalité et des moyens essentiels du traitement. La collecte de données à caractère personnel provenant du dossier médical du patient aux fins de la recherche doit être distinguée de la conservation et de l'utilisation des mêmes données aux fins des soins prodigués au patient, pour lesquels le prestataire de soins reste le responsable du traitement.

Si le chercheur ne participe pas à la rédaction du protocole (il accepte simplement le protocole déjà établi par le promoteur) et que le protocole n'est conçu que par le promoteur, le chercheur devrait être considéré comme un sous-traitant et le promoteur comme le responsable du traitement dans le cadre de cet essai clinique.

Exemple: chasseurs de têtes

L'entreprise X aide l'entreprise Y à recruter du personnel, grâce à son fameux service à valeur ajoutée «global matchz». L'entreprise X recherche des candidats adéquats aussi bien parmi les CV reçus directement par l'entreprise Y que parmi ceux qui figurent déjà dans sa propre base de données. Cette base de données est créée et gérée par la seule entreprise X. De la sorte, l'entreprise X améliore l'adéquation entre les offres d'emploi et les demandeurs d'emploi et augmente ainsi ses revenus. Bien qu'elles n'aient pas formellement pris ensemble une décision, les entreprises X et Y participent conjointement au traitement dans le but de trouver des candidats adéquats sur la base de décisions convergentes: la décision de créer et de gérer le service «global matchz» pour l'entreprise X et la décision de l'entreprise Y d'enrichir la base de données avec les CV qu'elle reçoit directement. Ces décisions se complètent mutuellement et sont indissociables et nécessaires au traitement consistant

[31] Le comité européen de la protection des données prévoit de fournir des orientations supplémentaires concernant les essais cliniques dans le cadre de ses prochaines lignes directrices concernant le traitement de données à caractère personnel à des fins de recherche scientifique et médicale.

à trouver des candidats adéquats. Par conséquent, dans ce cas particulier, les deux entreprises devraient être considérées comme des responsables conjoints du traitement. Toutefois, l'entreprise X est le seul responsable du traitement nécessaire à la gestion de sa base de données et l'entreprise Y est le seul responsable du traitement ultérieur de recrutement pour sa propre finalité (organisation d'entretiens, conclusion du contrat et gestion des données RH).

Exemple: analyse de données relatives à la santé

L'entreprise ABC, qui développe une application de contrôle de la tension artérielle, et l'entreprise XYZ, qui fournit des applications destinées aux professionnels de la santé, souhaitent toutes deux étudier comment les changements de la tension artérielle peuvent contribuer à prédire certaines maladies. Les deux entreprises décident de lancer un projet conjoint et s'adressent à l'hôpital DEF pour qu'il y participe aussi.

Les données à caractère personnel qui seront traitées dans le cadre de ce projet sont des données que l'entreprise ABC, l'hôpital DEF et l'entreprise XYZ traitent séparément en tant que responsables du traitement individuels. La décision de traiter ces données pour étudier les changements de la tension artérielle est prise conjointement par les trois acteurs. L'entreprise ABC, l'hôpital DEF et l'entreprise XYZ ont déterminé conjointement les finalités du traitement. L'entreprise XYZ prend l'initiative de proposer les moyens essentiels du traitement. L'entreprise ABC et l'hôpital DEF acceptent ces moyens essentiels, après avoir également participé au développement de certaines fonctionnalités de l'application, de sorte qu'ils puissent exploiter suffisamment les résultats. Les trois organisations conviennent donc d'une finalité commune pour le traitement, à savoir l'évaluation de la manière dont les changements de la tension artérielle peuvent contribuer à prédire certaines maladies. Une fois la recherche terminée, l'entreprise ABC, l'hôpital DEF et l'entreprise XYZ peuvent tirer profit de l'évaluation en utilisant ses résultats pour leurs activités respectives. Compte tenu de l'ensemble de ces raisons, elles sont considérées comme des responsables conjoints du traitement pour ce traitement conjoint spécifique.

Si l'entreprise XYZ avait simplement été invitée par les autres à procéder à cette évaluation sans poursuivre ses propres finalités et avait simplement traité les données pour le compte des autres, elle serait considérée comme un sous-traitant, même si elle était chargée de déterminer les moyens non essentiels.

3.2.3 Situations dans lesquelles il n'y a pas de responsabilité conjointe

69. Le fait que plusieurs acteurs participent au même traitement ne signifie pas qu'ils agissent nécessairement en tant que responsables conjoints de ce traitement. Tous les types de partenariat, de coopération ou de collaboration n'impliquent pas que les entités soient des responsables conjoints du traitement, étant donné que cette qualité requiert une analyse au cas par cas de chaque traitement et du rôle précis que joue chaque entité dans chaque traitement. Les exemples ci-dessous illustrent de manière non exhaustive des situations dans lesquelles il n'y a pas de responsabilité conjointe du traitement.

70. Ainsi, l'échange des mêmes données ou ensembles de données entre deux entités sans qu'elles déterminent conjointement les finalités ou les moyens du traitement devrait être considéré comme une communication de données entre responsables de traitement distincts.

Exemple: communication de données relatives au personnel à l'administration fiscale

Une entreprise collecte et traite les données à caractère personnel de ses employés dans le but de gérer les salaires, les assurances maladie, etc. Une loi oblige l'entreprise à transmettre toutes les données relatives aux salaires à l'administration fiscale afin de renforcer le contrôle fiscal.

Dans cet exemple, même si l'entreprise et l'administration fiscale traitent les mêmes données relatives aux salaires, l'absence de finalités et de moyens déterminés conjointement concernant ce traitement aura pour effet que les deux entités seront considérées comme deux responsables distincts du traitement.

71. La responsabilité conjointe du traitement peut également être exclue dans le cas où plusieurs entités utilisent une base de données ou une infrastructure commune, dès lors que chaque entité détermine ses propres finalités de manière indépendante.

Exemple: opérations de marketing au sein d'un groupe d'entreprises utilisant une base de données partagée

Un groupe d'entreprises utilise la même base de données pour la gestion des clients et des clients potentiels. Cette base de données est hébergée sur les serveurs de la société mère, qui est donc un sous-traitant des entreprises en ce qui concerne le stockage des données. Chaque entité du groupe saisit les données de ses propres clients et clients potentiels et traite ces données uniquement pour ses propres finalités. De même, chaque entité décide en toute indépendance de l'accès, des durées de conservation, de la rectification ou de la suppression des données de ses clients et clients potentiels. Les entités ne peuvent ni accéder aux données des autres ni les utiliser. Le simple fait que ces entreprises utilisent une base de données commune du groupe n'implique pas en soi une responsabilité conjointe des traitements. Dans ces circonstances, chaque entreprise est donc un responsable distinct du traitement.

Exemple: responsables du traitement indépendants utilisant une infrastructure commune

L'entreprise XYZ héberge une base de données qu'elle met à la disposition d'autres entreprises afin de traiter et d'héberger les données à caractère personnel de leur personnel. L'entreprise XYZ est un sous-traitant au regard du traitement et de la conservation des données du personnel des autres entreprises, étant donné que ces opérations sont effectuées pour le compte et selon les instructions de ces autres entreprises. En outre, les autres entreprises traitent les données sans que l'entreprise XYZ n'intervienne et pour des finalités qui ne sont absolument pas les mêmes que celles de l'entreprise XYZ.

72. Il peut également arriver que divers acteurs traitent successivement les mêmes données à caractère personnel dans une chaîne d'opérations de traitement, chacun de ces acteurs ayant une finalité et des moyens indépendants dans leur partie de la chaîne. En l'absence d'une participation conjointe à la détermination des finalités et des moyens de la même opération de traitement ou d'un ensemble d'opérations, il y a lieu d'exclure une responsabilité conjointe du traitement et les différents acteurs doivent être considérés comme des responsables du traitement indépendants et successifs.

Exemple: analyse statistique pour une mission d'intérêt public

Une autorité publique (autorité A) a pour mission légale de réaliser des analyses pertinentes et d'élaborer des statistiques sur l'évolution du taux d'emploi dans le pays. Pour ce faire, de nombreuses autres entités publiques sont légalement tenues de communiquer des données spécifiques à l'autorité A. Celle-ci décide d'utiliser un système spécifique pour traiter les données, y compris leur

collecte. Cela signifie également que les autres entités sont tenues d'utiliser ce système pour la communication des données. Dans cet exemple, sans préjudice d'une répartition des rôles prévue par la loi, l'autorité A sera le seul responsable du traitement aux fins des analyses et des statistiques du taux d'emploi traitées dans le système, parce que c'est l'autorité A qui détermine la finalité du traitement et a décidé de l'organisation du traitement. Il va de soi que les autres entités publiques, en tant que responsables de leurs propres activités de traitement, sont chargées de veiller à l'exactitude des données qu'elles ont traitées auparavant et qu'elles communiquent ensuite à l'autorité A.

4 DÉFINITION D'UN SOUS-TRAITANT

73. L'article 4, paragraphe 8, du RGPD définit un sous-traitant comme étant la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. À l'instar de la définition du responsable du traitement, la définition du sous-traitant envisage un large éventail d'acteurs; il peut s'agir «*[d'une] personne physique ou morale, [d'une] autorité publique, [d'un] service ou [d']un autre organisme*». Cela signifie qu'il n'existe en principe pas de limitation quant au type d'acteur susceptible d'assumer le rôle du sous-traitant. Il peut s'agir d'une organisation, mais également d'un individu.

74. Le RGPD établit des obligations directement et spécifiquement applicables aux sous-traitants, comme le précise plus avant la partie II, section 1, des présentes lignes directrices. Un sous-traitant peut être tenu responsable ou se voir infliger une amende en cas de non-respect de ces obligations ou s'il outrepasse ou enfreint les instructions légales du responsable du traitement.

75. Le traitement de données à caractère personnel peut impliquer de multiples sous-traitants. Par exemple, un responsable du traitement peut choisir lui-même de faire directement appel à des sous-traitants multiples, en faisant intervenir des sous-traitants différents à des étapes distinctes du traitement (sous-traitants multiples). Un responsable du traitement peut également décider de recruter un seul sous-traitant, lequel, avec l'autorisation du responsable du traitement, engage à son tour un ou plusieurs autres sous-traitants («sous-traitants ultérieurs»). L'activité de traitement confiée au sous-traitant peut être limitée à une tâche ou à un contexte très spécifique ou peut être plus générale et étendue.

76. Pour être considéré comme un sous-traitant, deux conditions de base doivent être satisfaites:

    a) être *une entité distincte* du responsable du traitement et

    b) traiter des données à caractère personnel *pour le compte du responsable du traitement*.

77. Une *entité distincte* signifie que le responsable du traitement décide de déléguer tout ou partie des activités de traitement à une organisation extérieure. Au sein d'un groupe d'entreprises, l'une d'entre elles peut être le sous-traitant d'une autre agissant en qualité de responsable du traitement, étant donné que les deux entreprises sont des entités distinctes. En revanche, un service d'une entreprise ne peut pas être le sous-traitant d'un autre service au sein de la même entité.

78. Lorsque le responsable du traitement décide de traiter lui-même les données en utilisant ses propres ressources au sein de son organisation, par exemple par l'intermédiaire de son personnel, dans ce cas, il n'y a pas de sous-traitant. Les employés et les autres personnes qui agissent sous l'autorité directe du responsable du traitement, tels que le personnel intérimaire, ne sont pas considérés comme des sous-traitants puisqu'ils traitent des données à caractère personnel dans le cadre de l'entité du

responsable du traitement. Conformément à l'article 29, ils sont également tenus de suivre les instructions du responsable du traitement.

79. Le *traitement de données à caractère personnel pour le compte du responsable du traitement* requiert, tout d'abord, que l'entité distincte traite les données à caractère personnel au profit du responsable du traitement. L'article 4, paragraphe 2, définit le traitement comme un concept englobant un large éventail d'opérations allant de la collecte, du stockage et de la consultation à l'utilisation, la diffusion ou toute autre forme de mise à disposition et à la destruction. La notion de «traitement» est décrite plus en détail à la sous-section 2.1.5 ci-dessus.

80. Ensuite, le traitement doit être effectué pour le compte d'un responsable du traitement, mais pas sous son autorité ou son contrôle direct. Agir «pour le compte de» signifie servir les intérêts de quelqu'un et rappelle le concept juridique de la «délégation». Dans le cas de la législation relative à la protection des données, un sous-traitant est amené à exécuter les instructions données par le responsable du traitement à tout le moins en ce qui concerne la finalité du traitement et les moyens essentiels. La licéité du traitement au sens de l'article 6, et le cas échéant de l'article 9, du règlement découlera de l'activité du responsable du traitement et le sous-traitant ne doit pas traiter les données autrement que selon les instructions du responsable du traitement. Comme indiqué plus haut, même ainsi, les instructions du responsable du traitement peuvent néanmoins lui laisser une certaine latitude quant à la manière de servir au mieux les intérêts du responsable du traitement, en permettant au sous-traitant de choisir les moyens techniques et organisationnels les plus appropriés[32].

81. Agir «pour le compte de» signifie également que le sous-traitant ne peut pas effectuer le traitement pour sa ou ses propres finalités. Comme le prévoit l'article 28, paragraphe 10, un sous-traitant viole le RGPD lorsqu'il outrepasse les instructions du responsable du traitement et qu'il commence à déterminer ses propres finalités et moyens. Il sera alors considéré comme un responsable du traitement pour ce traitement et pourra faire l'objet de sanctions pour avoir outrepassé les instructions du responsable du traitement.

Exemple: prestataire de services considéré comme un sous-traitant mais agissant comme un responsable du traitement

Le prestataire de services MarketinZ fournit des services de publicité promotionnelle et de marketing direct à diverses entreprises. L'entreprise GoodProductZ conclu un contrat avec MarketinZ, en vertu duquel cette dernière fournit de la publicité commerciale aux clients de GoodProductZ et est considérée comme un sous-traitant des données. Cependant, MarketinZ décide d'utiliser la base de données des clients de GoodProductZ à d'autres fins que la publicité pour GoodProductZ, notamment pour développer sa propre activité commerciale. La décision d'ajouter une finalité supplémentaire à celle pour laquelle les données à caractère personnel ont été transférées transforme MarketinZ en responsable du traitement de cet ensemble d'opérations de traitement et le traitement des données à cette fin constituerait une violation du RGPD.

82. Le comité européen de la protection des données rappelle que tous les prestataires de services qui traitent des données à caractère personnel dans le cadre de la prestation d'un service ne sont pas des «sous-traitants» au sens du RGPD. Le rôle de sous-traitant ne découle pas de la nature de l'entité qui traite les données, mais de ses activités concrètes dans un contexte précis. En d'autres termes, la même entité peut agir à la fois comme responsable du traitement pour certaines opérations de traitement et comme sous-traitant pour d'autres, et la qualité de responsable du traitement ou de sous-traitant doit être appréciée au regard de chaque ensemble de données ou d'opérations de

[32] Voir partie I, sous-section 2.1.4, qui décrit la distinction entre les moyens essentiels et non essentiels.

traitement. La nature du service déterminera si le traitement équivaut à un traitement de données à caractère personnel pour le compte du responsable du traitement au sens du RGPD. Dans la pratique, lorsque le service fourni ne vise pas spécifiquement le traitement de données à caractère personnel ou lorsque ce traitement ne constitue pas un élément essentiel du service, le prestataire de services peut être en mesure de déterminer de manière indépendante les finalités et les moyens du traitement qui est nécessaire à la prestation du service. Dans ce cas, le prestataire de services doit être considéré comme un responsable du traitement distinct et non comme un sous-traitant[33]. Une analyse au cas par cas reste toutefois nécessaire afin de déterminer le degré d'influence effectif de chaque entité sur la détermination des finalités et des moyens du traitement.

Exemple: service de taxi

Un service de taxi propose une plateforme en ligne qui permet aux entreprises de réserver un taxi pour transporter des employés ou des invités à destination et au départ de l'aéroport. Lors de la réservation d'un taxi, l'entreprise ABC indique le nom de l'employé qui doit être pris en charge à l'aéroport de sorte que le chauffeur puisse confirmer l'identité de l'employé au moment de la prise en charge. Dans ce cas, le service de taxi traite les données à caractère personnel de l'employé dans le cadre de son service pour l'entreprise ABC, mais le traitement n'est pas la finalité du service. Le service de taxi a conçu la plateforme de réservation en ligne dans le cadre du développement de sa propre activité commerciale visant à fournir des services de transport, sans avoir reçu d'instructions de l'entreprise ABC. Le service de taxi détermine également de manière indépendante les catégories de données qu'il collecte et la durée de leur conservation. Le service de taxi agit donc en tant que responsable du traitement à part entière, nonobstant le fait que le traitement a lieu à la suite d'une demande de service émanant de l'entreprise ABC.

83. Le comité européen de la protection des données relève qu'un prestataire de services peut toujours agir comme sous-traitant même si le traitement de données à caractère personnel n'est pas l'objet principal ou premier du service, à condition que le client du service détermine toujours les finalités et les moyens du traitement dans la pratique. Lorsqu'ils examinent s'il convient ou non de confier le traitement de données à caractère personnel à un prestataire de services particulier, les responsables du traitement devraient évaluer attentivement si le prestataire de services en question leur permet d'exercer un contrôle suffisant, compte tenu de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques potentiels pour les personnes concernées.

Exemple: centre d'appels

L'entreprise X sous-traite son support client à l'entreprise Y, qui fournit un centre d'appels afin de répondre aux questions des clients de l'entreprise X. Le service de support client signifie que l'entreprise Y doit avoir accès à la base de données clients de l'entreprise X. L'entreprise Y ne peut avoir accès aux données que pour fournir le soutien que l'entreprise X a acheté et elle ne peut pas traiter les données pour d'autres finalités que celles indiquées par l'entreprise X. L'entreprise Y doit être considérée comme un sous-traitant de données à caractère personnel et un accord de sous-traitant doit être conclu entre les entreprises X et Y.

[33] Voir également le considérant 81 du RGPD, qui fait référence au fait de «[confier] des activités de traitement à un sous-traitant», en précisant que l'activité de traitement en tant que telle constitue un élément important de la décision du responsable du traitement de demander au sous-traitant de traiter des données à caractère personnel pour son compte.

Exemple: support informatique général

L'entreprise Z engage un prestataire de services informatiques afin de fournir un soutien général pour ses systèmes informatiques qui contiennent une grande quantité de données à caractère personnel. L'accès aux données à caractère personnel n'est pas l'objet principal du service de support, mais il est inévitable que le prestataire de services informatiques ait systématiquement accès à des données à caractère personnel lors de l'exécution du service. L'entreprise Z conclut donc que le prestataire de services informatiques – qui est une entreprise distincte et est inévitablement amené à traiter des données à caractère personnel bien qu'il ne s'agisse pas de l'objectif principal du service – doit être considéré comme un sous-traitant. Un accord de sous-traitance est donc conclu avec le prestataire des services informatiques.

Exemple: un consultant informatique corrige un bogue logiciel

L'entreprise ABC fait appel à un spécialiste informatique d'une autre entreprise pour corriger un bogue dans un logiciel qu'elle utilise. Le consultant informatique n'est pas engagé pour traiter des données à caractère personnel et l'entreprise ABC décide que tout accès à des données à caractère personnel sera purement accessoire et donc très limité dans la pratique. ABC conclut donc que le spécialiste informatique n'est pas un sous-traitant (ni un responsable du traitement à part entière) et qu'elle prendra les mesures appropriées, conformément à l'article 32 du RGPD, afin d'éviter que le consultant informatique ne traite des données à caractère personnel sans autorisation.

84. Comme indiqué plus haut, rien n'empêche le sous-traitant de proposer un service défini à titre préliminaire, mais le responsable du traitement doit prendre la décision finale d'approuver activement la manière dont le traitement est effectué, à tout le moins en ce qui concerne les moyens essentiels de celui-ci. Comme indiqué précédemment, un sous-traitant dispose d'un pouvoir discrétionnaire en ce qui concerne les moyens non essentiels (voir sous-section 2.1.4 ci-dessus).

Exemple: prestataires de services informatiques en nuage

Une municipalité a décidé de recourir à un prestataire de services informatiques en nuage pour traiter les informations de ses services scolaires et éducatifs. Le service d'informatique en nuage fournit des services de messagerie, de vidéoconférence, de stockage de documents, de gestion de calendrier, de traitement de textes, etc., et nécessitera le traitement de données à caractère personnel sur les élèves et les enseignants. Le prestataire de services informatiques en nuage a proposé un service standardisé qui est proposé dans le monde entier. La municipalité doit toutefois s'assurer que l'accord conclu est conforme à l'article 28, paragraphe 3, du RGPD, à savoir que les données à caractère personnel dont elle est le responsable du traitement ne sont traitées que pour les finalités déterminées par la municipalité. Elle doit également veiller à ce que ses instructions spécifiques concernant les durées de conservation, l'effacement des données, etc., soient respectées par les prestataires de services informatiques en nuage, indépendamment de ce qu'offre généralement le service standardisé.

5 DÉFINITION DU TIERS/DESTINATAIRE

85. Le règlement définit non seulement les notions de responsable du traitement et de sous-traitant, mais également celles de destinataire et de tiers. À la différence des notions de responsable du traitement et de sous-traitant, le règlement ne prévoit pas d'obligations ou de responsabilités spécifiques pour les destinataires et les tiers. On peut dire qu'il s'agit de notions relatives, en ce sens qu'elles décrivent une relation avec un responsable du traitement ou un sous-traitant sous un angle particulier, par

exemple un responsable du traitement ou un sous-traitant communique des données à un destinataire. Le destinataire de données à caractère personnel et un tiers peuvent être simultanément considérés comme un responsable du traitement ou un sous-traitant sous d'autres angles. Par exemple, des entités qui doivent être considérées comme des destinataires ou des tiers d'un certain point de vue, sont des responsables du traitement à l'égard du traitement dont elles déterminent la finalité et les moyens.

Tiers

86. L'article 4, paragraphe 10, du RGPD définit un «*tiers*» comme une personne physique ou morale, une autorité publique, un service ou un organisme autre que la

- la personne concernée,
- le responsable du traitement,
- le sous-traitant et
- les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

87. Cette définition correspond, de façon générale, à la définition antérieure du «*tiers*» énoncée dans la directive 95/46/CE.

88. Alors que les termes «*données à caractère personnel*», «*personne concernée*», «*responsable du traitement*» et «*sous-traitant*» sont définis dans le règlement, la notion de «*personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel*» ne l'est pas. Elle est toutefois généralement comprise comme une référence aux personnes qui font partie de l'entité juridique du responsable du traitement ou du sous-traitant (un employé ou une fonction très comparable à celle des employés, par exemple le personnel intérimaire fourni par une agence de travail intérimaire), mais uniquement dans la mesure où elles sont autorisées à traiter des données à caractère personnel. Un employé, etc., qui obtient un accès aux données auxquelles il n'est pas autorisé à accéder et pour des finalités autres que celles de l'employeur, ne relève pas de cette catégorie. En revanche, cet employé devrait être considéré comme un tiers par rapport au traitement effectué par l'employeur. Dans la mesure où l'employé traite des données à caractère personnel pour ses propres finalités, distinctes de celles de son employeur, il sera considéré comme un responsable du traitement et assumera toutes les conséquences et responsabilités qui en découlent en matière de traitement de données à caractère personnel[34].

89. Un tiers désigne donc une entité qui, dans le cas spécifique en cause, n'est ni une personne concernée, ni un responsable du traitement, ni un sous-traitant ni un employé. Par exemple, le responsable du traitement peut recruter un sous-traitant et lui donner instruction de transférer les données à caractère personnel à un tiers. Ce tiers sera alors considéré comme un responsable du traitement à part entière pour ce qui concerne le traitement qu'il effectue pour ses propres finalités. Il est à noter qu'au sein d'un groupe d'entreprises, une entreprise autre que le responsable du traitement ou le sous-traitant est un tiers, même si elle appartient au même groupe que l'entreprise qui agit en tant que responsable du traitement ou sous-traitant.

[34] L'employeur (en tant que responsable initial du traitement) pourrait néanmoins conserver une certaine responsabilité lorsque le nouveau traitement survient en raison de l'absence de mesures de sécurité appropriées.

Exemple: services de nettoyage

L'entreprise A conclut un contrat avec une société de nettoyage pour l'entretien de ses bureaux. Les nettoyeurs ne sont pas censés avoir accès à des données à caractère personnel ou les traiter d'une autre manière. Bien qu'ils puissent, à l'occasion, voir de telles données lorsqu'ils se déplacent dans les bureaux, ils peuvent accomplir leur tâche sans accéder à des données et leur contrat leur interdit d'accéder aux données à caractère personnel que l'entreprise conserve en tant que responsable du traitement ou de les traiter d'une autre manière. Les nettoyeurs ne sont pas employés par l'entreprise A et ils ne sont pas non plus considérés comme étant placés sous l'autorité directe de cette entreprise. Il n'y a pas d'intention d'engager la société de nettoyage ou ses employés pour traiter des données à caractère personnel pour le compte de l'entreprise A. La société de nettoyage et son personnel doivent donc être considérés comme un tiers et le responsable du traitement doit veiller à ce que des mesures de sécurité appropriées soient mises en place afin d'éviter qu'ils aient accès à des données et imposer un devoir de confidentialité pour le cas où ils verraient accidentellement des données à caractère personnel.

Exemple: groupes d'entreprises – société mère et filiales

Les entreprises X et Y font partie du groupe Z. Les entreprises X et Y traitent toutes deux des données sur leurs employés respectifs à des fins d'administration des ressources humaines. À un moment donné, la société mère ZZ décide de demander les données relatives aux employés de toutes les filiales afin d'élaborer des statistiques pour l'ensemble du groupe. Lors du transfert des données des entreprises X et Y à ZZ, cette dernière doit aussi être considérée comme un tiers, indépendamment du fait que toutes les entreprises font partie du même groupe. L'entreprise ZZ sera considérée comme le responsable du traitement dans le cadre de son traitement des données à des fins statistiques.

Destinataire

90. L'article 4, paragraphe 9, du RGPD définit un «*destinataire*» comme étant la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Les autorités publiques ne doivent toutefois pas être considérées comme des destinataires lorsqu'elles reçoivent des données à caractère personnel dans le cadre d'une demande particulière conformément au droit de l'Union ou au droit d'un État membre (par exemple, les autorités fiscales et douanières, les cellules d'enquête financière, etc.)[35].

91. Cette définition correspond, de façon générale, à la définition antérieure du «*destinataire*», mentionnée dans la directive 95/46/CE.

92. La définition couvre quiconque reçoit des données à caractère personnel, qu'il s'agisse d'un tiers ou non. Ainsi, lorsqu'un responsable du traitement envoie des données à caractère personnel à une autre entité, à savoir un sous-traitant ou un tiers, cette entité est un destinataire. Un tiers destinataire est considéré comme responsable de tout traitement qu'il effectue pour sa ou ses propres finalités après réception des données.

Exemple: communication de données entre entreprises

[35] Voir également le considérant 31 du RGPD.

L'agence de voyages ExploreMore organise des voyages à la demande de ses clients particuliers. Dans le cadre de ce service, elle envoie les données à caractère personnel de ses clients à des compagnies aériennes, des hôtels et des organisateurs d'excursions afin de leur permettre de fournir leurs services respectifs. ExploreMore, les hôtels, les compagnies aériennes et les organisateurs d'excursions doivent tous être considérés comme des responsables du traitement qu'ils effectuent dans le cadre de leurs services respectifs. Il n'y a pas de relation du type responsable du traitement/sous-traitant. Cependant, les compagnies aériennes, les hôtels et les organisateurs d'excursions doivent être considérés comme des destinataires lorsqu'ils reçoivent les données à caractère personnel d'ExploreMore.

PARTIE II – CONSÉQUENCES DE L'ATTRIBUTION DES DIFFÉRENTS RÔLES

1 RELATION ENTRE LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

93. Une nouvelle caractéristique distincte du RGPD réside dans les dispositions imposant directement des obligations aux sous-traitants. Ainsi, un sous-traitant doit s'assurer que les personnes autorisées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité (article 28, paragraphe 3); un sous-traitant doit tenir un registre de toutes les catégories d'activités de traitement (article 30, paragraphe 2) et mettre en œuvre les mesures techniques et organisationnelles appropriées (article 32). Un sous-traitant doit également désigner un délégué à la protection des données dans certaines circonstances (article 37) et a le devoir de notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance (article 33, paragraphe 2). En outre, les règles relatives aux transferts de données vers des pays tiers (chapitre V) s'appliquent aux sous-traitants tout autant qu'aux responsables du traitement. À cet égard, le comité européen de la protection des données estime que l'article 28, paragraphe 3, du RGPD, tout en imposant un contenu spécifique au contrat nécessaire que doivent conclure le responsable du traitement et le sous-traitant, impose des obligations directes aux sous-traitants, notamment l'obligation d'aider le responsable du traitement à garantir le respect des règles[36].

1.1 Choix du sous-traitant

94. 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 concernée[37]. 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.

[36] Ainsi, le sous-traitant devrait aider le responsable du traitement, si nécessaire et sur demande, à assurer le respect des obligations découlant de la réalisation d'analyses d'impact relatives à la protection des données (considérant 95 du RGPD). Cela doit apparaître dans le contrat conclu entre le responsable du traitement et le sous-traitant conformément à l'article 28, paragraphe 3, point f), du RGPD.
[37] Article 28, paragraphe 1, et considérant 81 du RGPD.

95. Les garanties «fournies» par le sous-traitant sont celles qu'il est en mesure de **démontrer à la satisfaction du responsable du traitement**, puisque ce sont les seules à pouvoir être effectivement prises en compte par le responsable du traitement lors de l'évaluation du respect de ses obligations. Cela nécessitera souvent un échange de documents pertinents (par exemple, la politique en matière de respect de la vie privée, les conditions de service, l'enregistrement des activités de traitement, la politique en matière de gestion des documents, la politique de sécurité de l'information, les rapports des audits externes en matière de protection des données, les certifications internationales reconnues, comme la série ISO 27000).

96. 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. En conséquence, le comité européen de la protection des données ne peut fournir une liste exhaustive des documents que le sous-traitant doit présenter ou des actions qu'il doit démontrer dans une situation donnée, car cela dépend dans une large mesure des circonstances particulières du traitement.

97. Les éléments suivants[38] 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.

98. En outre, l'adhésion à un code de conduite ou à un mécanisme de certification approuvé peut être utilisée comme un moyen de démontrer que les garanties sont suffisantes[39]. Il est donc recommandé aux sous-traitants d'informer le responsable du traitement de cette circonstance, ainsi que de toute modification de cette adhésion.

99. L'obligation de faire appel uniquement à des sous-traitants «qui présentent des garanties suffisantes», prévue à l'article 28, paragraphe 1, du RGPD, est une obligation permanente. Elle ne s'éteint pas au moment où le responsable du traitement et le sous-traitant concluent un contrat ou un autre acte juridique. Au contraire, 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[40].

1.2 Forme du contrat ou d'un autre acte juridique

100. 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.

101. Cet acte juridique doit se présenter sous une **forme écrite, y compris en format électronique**[41]. Par conséquent, les accords non écrits (aussi détaillés ou efficaces soient-ils) ne sauraient être considérés comme suffisants pour satisfaire aux exigences énoncées à l'article 28 du RGPD. Afin d'éviter de rencontrer des difficultés pour démontrer que le contrat ou un autre acte juridique est effectivement

[38] Considérant 81 du RGPD.
[39] Article 28, paragraphe 5, et considérant 81 du RGPD.
[40] Voir également l'article 28, paragraphe 3, point h), du RGPD.
[41] Article 28, paragraphe 9, du RGPD.

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).

102. En outre, le contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre doit **lier le sous-traitant** au responsable du traitement, c'est-à-dire qu'il doit imposer au sous-traitant des obligations contraignantes en vertu du droit de l'Union ou du droit d'un État membre. Il doit également préciser les obligations du responsable du traitement. Dans la plupart des cas, un contrat sera conclu, mais le règlement fait également référence à «un autre acte juridique», tel qu'un droit national (primaire ou dérivé) ou un autre instrument juridique. Si l'acte juridique ne contient pas les éléments minimaux requis, il doit être complété par un contrat ou un autre acte juridique comprenant les éléments manquants.

103. Étant donné que le règlement 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[42]. 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[43]. Sous réserve des dispositions de l'article 83 du RGPD, l'autorité de contrôle compétente sera en mesure d'infliger une amende administrative tant au responsable du traitement qu'au sous-traitant, compte tenu des circonstances propres à chaque situation. Les contrats qui ont été conclus avant la date d'application du RGPD auraient dû être actualisés à la lumière de l'article 28, paragraphe 3. L'absence d'une telle mise à jour visant à mettre un contrat existant en conformité avec les exigences du RGPD, constitue une violation de l'article 28, paragraphe 3.

Un accord écrit au titre de l'article 28, paragraphe 3, du RGPD peut être intégré dans un contrat plus large, tel qu'un accord de niveau de service. Afin de faciliter la démonstration du respect des dispositions du RGPD, le comité européen de la protection des données recommande que les éléments du contrat visant à donner effet à l'article 28 du règlement soient clairement identifiés en tant que tels à un seul endroit (par exemple dans une annexe).

104. 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**[44].

[42] La présence (ou l'absence) d'accord écrit n'est toutefois pas déterminante aux fins de l'existence d'une relation entre le responsable du traitement et le sous-traitant. Lorsqu'il existe des raisons de penser que le contrat ne correspond pas à la réalité en matière de contrôle effectif, l'accord peut être écarté sur la base d'une analyse factuelle des circonstances entourant la relation entre les parties et le traitement de données à caractère personnel effectués. Inversement, une relation entre un responsable du traitement et un sous-traitant peut toujours être considérée comme existante en l'absence d'accord de traitement écrit. Cela impliquerait néanmoins une violation de l'article 28, paragraphe 3, du RGPD. En outre, dans certaines circonstances, l'absence de définition claire de la relation entre le responsable du traitement et le sous-traitant peut soulever le problème de l'absence de base juridique sur laquelle chaque traitement devrait être fondé, par exemple pour la communication de données entre le responsable du traitement et le sous-traitant.

[43] L'article 28, paragraphe 3, ne s'applique pas uniquement aux responsables du traitement. Lorsque seul le sous-traitant est couvert par le champ d'application territorial du RGPD, l'obligation n'est directement applicable qu'au sous-traitant, voir également les lignes directrices 3/2018 du comité européen de la protection des données relatives au champ d'application territorial du RGPD, p. 12.

[44] Article 28, paragraphe 6, du RGPD. Le comité européen de la protection des données rappelle que les clauses contractuelles types aux fins du respect de l'article 28 du RGPD ne sont pas les clauses contractuelles types visées à l'article 46, paragraphe 2. Alors que les premières précisent et clarifient la manière dont les dispositions de l'article 28, paragraphes 3 et 4, seront respectées, les secondes prévoient des garanties appropriées en cas de

105. À titre subsidiaire, un ensemble de clauses contractuelles types peut être adopté par la Commission[45] ou par une autorité de contrôle, conformément au mécanisme de contrôle de la cohérence[46]. Ces clauses pourraient faire partie d'une certification délivrée au responsable du traitement ou au sous-traitant en vertu des articles 42 ou 43[47].

106. Le comité européen de la protection des données tient à préciser que les responsables du traitement et les sous-traitants ne sont pas tenus de conclure un contrat basé sur des clauses contractuelles types (CCT) et que celui-ci ne doit pas nécessairement être préféré à la négociation d'un contrat individuel. Les deux options permettent de se conformer à la législation relative à la protection des données, en fonction des circonstances spécifiques, pour autant qu'elles satisfassent aux exigences de l'article 28, paragraphe 3.

107. Si les parties souhaitent bénéficier de clauses contractuelles types, les clauses de leur accord qui concernent la protection des données doivent être identiques à celles des CCT. Ces dernières laissent souvent des champs vides à compléter ou des options à choisir par les parties. De même, comme indiqué plus haut, les CCT seront généralement intégrées dans un accord plus large décrivant l'objet du contrat, ses conditions financières et d'autres clauses convenues; les parties auront la possibilité d'ajouter des clauses supplémentaires (par exemple, le droit applicable et la juridiction compétente) pour autant qu'elles ne contredisent pas, directement ou indirectement, les CCT[48] et qu'elles ne portent pas atteinte à la protection assurée par le RGPD et la législation de l'UE ou des États membres en matière de protection des données.

108. Les contrats entre les responsables du traitement et les sous-traitants peuvent parfois être rédigés unilatéralement par l'une des parties. La ou les parties qui rédigent le contrat peuvent dépendre de plusieurs facteurs, notamment, la position des parties sur le marché et le pouvoir contractuel, leur expertise technique ainsi que l'accès aux services juridiques. Ainsi, certains prestataires de services ont tendance à établir des conditions générales types, qui incluent des accords de traitement de données.

109. 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

---

transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale en l'absence de décision d'adéquation en application de l'article 45, paragraphe 3.

[45] Article 28, paragraphe 7, du RGPD. Article 28, paragraphe 7, du RGPD. Article 28, paragraphe 7, du RGPD. Article 28, paragraphe 7, du RGPD. Voir avis conjoint 1/2021 de l'EDPB et du CEPD concernant les clauses contractuelles types entre responsables du traitement et sous-traitants: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_fr

[46] Article 28, paragraphe 8, du RGPD. Le registre des décisions prises par les autorités de contrôle et les juridictions sur des questions traitées dans le cadre du mécanisme de contrôle de la cohérence, y compris les clauses contractuelles types aux fins du respect des dispositions de l'article 28 du RGPD, peut être consulté à l'adresse suivante: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en.

[47] Article 28, paragraphe 6, du RGPD.

[48] Le comité européen de la protection des données rappelle que le même degré de flexibilité existe lorsque les parties choisissent d'utiliser les CCT en tant que garantie appropriée pour les transferts vers des pays tiers au titre de l'article 46, paragraphe 2, point c) ou d), du RGPD. Le considérant 109 du règlement précise que «*la possibilité qu'ont les responsables du traitement et les sous-traitants de recourir à des clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle ne devrait pas les empêcher d'inclure ces clauses dans un contrat plus large, tel qu'un contrat entre le sous-traitant et un autre sous-traitant, ni d'y ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses contractuelles types [...] et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées*. *Les responsables du traitement et les sous-traitants devraient être encouragés à fournir des garanties supplémentaires par l'intermédiaire d'engagements contractuels qui viendraient compléter les clauses types de protection*».

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. Dans certains cas, un responsable du traitement ou un sous-traitant peut disposer d'un pouvoir de négociation moindre pour adapter l'accord relatif à la protection des données à ses besoins. Le recours aux clauses contractuelles types adoptées au titre de l'article 28 (paragraphes 7 et 8) peut contribuer à rétablir l'équilibre entre les positions de négociation et à assurer que les contrats sont conformes au RGPD.

110. Le fait que le contrat et ses modalités détaillées soient établis par le prestataire de services plutôt que par le responsable du traitement n'est pas problématique en soi et ne suffit pas à conclure que le prestataire de services devrait être considéré comme un responsable du traitement. En outre, le déséquilibre entre le pouvoir contractuel d'un petit responsable du traitement et celui de grands prestataires de services ne devrait pas être considéré comme une justification permettant au responsable du traitement d'accepter des clauses et des conditions contractuelles non conformes à la législation en matière de protection des données, pas plus qu'il n'exonère le responsable du traitement de ses obligations en la matière. Le responsable du traitement doit examiner les conditions et, dans la mesure où il les accepte librement et utilise le service, il assume également l'entière responsabilité du respect du RGPD. Toute modification proposée par un sous-traitant aux accords de traitement de données figurant dans les conditions générales types devrait être directement notifiée au responsable du traitement et approuvée par lui, en gardant à l'esprit la marge de manœuvre dont dispose le sous-traitant en ce qui concerne les éléments non essentiels des moyens (voir paragraphes 40 et 41 ci-dessus). La simple publication de ces modifications sur le site internet du sous-traitant n'est pas conforme aux exigences de l'article 28.

1.3 Forme du contrat ou de l'autre acte juridique

111. Avant d'examiner plus avant chacune des exigences établies par le RGPD concernant le contenu du contrat ou d'un autre acte juridique, quelques remarques générales s'imposent.

112. 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. Loin d'être un exercice pro forma, la négociation et la rédaction du contrat sont l'occasion de préciser des détails du traitement[49]. En effet, «la protection des droits et libertés des personnes concernées, de même que la responsabilité des responsables du traitement et des sous-traitants [...] exige une répartition claire des responsabilités» au titre du RGPD[50].

113. 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***

[49] Voir aussi avis 14/2019 du comité européen de la protection des données sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28, paragraphe 8, du RGPD), p. 5.
[50] Considérant 79 du RGPD.

personne concernée»[51]. 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. Dans le même temps, le contrat devrait inclure certains éléments susceptibles d'aider le sous-traitant à comprendre les risques que le traitement comporte pour les droits et libertés des personnes concernées; en effet, l'activité étant exercée pour le compte du responsable du traitement, celui-ci a souvent une compréhension plus approfondie des risques que comporte le traitement puisqu'il connaît les circonstances dans lesquelles s'inscrit le traitement.

114. 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**[52] 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

[51] Considérant 81 du RGPD.

[52] La durée du traitement n'est pas nécessairement la même que la durée de l'accord (il peut exister des obligations légales de conserver les données plus ou moins longtemps).

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.

115. Alors que le RGPD énumère les éléments qui doivent toujours figurer dans l'accord, il peut être nécessaire d'inclure d'autres informations pertinentes, en fonction du contexte et des risques du traitement ainsi que de toute exigence supplémentaire applicable.

1.3.1 Le sous-traitant ne doit traiter les données que sur instruction documentée du responsable du traitement [article 28, paragraphe 3, point a), du RGPD]

116. La nécessité de préciser cette obligation découle du fait que le sous-traitant traite des données pour le compte du responsable du traitement. Les responsables du traitement doivent fournir à leurs sous-traitants des instructions pour chaque activité de traitement. Ces instructions peuvent inclure le traitement autorisé et acceptable de données à caractère personnel, des procédures plus détaillées, des moyens de sécuriser des données, etc. Le sous-traitant ne va pas au-delà des instructions du responsable du traitement. Il peut toutefois suggérer des éléments qui, s'ils sont acceptés par le responsable du traitement, deviennent partie intégrante des instructions données.

117. Lorsqu'un sous-traitant traite des données qui outrepassent ou vont au-delà des instructions du responsable du traitement, ce qui équivaut à une décision déterminant les finalités et les moyens du traitement, le sous-traitant manque à ses obligations et sera même considéré comme un responsable du traitement au regard de ce traitement, conformément à l'article 28, paragraphe 10 (voir section 1.5 ci-dessous[53]).

118. Les instructions données par le responsable du traitement doivent être **documentées**. À cet effet, il est recommandé d'inclure une procédure et un modèle destinés à donner des instructions supplémentaires dans une annexe au contrat ou à un autre acte juridique. Les instructions peuvent aussi être fournies sous n'importe quelle forme écrite (par exemple, par courrier électronique), ainsi que sous toute autre forme documentée, pour autant qu'il soit possible d'en conserver la trace. En tout état de cause, afin d'éviter toute difficulté pour démontrer que les instructions du responsable du traitement ont été dûment documentées, le comité européen de la protection des données recommande de conserver ces instructions avec le contrat ou un autre acte juridique.

119. L'obligation faite au sous-traitant de s'abstenir de toute activité de traitement qui ne serait pas fondée sur les instructions du responsable du traitement s'applique également aux **transferts** de données à caractère personnel vers un pays tiers ou à une organisation internationale. Le contrat devrait préciser les exigences applicables aux transferts vers des pays tiers ou à des organisations internationales, compte tenu des dispositions du chapitre V du RGPD.

120. Le comité européen de la protection des données recommande au responsable du traitement d'accorder toute l'attention voulue à ce point spécifique, en particulier lorsque le sous-traitant délègue certaines activités de traitement à d'autres sous-traitants et lorsque le sous-traitant possède des divisions ou des unités situées dans des pays tiers. Si les instructions du responsable du traitement ne permettent pas les transferts ou les communications vers des pays tiers, le sous-traitant ne sera pas autorisé à confier le traitement à un sous-traitant ultérieur d'un pays tiers, pas plus qu'il ne pourra faire traiter les données dans une de ses divisions situées en dehors de l'Union.

[53] Voir partie II, section 1.5 («Sous-traitant déterminant les finalités et les moyens du traitement»).

121. Un sous-traitant peut traiter des données autrement que sur instruction documentée du responsable du traitement **lorsque le sous-traitant est tenu de traiter et/ou de transférer des données à caractère personnel conformément au droit de l'Union ou au droit de l'État membre auquel le sous-traitant est soumis**. Cette disposition illustre en outre l'importance de négocier et de rédiger avec soin les accords de traitement des données, étant donné que, par exemple, l'une ou l'autre partie peut devoir demander des conseils juridiques concernant l'existence d'une telle obligation légale. Cela doit se faire en temps utile, le sous-traitant étant tenu d'informer le responsable du traitement de cette exigence avant le début du traitement. Ce n'est que dans le cas où ce même droit (de l'Union ou d'un État membre) interdit au sous-traitant d'informer le responsable du traitement pour des «motifs importants d'intérêt public» que cette obligation d'information ne s'applique pas. En tout état de cause, tout transfert ou communication de données ne peut avoir lieu que s'il est autorisé par le droit de l'Union, y compris en vertu de l'article 48 du RGPD.

1.3.2 Le sous-traitant doit veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité [article 28, paragraphe 3, point b), du RGPD]

122. Le contrat doit mentionner que le sous-traitant doit veiller à ce que toute personne qu'il autorise à traiter les données à caractère personnel s'engage à respecter la confidentialité. Cela peut se faire au moyen d'un accord contractuel spécifique ou en vertu d'obligations légales déjà en vigueur.

123. Le vaste concept de «personnes autorisées à traiter les données à caractère personnel» englobe les employés et les travailleurs intérimaires. D'une manière générale, le sous-traitant ne devrait mettre les données à caractère personnel qu'à la disposition des employés qui en ont effectivement besoin pour accomplir les tâches pour lesquelles le sous-traitant a été recruté par le responsable du traitement.

124. L'engagement ou l'obligation de confidentialité doit être «approprié», c'est-à-dire qu'il doit effectivement interdire à la personne autorisée de divulguer des informations confidentielles sans autorisation et qu'il doit être suffisamment large pour englober toutes les données à caractère personnel traitées pour le compte du responsable du traitement, ainsi que les conditions dans lesquelles les données à caractère personnel sont traitées.

1.3.3 Le sous-traitant doit prendre toutes les mesures requises en vertu de l'article 32 [article 28, paragraphe 3, point c), du RGPD]

125. L'article 32 exige que le responsable du traitement et le sous-traitant mettent en œuvre les mesures de sécurité techniques et organisationnelles appropriées. Alors que cette obligation est déjà directement imposée au sous-traitant dont les opérations de traitement relèvent du champ d'application du RGPD, l'obligation de prendre toutes les mesures requises en vertu de l'article 32 doit encore figurer dans le contrat relatif aux activités de traitement que lui confie le responsable du traitement.

126. Comme indiqué précédemment, le contrat relatif aux activités de traitement ne devrait pas se limiter à reproduire les dispositions du RGPD. Le contrat doit inclure ou mentionner des informations relatives aux mesures de sécurité à adopter, **l'obligation faite au sous-traitant d'obtenir le consentement du responsable du traitement avant d'apporter des modifications** et le réexamen régulier des mesures de sécurité afin de s'assurer de leur adéquation au regard des risques, lesquels peuvent évoluer au fil du temps. Le degré de détail des informations relatives aux mesures de sécurité à inclure dans le

contrat doit permettre au responsable du traitement d'apprécier le caractère approprié des mesures conformément à l'article 32, paragraphe 1, du RGPD. En outre, la description est également nécessaire pour permettre au responsable du traitement de se conformer à son obligation de rendre des comptes en vertu de l'article 5, paragraphe 2, et de l'article 24 du RGPD en ce qui concerne les mesures de sécurité imposées au sous-traitant. Une obligation correspondante faite au sous-traitant d'aider le responsable du traitement et de mettre à sa disposition toutes les informations nécessaires pour démontrer le respect des règles peut être déduite de l'article 28, paragraphe 3, points f) et h), du RGPD.

127. Le niveau de détail des instructions données par le responsable du traitement au sous-traitant concernant les mesures à mettre en œuvre dépendra des circonstances spécifiques de l'espèce. Dans certains cas, le responsable du traitement peut donner une description claire et détaillée des mesures de sécurité à mettre en œuvre. Dans d'autres, il peut décrire les objectifs de sécurité minimaux à atteindre, tout en demandant au sous-traitant de proposer la mise en œuvre de mesures de sécurité spécifiques. En tout état de cause, le responsable du traitement doit donner au sous-traitant une description des activités de traitement et des objectifs de sécurité (fondée sur l'évaluation des risques réalisée par le responsable du traitement) et approuver les mesures proposées par le sous-traitant. Cela pourrait figurer dans une annexe au contrat. Le responsable du traitement exerce son pouvoir de décision sur les caractéristiques principales des mesures de sécurité, que ce soit en dressant une liste précise des mesures ou en approuvant celles proposées par le sous-traitant.

1.3.4 Le sous-traitant doit respecter les conditions visées à l'article 28, paragraphes 2 et 4, pour recruter un autre sous-traitant [article 28, paragraphe 3, point d), du RGPD]

128. L'accord doit préciser que le sous-traitant ne peut pas recruter un autre sous-traitant sans l'autorisation écrite préalable du responsable du traitement, que cette autorisation soit spécifique ou générale. Dans le cas d'une autorisation générale, le sous-traitant doit informer le responsable du traitement de tout changement de sous-traitants ultérieurs en vertu d'une autorisation écrite et donner au responsable du traitement la possibilité de s'y opposer. Il est recommandé que le contrat définisse la procédure à suivre à cet effet. Il convient d'observer que l'obligation du sous-traitant d'informer le responsable du traitement de tout changement de sous-traitant ultérieur implique que le sous-traitant indique ou signale activement ces changements au responsable du traitement[54]. De même, lorsqu'une autorisation spécifique est requise, le contrat devrait définir la procédure à suivre pour l'obtenir.

129. Lorsque le sous-traitant recrute un autre sous-traitant, un contrat doit être conclu entre eux et imposer les mêmes obligations en matière de protection des données que celles imposées au sous-traitant initial, ou ces obligations doivent être imposées par un autre acte juridique en vertu du droit de l'Union ou du droit d'un État membre (voir aussi paragraphe 160 ci-dessous). Cela inclut l'obligation visée à l'article 28, paragraphe 3, point h), de permettre la réalisation d'audits par le responsable du traitement ou un autre auditeur qu'il a mandaté, et de contribuer à ces audits[55]. Le sous-traitant est responsable vis-à-vis du responsable du traitement du respect des obligations relatives à la protection

[54] À cet égard, il n'est en revanche pas suffisant, par exemple, que le sous-traitant se contente de donner au responsable du traitement un accès généralisé à une liste de sous-traitants ultérieurs qui pourrait être mise jour de temps à autre, sans indiquer chaque nouveau sous-traitant ultérieur envisagé. En d'autres termes, le sous-traitant doit informer activement le responsable du traitement de tout changement apporté à la liste (c'est-à-dire, en particulier, chaque nouveau sous-traitant ultérieur envisagé).

[55] Voir aussi avis 14/2019 du comité européen de la protection des données sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28, paragraphe 8, du RGPD), 9 juillet 2019; paragraphe 44.

des données par les autres sous-traitants (pour de plus amples détails sur le contenu recommandé de l'accord, voir section 1.6 ci-dessous[56]).

1.3.5 Le sous-traitant doit aider le responsable du traitement à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits [article 28, paragraphe 3, point e), du RGPD]

130. Bien que le responsable du traitement soit chargé de veiller à ce que les demandes des personnes concernées soient traitées, le contrat doit stipuler que le sous-traitant a l'obligation de l'aider «par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible». La nature de cette aide peut varier considérablement «compte tenu de la nature du traitement» et en fonction du type d'activité qui est confiée au sous-traitant. Les détails concernant l'aide à fournir par le sous-traitant devraient figurer dans le contrat ou dans une annexe à celui-ci.

131. Si l'aide peut consister simplement à transmettre rapidement toute demande reçue et/ou à permettre au responsable du traitement d'extraire et de gérer directement les données à caractère personnel pertinentes, le sous-traitant se verra parfois confier des tâches plus spécifiques et techniques, en particulier lorsqu'il est en mesure d'extraire et de gérer les données à caractère personnel.

132. Il est essentiel de garder à l'esprit que, bien que la gestion pratique des demandes individuelles puisse être confiée au sous-traitant, le responsable du traitement porte la responsabilité de se conformer à ces demandes. Par conséquent, l'appréciation de la recevabilité des demandes des personnes concernées et/ou du respect des exigences imposées par le RGPD devrait être réalisée par le responsable du traitement soit au cas par cas, soit au moyen d'instructions claires communiquées au sous-traitant dans le contrat, avant le début du traitement. De même, les délais fixés au chapitre III ne peuvent pas être reportés par le responsable du traitement, étant donné que les informations nécessaires doivent être fournies par le sous-traitant.

1.3.6 Le sous-traitant doit aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 [article 28, paragraphe 3, point f), du RGPD]

133. L'accord devrait éviter de se contenter de répéter ces obligations d'assistance et **devrait contenir des précisions sur la manière dont le sous-traitant est invité à aider le responsable du traitement à remplir les obligations énumérées**. Par exemple, des procédures et des formulaires types peuvent être joints en annexes à l'accord pour permettre au sous-traitant de fournir au responsable du traitement toutes les informations nécessaires.

134. Le type et le degré d'aide à fournir par le sous-traitant peuvent varier considérablement «*compte tenu de la nature du traitement et des informations à la disposition du sous-traitant*». Le responsable du traitement doit informer le sous-traitant de manière adéquate des risques inhérents au traitement et de toute autre circonstance susceptible d'aider le sous-traitant à s'acquitter de son obligation.

135. Pour en venir aux obligations spécifiques, le sous-traitant est d'abord tenu d'aider le responsable du traitement à respecter l'obligation d'adopter des mesures techniques et organisationnelles appropriées afin de garantir la sécurité du traitement[57]. Bien que cela puisse, dans une certaine mesure, empiéter sur l'exigence selon laquelle le sous-traitant adopte lui-même des mesures de sécurité appropriées, lorsque les opérations de traitement du sous-traitant relèvent du champ

[56] Voir partie II – section 1.6 («Sous-traitants ultérieurs»).
[57] Article 32 du RGPD.

d'application du RGPD, ces deux obligations demeurent distinctes, l'une se référant aux mesures propres au sous-traitant et l'autre à celles du responsable du traitement.

136. Deuxièmement, le sous-traitant doit aider le responsable du traitement à remplir son obligation de notifier les violations de données à caractère personnel à l'autorité de contrôle et aux personnes concernées. Le sous-traitant doit informer le responsable du traitement chaque fois qu'il découvre une violation de données à caractère personnel affectant les installations ou les systèmes informatiques du sous-traitant ou d'un sous-traitant ultérieur et aider le responsable du traitement à obtenir les informations devant figurer dans le rapport destiné à l'autorité de contrôle[58]. Le RGPD exige que le responsable du traitement notifie une violation dans les meilleurs délais afin de réduire au minimum le préjudice pour les personnes et de pouvoir remédier au mieux à la violation de manière appropriée. La notification du sous-traitant au responsable du traitement devrait donc également être faite dans les meilleurs délais[59]. En fonction des caractéristiques spécifiques du traitement confié au sous-traitant, il peut être utile que les parties incluent dans le contrat un délai spécifique (par exemple, le nombre d'heures) dans lequel le sous-traitant devrait informer le responsable du traitement, ainsi que le point de contact de ces notifications, la modalité et le contenu minimum attendu par le responsable du traitement[60]. L'accord contractuel entre le responsable du traitement et le sous-traitant peut également inclure une autorisation et l'obligation que le sous-traitant communique directement une violation de données conformément aux articles 33 et 34, mais la responsabilité juridique de la notification continue d'incomber au responsable du traitement[61]. Si le sous-traitant notifie directement une violation de données à l'autorité de contrôle et informe les personnes concernées conformément aux articles 33 et 34, il doit également informer le responsable du traitement et lui fournir des copies de la notification et des informations aux personnes concernées.

137. En outre, le sous-traitant doit également aider le responsable du traitement à réaliser des analyses d'impact relatives à la protection des données, si nécessaire, et à consulter l'autorité de contrôle lorsque les résultats font apparaître qu'il existe un risque élevé qui ne peut être atténué.

138. Le devoir d'assistance ne consiste pas en un transfert de responsabilité, car ces obligations sont imposées au responsable du traitement. Par exemple, bien que l'analyse d'impact relative à la protection des données puisse, en pratique, être effectuée par un sous-traitant, le responsable du traitement reste responsable de l'obligation de réaliser l'analyse[62] et le sous-traitant est uniquement tenu d'aider le responsable du traitement «si nécessaire et sur demande»[63]. Par conséquent, c'est le responsable du traitement qui doit prendre l'initiative de réaliser une analyse d'impact relative à la protection des données, et non le sous-traitant.

[58] Article 33, paragraphe 3, du RGPD.

[59] Pour de plus amples informations, voir les lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, WP250rev.01, 6 février 2018, p. 13-14.

[60] Voir aussi avis 14/2019 du comité européen de la protection des données sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28, paragraphe 8, du RGPD), 9 juillet 2019; paragraphe 40.

[61] Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, Wp250rev.01, 6 février 2018, p. 14.

[62] Voir Groupe de travail «Article 29» sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rev.01, p. 14.

[63] Considérant 95 du RGPD.

1.3.7 Au terme des activités de traitement, le sous-traitant doit, selon le choix du responsable du traitement, supprimer toutes les données à caractère personnel ou les renvoyer au responsable du traitement et détruire les copies existantes [article 28, paragraphe 3, point g), du RGPD]

139. Les clauses contractuelles visent à garantir que les données à caractère personnel bénéficient d'une protection appropriée au terme de la «prestation de services relatifs au traitement»: il appartient donc au responsable du traitement de décider ce que le sous-traitant devrait faire à l'égard des données à caractère personnel.

140. Le responsable du traitement peut décider d'emblée que les données à caractère personnel seront supprimées ou renvoyées en le précisant dans le contrat, au moyen d'une communication écrite transmise en temps utile au sous-traitant. Le contrat ou un autre acte juridique devrait mentionner que le responsable du traitement peut modifier son choix avant le terme de la prestation de services relatifs au traitement. Le contrat devrait préciser la procédure à suivre pour fournir ces instructions.

141. Si le responsable du traitement opte pour la suppression des données, le sous-traitant devrait veiller à ce qu'elle soit effectuée de manière sécurisée, afin de se conformer également à l'article 32 du RGPD. Le sous-traitant devrait confirmer au responsable du traitement que la suppression a été effectuée dans le délai convenu et selon les modalités convenues.

142. Le sous-traitant doit détruire toutes les copies existantes des données, à moins que le droit de l'Union ou le droit d'un État membre n'exige la poursuite de la conservation. Si le sous-traitant ou le responsable du traitement a connaissance d'une telle obligation légale, il devrait en informer l'autre partie dans les meilleurs délais.

1.3.8 Le contractant doit mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits [article 28, paragraphe 3, point h), du RGPD]

143. Le contrat doit préciser la fréquence et la manière dont le flux d'informations entre le sous-traitant et le responsable du traitement devrait avoir lieu, de sorte que le second soit pleinement informé des détails du traitement qui sont pertinents pour démontrer le respect des obligations énoncées à l'article 28 du RGPD. Par exemple, les parties pertinentes des registres des activités de traitement du sous-traitant peuvent être communiquées au responsable du traitement. Le sous-traitant devrait fournir toutes les informations sur la manière dont l'activité de traitement sera effectuée pour le compte du responsable du traitement. Ces informations devraient comprendre des données sur le fonctionnement des systèmes utilisés, les mesures de sécurité, la manière dont les exigences en matière de conservation des données sont respectées, la localisation des données, les transferts de données, les personnes qui ont accès aux données et les destinataires des données, les sous-traitants ultérieurs utilisés, etc.

144. D'autres détails doivent également être mentionnés dans le contrat en ce qui concerne la capacité de réaliser les inspections et les audits par le responsable du traitement ou un autre auditeur qu'il a mandaté et l'obligation d'y contribuer.

Le RGPD précise quels sont les inspections et les audits que doit réaliser le responsable du traitement ou un tiers mandaté par lui. L'objet de ces audits est de garantir que le responsable du traitement dispose de toutes les informations relatives à l'activité de traitement effectuée pour son compte et

aux garanties fournies par le sous-traitant. Le sous-traitant peut suggérer un auditeur particulier, mais la décision finale doit revenir au responsable du traitement conformément à l'article 28, paragraphe 3, point h), du RGPD[64]. En outre, même si l'inspection est effectuée par un auditeur suggéré par le sous-traitant, le responsable du traitement conserve le droit de contester la portée, la méthodologie et les résultats de l'inspection[65].

Les parties devraient coopérer de bonne foi et déterminer si et quand il convient de réaliser des audits dans les locaux du sous-traitant, ainsi que le type d'audit ou d'inspection (à distance, sur site, autre manière pour recueillir les informations nécessaires) qui serait nécessaire et approprié dans le cas d'espèce, compte tenu également des préoccupations en matière de sécurité. Le choix final à cet égard incombe au responsable du traitement. Grâce aux résultats de l'inspection, le responsable du traitement devrait être en mesure de demander au sous-traitant de prendre des mesures ultérieures, par exemple remédier aux lacunes et aux défaillances constatées[66]. De même, des procédures spécifiques devraient être établies pour l'inspection des sous-traitants ultérieurs par le responsable du traitement et le sous-traitant (voir section 1.6 ci-dessous[67]).

145. La question de la répartition des coûts des audits entre le responsable du traitement et le sous-traitant n'est pas couverte par le RGPD et est subordonnée à des considérations commerciales. Toutefois, l'article 28, paragraphe 3, point h), exige que le contrat prévoie que le sous-traitant est tenu de mettre à la disposition du responsable du traitement toutes les informations nécessaires pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. Dans la pratique, cela signifie que les parties ne devraient pas insérer dans le contrat des clauses prévoyant le paiement de coûts ou d'honoraires qui seraient manifestement disproportionnés ou excessifs et auraient, de ce fait, un effet dissuasif sur l'une des parties. De telles clauses impliqueraient, en effet, que les droits et obligations énoncés à l'article 28, paragraphe 3, point h), ne seraient jamais exercés dans la pratique et deviendraient purement théoriques, alors qu'ils font partie intégrante des garanties en matière de protection des données prévues à l'article 28 du RGPD.

1.4 Instructions contraires à la législation en matière de protection des données

146. L'article 28, paragraphe 3, dispose que le sous-traitant doit informer immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

147. En effet, le sous-traitant a l'obligation de se conformer aux instructions du responsable du traitement, mais il a également une obligation générale de respecter la loi. Une instruction contraire à la législation en matière de protection des données semble créer un conflit entre les deux obligations susvisées.

148. Une fois informé que l'une de ses instructions pourrait être contraire à la législation en matière de protection des données, le responsable du traitement devra évaluer la situation et déterminer si l'instruction constitue effectivement une violation de la législation en matière de protection des données.

[64] Voir avis conjoint 1/2021 de l'EDPB et du CEPD concernant les clauses contractuelles types entre responsables du traitement et sous-traitants, paragraphe 43.
[65] Voir avis 14/2019 du comité européen de la protection des données sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28, paragraphe 8, du RGPD), paragraphe 43.
[66] Voir avis 14/2019 du comité européen de la protection des données sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28, paragraphe 8, du RGPD), paragraphe 43.
[67] Voir partie II – section 1.6 («Sous-traitants ultérieurs»).

149. Le comité européen de la protection des données recommande aux parties de négocier et de convenir contractuellement des conséquences de la notification d'une instruction illicite envoyée par le sous-traitant et de l'inaction du responsable du traitement dans ce contexte. Un exemple serait l'insertion d'une clause relative à la résiliation du contrat si le responsable du traitement maintient son instruction illicite. Un autre exemple serait une clause relative à la possibilité pour le sous-traitant de suspendre la mise en œuvre de l'instruction concernée jusqu'à ce que le responsable du traitement confirme, modifie ou retire son instruction[68].

1.5 Sous-traitant déterminant les finalités et les moyens du traitement

150. Si le sous-traitant viole le règlement en déterminant les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement (article 28, paragraphe 10, du RGPD).

1.6 Sous-traitants ultérieurs

151. Les activités de traitement des données sont souvent effectuées par un grand nombre d'acteurs et les chaînes de sous-traitance deviennent de plus en plus complexes. Le RGPD introduit des obligations spécifiques qui sont déclenchées lorsqu'un sous-traitant (ultérieur) envisage de recruter un autre acteur, ajoutant ainsi un maillon supplémentaire à la chaîne, en lui confiant des activités nécessitant le traitement de données à caractère personnel. La question de savoir si le prestataire de services agit comme un sous-traitant ultérieur devrait être analysée conformément à ce qui a été décrit plus haut à propos de la notion de sous-traitant (voir paragraphe 83 ci-dessus).

152. Bien que la chaîne puisse être assez longue, le responsable du traitement conserve son rôle central dans la détermination des finalités et des moyens du traitement. L'article 28, paragraphe 2, du RGPD dispose que le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement (y compris sous forme électronique). Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité de s'opposer à ces changements. Dans les deux cas, le sous-traitant doit obtenir l'autorisation écrite du responsable du traitement avant qu'un traitement de données à caractère personnel ne soit confié à un sous-traitant ultérieur. Pour évaluer et décider d'autoriser ou non la sous-traitance, une liste des sous-traitants ultérieurs envisagés (comprenant pour chacun d'entre eux: la localisation, ce qu'ils feront et la preuve des garanties qui ont été mises en œuvre) devra être fournie au responsable du traitement par le sous-traitant[69].

153. L'autorisation préalable écrite peut être spécifique, c'est-à-dire qu'elle fait référence à un sous-traitant ultérieur spécifique pour une activité de traitement donnée à un moment précis, ou générale. Cela devrait être précisé dans le contrat ou un autre acte juridique régissant le traitement.

154. Lorsque le responsable du traitement décide d'accepter certains sous-traitants ultérieurs au moment de la signature du contrat, une liste des sous-traitants ultérieurs agréés devrait figurer dans le contrat

[68] Voir avis conjoint 1/2021 de l'EDPB et du CEPD concernant les clauses contractuelles types entre responsables du traitement et sous-traitants, paragraphe 39.

[69] Ces informations sont nécessaires pour que le responsable du traitement puisse se conformer au principe de responsabilité établi à l'article 24 et aux dispositions de l'article 28, paragraphe 1, de l'article 32 et du chapitre V du RGPD.

ou dans une annexe à celui-ci. Cette liste devrait ensuite être tenue à jour, conformément à l'autorisation générale ou spécifique donnée par le responsable du traitement.

155. Si le responsable du traitement choisit de donner une **autorisation spécifique**, il devrait préciser par écrit à quel sous-traitant ultérieur et à quelle activité de traitement il fait référence. Tout changement ultérieur devra également être autorisé par le responsable du traitement avant son exécution. Si la demande d'autorisation spécifique du sous-traitant n'a pas reçu de réponse dans le délai imparti, elle devrait être considérée comme rejetée. Le responsable du traitement devrait prendre sa décision d'accorder ou non son autorisation en tenant compte de son obligation de ne recourir qu'à des sous-traitants offrant des «garanties suffisantes» (voir section 1.1 ci-dessus[70]).

156. Le responsable du traitement peut également donner une **autorisation générale** au recours à des sous-traitants ultérieurs (contractuellement, en incluant une liste de ces sous-traitants ultérieurs dans une annexe), qui devrait être complétée par des critères permettant d'orienter le choix du sous-traitant (par exemple, des garanties en matière de mesures techniques et organisationnelles, des connaissances spécialisées, la fiabilité et les ressources)[71]. Dans ce cas, le sous-traitant doit informer le responsable du traitement en temps utile de tout ajout ou remplacement envisagé des sous-traitants ultérieurs afin de donner au responsable du traitement la possibilité de s'y opposer.

157. Par conséquent, la principale différence entre l'autorisation spécifique et l'autorisation générale réside dans le sens donné au silence du responsable du traitement: en cas d'autorisation générale, le fait que le responsable du traitement ne signale pas son opposition dans le délai imparti peut être interprété comme une autorisation.

158. Dans les deux scénarios, le contrat devrait comporter des précisions sur le délai d'approbation ou d'objection du responsable du traitement et sur la manière dont les parties entendent communiquer sur le sujet (par exemple, des modèles). Ce délai doit être raisonnable au regard du type de traitement, de la complexité des activités confiées au sous-traitant (et aux sous-traitants ultérieurs) et des relations entre les parties. En outre, le contrat devrait préciser les étapes pratiques en cas d'objection du responsable du traitement (par exemple, en indiquant le délai dans lequel le responsable du traitement et le sous-traitant devraient décider si le traitement doit être arrêté).

159. Indépendamment des critères suggérés par le responsable du traitement pour sélectionner les prestataires de services, le sous-traitant demeure pleinement responsable devant le responsable du traitement de l'exécution de leurs obligations par les sous-traitants ultérieurs (article 28, paragraphe 4, du RGPD). Par conséquent, le sous-traitant devrait veiller à proposer des sous-traitants ultérieurs qui offrent des garanties suffisantes.

160. Par ailleurs, lorsqu'un sous-traitant entend recruter un sous-traitant ultérieur (agréé), il doit conclure avec celui-ci un contrat imposant les mêmes obligations que celles imposées par le responsable du traitement au premier sous-traitant ou les obligations doivent être imposées par un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre. Toute la chaîne d'activités de traitement doit être régie par des accords écrits. L'imposition des «mêmes» obligations devrait être interprétée de manière fonctionnelle plutôt que formelle; en effet, il n'est pas nécessaire que le contrat comporte exactement les mêmes termes que ceux utilisés dans le contrat conclu entre le

[70] Voir partie II, section 1.1 («Choix du sous-traitant»).

[71] Cette obligation du responsable du traitement découle du principe de responsabilité énoncé à l'article 24 et de l'obligation de se conformer aux dispositions de l'article 28, paragraphe 1, de l'article 32 et du chapitre V du RGPD.

responsable du traitement et le sous-traitant, mais il devrait assurer que les obligations sont identiques en substance. Cela signifie également que si le sous-traitant confie à un sous-traitant ultérieur une partie spécifique du traitement, à laquelle certaines des obligations ne peuvent s'appliquer, ces obligations ne devraient pas être mentionnées «par défaut» dans le contrat conclu avec le sous-traitant ultérieur, étant donné que cela ne ferait que générer de l'insécurité. À titre d'exemple, en ce qui concerne l'assistance en matière d'obligations relatives aux violations de données, la notification d'une violation de données pourrait être directement adressée par un sous-traitant ultérieur au responsable du traitement si les trois parties sont d'accord. Toutefois, en cas de notification directe, le sous-traitant devrait être informé et obtenir une copie de la notification.

2 CONSÉQUENCES DE LA RESPONSABILITÉ CONJOINTE DU TRAITEMENT

2.1 Définir de manière transparente les obligations respectives des responsables conjoints du traitement aux fins d'assurer le respect des exigences du RGPD

161. L'article 26, paragraphe 1, du RGPD dispose que les responsables conjoints du traitement définissent de manière transparente, par accord entre eux, leurs obligations respectives aux fins d'assurer le respect des exigences du règlement.

162. Les responsables conjoints du traitement doivent donc déterminer «qui fait quoi» en décidant ensemble qui devra exécuter quelles tâches afin d'assurer que le traitement est conforme aux exigences du RGPD en ce qui concerne le traitement conjoint en cause. En d'autres termes, il convient de répartir les responsabilités en matière de conformité, ainsi qu'il résulte de l'utilisation du terme «*respectives*» à l'article 26, paragraphe 1. Cela n'exclut pas que le droit de l'Union ou le droit d'un État membre puisse déjà établir certaines responsabilités de chaque responsable conjoint du traitement. Si tel est le cas, l'accord entre les responsables conjoints du traitement devrait également couvrir toute responsabilité supplémentaire nécessaire aux fins d'assurer le respect des exigences du RGPD qui ne sont pas couvertes par les dispositions légales[72].

163. Ces règles ont pour but de garantir que, lorsque des acteurs multiples sont concernés, en particulier dans des environnements de traitement des données complexes, la responsabilité du respect des règles de protection des données est clairement répartie afin d'éviter que la protection des données à caractère personnel ne soit réduite ou qu'un conflit négatif de compétence ne conduise à des failles entraînant le non-respect de certaines obligations par l'une des parties participant au traitement. Il convient de préciser ici que toutes les responsabilités doivent être réparties en fonction des circonstances factuelles de l'espèce afin de parvenir à un accord opérationnel. Le comité européen de la protection des données relève qu'il existe des cas où l'influence d'un responsable conjoint du traitement et son influence factuelle compliquent la conclusion d'un accord. Toutefois, de telles circonstances n'annulent pas la responsabilité conjointe du traitement et ne sauraient servir à exonérer une partie de ses obligations au titre du RGPD.

[72] «En tout état de cause, l'accord entre les responsables conjoints du traitement devrait couvrir de manière exhaustive l'ensemble des obligations des responsables conjoints du traitement, y compris celles qui peuvent déjà avoir été énoncées dans le droit pertinent de l'Union ou d'un État membre et sans préjudice de l'obligation des responsables conjoints du traitement de mettre à disposition les grandes lignes de l'accord entre les responsables conjoints du traitement, conformément à l'article 26, paragraphe 2, du RGPD».

164. Plus précisément, l'article 26, paragraphe 1, précise que les responsables conjoints du traitement définissent leurs obligations respectives (c'est-à-dire leurs tâches) aux fins d'assurer le respect des exigences du RGPD, «*notamment*» en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, sauf si, et dans la mesure où, leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis.

165. Il ressort clairement de cette disposition que les responsables conjoints du traitement doivent déterminer qui sera chargé de répondre aux demandes des personnes concernées, lorsque celles-ci exercent les droits que leur confère le RGPD, et de leur communiquer les informations visées aux articles 13 et 14 dudit règlement. Il ne s'agit que de définir, dans leurs relations internes, quelle partie est tenue de répondre aux demandes des personnes concernées. Indépendamment des termes de tout accord de ce type, la personne concernée peut contacter chacun des responsables conjoints du traitement conformément à l'article 26, paragraphe 3, du RGPD. Toutefois, l'utilisation dans cette disposition de l'expression «*notamment*» indique que les obligations soumises à la répartition des responsabilités aux fins d'assurer le respect des exigences par chaque partie concernée ne sont pas exhaustives. Il s'ensuit que la répartition des responsabilités entre les responsables conjoints du traitement aux fins d'assurer le respect des exigences ne se limite pas aux sujets mentionnés à l'article 26, paragraphe 1, mais s'étend aux autres obligations du responsable du traitement au titre du RGPD. En effet, les responsables conjoints du traitement doivent veiller à ce que l'ensemble du traitement conjoint soit pleinement conforme au RGPD.

166. À cet effet, les mesures prises pour assurer le respect des exigences et les obligations connexes que les responsables conjoints du traitement devraient prendre en considération lorsqu'ils définissent leurs obligations respectives, outre celles spécifiquement visées à l'article 26, paragraphe 1, incluent notamment, mais sans s'y limiter:

- la mise en œuvre des principes généraux de la protection des données (article 5),
- la base juridique du traitement[73] (article 6),
- les mesures de sécurité (article 32),
- la notification d'une violation de données à caractère personnel à l'autorité de contrôle et à la personne concernée[74] (articles 33 et 34),
- les analyses d'impact relatives à la protection des données (articles 35 et 36)[75],

[73] Bien que le RGPD n'empêche pas les responsables conjoints du traitement d'utiliser une base juridique différente pour les différentes opérations de traitement qu'ils effectuent, il est recommandé, dans la mesure du possible, d'utiliser la même base juridique pour une finalité particulière.

[74] Voir aussi lignes directrices du comité européen de la protection des données sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, WP250rev.01, qui disposent que la responsabilité conjointe du traitement impliquera de «*déterminer quelle partie sera responsable du respect des obligations définies aux articles 33 et 34. Le G29 recommande que les arrangements contractuels entre responsables conjoints du traitement comprennent des dispositions déterminant quel responsable du traitement prendra la direction ou sera responsable du respect de l'obligation de notification des violations établie par le RGPD*» (p. 14).

[75] Voir aussi lignes directrices du comité européen de la protection des données concernant l'analyse d'impact relative à la protection des données (AIPD), WP 248 rév. 01, qui prévoient ce qui suit: «*Lorsque l'opération de traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives. Il convient que leur AIPD détermine quelle partie est responsable des différentes mesures destinées à faire face aux risques et à protéger les droits et libertés des personnes concernées, et que chaque*

- le recours à un sous-traitant (article 28),
- les transferts de données vers des pays tiers (chapitre V),
- l'organisation de contacts avec les personnes concernées et les autorités de contrôle.

167. D'autres éléments pourraient être pris en considération selon le traitement en cause et l'intention des parties, comme les restrictions à l'utilisation de données à caractère personnel pour une autre finalité par l'un des responsables conjoints du traitement. À cet égard, les deux responsables du traitement sont toujours tenus de veiller à disposer tous deux d'une base juridique pour le traitement. Parfois, dans le cadre d'une responsabilité conjointe du traitement, des données à caractère personnel sont échangées entre les responsables du traitement. S'agissant de la responsabilité, chaque responsable du traitement a le devoir de s'assurer que les données ne sont pas traitées ultérieurement d'une manière incompatible avec les finalités pour lesquelles elles ont été initialement collectées par le responsable du traitement qui partage les données[76].

168. Les responsables conjoints du traitement peuvent disposer d'un certain degré de flexibilité dans la répartition et l'attribution des obligations entre eux, pour autant qu'ils garantissent le plein respect des exigences du RGPD en ce qui concerne le traitement spécifique. La répartition devrait tenir compte de facteurs, tels que qui est compétent et en mesure de garantir efficacement les droits des personnes concernées et de se conformer aux obligations pertinentes découlant du RGPD. Le comité européen de la protection des données recommande de documenter les facteurs pertinents et l'analyse menée en interne afin d'attribuer les différentes obligations. Cette analyse fait partie de la documentation requise au titre du principe de responsabilité.

169. Les obligations ne doivent pas forcément être réparties de manière égale entre les responsables conjoints du traitement. À cet égard, la CJUE a récemment statué que «*[...] l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel*»[77]. Toutefois, il peut arriver que toutes les obligations ne puissent pas être réparties et que tous les responsables conjoints du traitement doivent respecter les mêmes exigences découlant du RGPD, compte tenu de la nature et du contexte du traitement conjoint. Ainsi, des responsables conjoints du traitement utilisant des outils ou des systèmes communs de traitement des données doivent tous veiller au respect, notamment, du principe de limitation de la finalité et mettre en œuvre des mesures appropriées pour garantir la sécurité des données à caractère personnel traitées par ces outils communs.

170. Un autre exemple est l'obligation faite à chaque responsable conjoint du traitement de tenir à jour un registre des activités de traitement ou de désigner un délégué à la protection des données (DPD), si les conditions visées à l'article 37, paragraphe 1, sont remplies. Ces obligations ne sont pas liées aux

responsable du traitement exprime ses besoins et partage les informations utiles en veillant à ne pas compromettre de secrets (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles, par ex.) et à ne pas divulguer de vulnérabilités» (p. 9).

[76] Chaque communication de données par un responsable du traitement requiert une base légale et une évaluation de la compatibilité, que le destinataire soit un responsable distinct ou conjoint du traitement. En d'autres termes, l'existence d'une responsabilité conjointe du traitement ne signifie pas automatiquement que le responsable conjoint du traitement qui reçoit les données puisse également traiter de manière licite les données pour d'autres finalités qui vont au-delà de la portée de la responsabilité conjointe.

[77] Arrêt dans l'affaire *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, point 43.

responsables conjoints du traitement, mais elles leur sont applicables en tant que responsables du traitement.

2.2 La répartition des responsabilités doit prendre la forme d'un accord

2.2.1 Forme de l'accord

171. L'article 26, paragraphe 1, du RGPD établit une nouvelle obligation pour les responsables conjoints du traitement, à savoir qu'ils doivent définir leurs responsabilités respectives «*par voie d'accord entre eux*». La forme juridique de cet accord n'est pas précisée par le RGPD. Par conséquent, les responsables conjoints du traitement sont libres de convenir de la forme de l'accord.

172. En outre, l'accord relatif à la répartition des responsabilités est contraignant pour chacun des responsables conjoints du traitement. Ils conviennent et s'engagent mutuellement à se conformer aux obligations respectives qui leur incombent en vertu de l'accord.

173. Dès lors, par souci de sécurité juridique et même si le RGPD ne contient pas d'obligation légale de conclure un contrat ou d'établir un autre acte juridique, le comité européen de la protection des données recommande que cet accord prenne la forme d'un document contraignant, tel qu'un contrat ou un autre acte juridique contraignant au titre du droit de l'UE ou de l'État membre auquel les responsables du traitement sont soumis. Cela apporterait une sécurité juridique et pourrait servir à démontrer la transparence et la responsabilité. En effet, en cas de non-respect de la répartition convenue dans l'accord, son caractère contraignant permet à un responsable du traitement de mettre en cause la responsabilité de l'autre partie pour ce qui, selon l'accord, relève de sa responsabilité. De même, conformément au principe de responsabilité, le recours à un contrat ou à un autre acte juridique permettra aux responsables conjoints du traitement de démontrer qu'ils respectent les obligations qui leur incombent en vertu du RGPD.

174. La manière dont les responsabilités, c'est-à-dire les tâches, sont attribuées à chaque responsable conjoint du traitement doit être décrite en termes simples et clairs dans l'accord[78]. Cette exigence est importante car elle garantit la sécurité juridique et évite d'éventuels conflits non seulement entre les responsables conjoints du traitement, mais aussi avec les personnes concernées et les autorités chargées de la protection des données.

175. Afin de mieux encadrer la répartition des responsabilités entre les parties, le comité européen de la protection des données recommande que l'accord fournisse également des informations générales sur le traitement conjoint, notamment en mentionnant l'objet et la finalité du traitement, le type de données à caractère personnel traitées et les catégories de personnes concernées.

2.2.2 Obligations à l'égard des personnes concernées

176. Le RGPD prévoit plusieurs obligations des responsables conjoints du traitement à l'égard des personnes concernées.

[78] Comme indiqué au considérant 79 du RGPD, «*(...) la responsabilité des responsables du traitement et des sous-traitants, y compris dans le cadre de la surveillance exercée par les autorités de contrôle et des mesures prises par celles-ci, exige une répartition claire des responsabilités au titre du présent règlement, y compris lorsque le responsable du traitement détermine les finalités et les moyens du traitement conjointement avec d'autres responsables du traitement*».

L'accord reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées

177. En complément à ce qui est expliqué à la section 2.1 des présentes lignes directrices, il est important que les responsables conjoints du traitement précisent dans l'accord leurs rôles respectifs, «*notamment*» en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations quant à la communication des informations visées aux articles 13 et 14. L'article 26 du RGPD souligne l'importance de ces obligations particulières. Les responsables conjoints du traitement doivent donc s'organiser et convenir de la manière dont les informations seront communiquées et par qui et de la manière dont les réponses aux demandes de la personne concernée seront fournies et par qui. Indépendamment du contenu de l'accord sur ce point spécifique, la personne concernée peut contacter l'un ou l'autre des responsables conjoints du traitement afin d'exercer ses droits, conformément à l'article 26, paragraphe 3, comme expliqué plus en détail ci-dessous.

178. La manière dont ces obligations sont organisées dans l'accord devrait «*dûment*», c'est-à-dire fidèlement, refléter la réalité du traitement conjoint concerné. Par exemple, si un seul responsable conjoint du traitement communique avec les personnes concernées aux fins du traitement conjoint, ce responsable du traitement pourrait être mieux à même d'informer les personnes concernées et, éventuellement, de répondre à leurs demandes.

Les grandes lignes de l'accord sont mises à la disposition de la personne concernée

179. Cette disposition vise à garantir que la personne concernée a connaissance des «*grandes lignes de l'accord*». Par exemple, la personne concernée doit savoir précisément quel responsable du traitement est le point de contact pour l'exercice des droits de la personne concernée (nonobstant le fait qu'elle peut exercer ses droits à l'égard de et contre chacun des responsables conjoints du traitement). L'obligation de mettre les grandes lignes de l'accord à la disposition de la personne concernée est importante en cas de responsabilité conjointe du traitement, pour que la personne concernée sache quel responsable du traitement est responsable de quoi.

180. Le RGPD ne précise pas ce que recouvre la notion de «*grandes lignes de l'accord*». Le comité européen de la protection des données recommande que les grandes lignes couvrent à tout le moins l'ensemble des éléments des informations visées aux articles 13 et 14, qui devraient déjà être accessibles à la personne concernée et, pour chacun de ces éléments, l'accord devrait préciser quel responsable conjoint du traitement est chargé d'en garantir le respect. Les grandes lignes de l'accord doivent également indiquer le point de contact, s'il a été désigné.

181. La manière dont ces informations sont mises à la disposition de la personne concernée n'est pas précisée. Contrairement à d'autres dispositions du RGPD (comme l'article 30, paragraphe 4, pour le registre des activités de traitement ou l'article 40, paragraphe 11, pour le registre des codes de conduite approuvés), l'article 26 n'indique pas que la mise à disposition devrait être «*sur demande*» ou qu'une «*publicité appropriée*» devrait être garantie. Par conséquent, il appartient aux responsables conjoints du traitement de décider du moyen le plus efficace de mettre les grandes lignes de l'accord à la disposition des personnes concernées (par exemple, avec les informations visées à l'article 13 ou 14, dans la politique de confidentialité ou sur demande du délégué à la protection des données, le cas échéant, ou du point de contact éventuellement désigné). Les responsables conjoints du traitement devraient veiller chacun à ce que les informations soient communiquées de manière cohérente.

Un point de contact pour les personnes concernées peut être désigné dans l'accord

182. L'article 26, paragraphe 1, prévoit la possibilité pour les responsables conjoints du traitement de désigner dans l'accord un point de contact pour les personnes concernées. Cette désignation n'est pas obligatoire.

183. Le fait de connaître un moyen unique de contacter d'éventuels responsables conjoints du traitement permet aux personnes concernées de savoir qui elles peuvent contacter pour toute question en lien avec le traitement de leurs données à caractère personnel. En outre, les multiples responsables conjoints du traitement peuvent ainsi coordonner plus efficacement leurs relations et leurs communications avec les personnes concernées.

184. C'est pourquoi, afin de faciliter l'exercice des droits que leur confère le RGPD par les personnes concernées, le comité européen de la protection des données recommande aux responsables conjoints du traitement de désigner ce point de contact.

185. Il peut s'agir du DPD, le cas échéant, du représentant dans l'Union (pour les responsables conjoints du traitement qui ne sont pas établis dans l'Union) ou de tout autre point de contact auprès duquel des informations peuvent être obtenues.

Indépendamment des termes de l'accord, les personnes concernées peuvent exercer leurs droits à l'égard et à l'encontre de chacun des responsables conjoints du traitement

186. En vertu de l'article 26, paragraphe 3, une personne concernée n'est pas liée par les termes de l'accord et peut exercer les droits que lui confère le RGPD à l'égard de et contre chacun des responsables conjoints du traitement.

187. Ainsi, dans le cas de responsables conjoints du traitement établis dans des États membres différents, ou si un seul responsable conjoint est établi dans l'Union, la personne concernée peut prendre contact, à sa guise, soit avec le responsable du traitement établi dans l'État membre de sa résidence habituelle ou de son lieu de travail, soit avec le responsable du traitement établi ailleurs dans l'Union ou dans l'EEE.

188. Même si l'accord et les grandes lignes de celui-ci désignent un point de contact pour recevoir et traiter toutes les demandes des personnes concernées, celles-ci peuvent toujours choisir une autre solution.

189. Il est donc important que les responsables conjoints du traitement prévoient déjà dans leur accord la manière dont ils géreront les réponses aux demandes qu'ils pourraient recevoir des personnes concernées. À cet égard, il est recommandé que les responsables conjoints du traitement communiquent aux autres responsables du traitement compétents ou au point de contact désigné les demandes reçues afin qu'elles soient traitées efficacement. Exiger des personnes concernées qu'elles prennent contact avec le point de contact désigné ou avec le responsable du traitement compétent leur imposerait une charge excessive, qui serait contraire à l'objectif de faciliter l'exercice des droits que leur confère le RGPD.

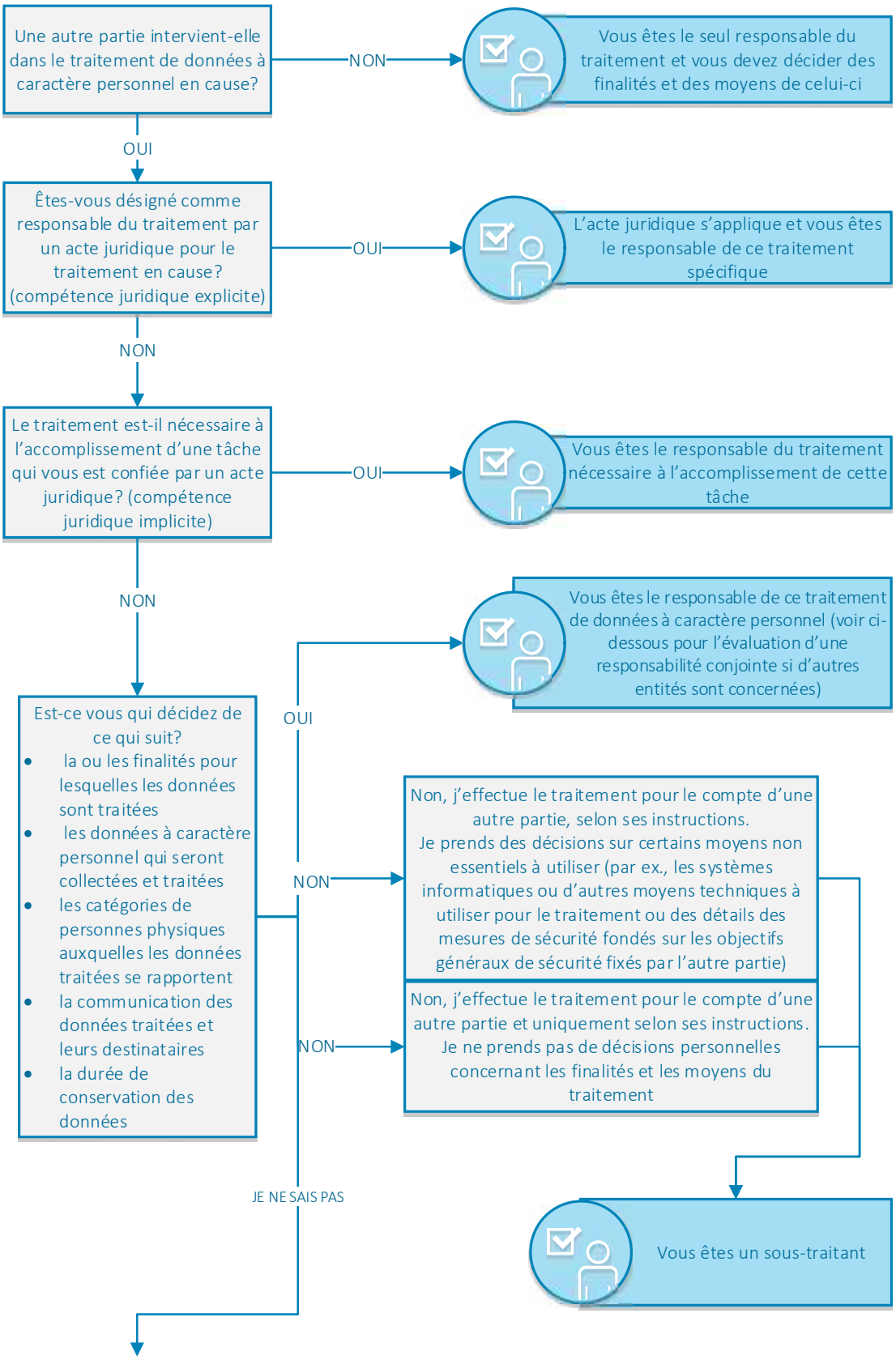
2.3 Obligations à l'égard des autorités chargées de la protection des données

190. Les responsables conjoints du traitement devraient prévoir dans l'accord la manière dont ils communiqueront avec les autorités de contrôle compétentes en matière de protection des données. Cette communication pourrait couvrir une éventuelle consultation au titre de l'article 36 du RGPD, la notification d'une violation de données à caractère personnel ou la désignation d'un délégué à la protection des données.

191. Il convient de rappeler que les autorités de contrôle ne sont pas liées par les termes de l'accord, que ce soit en ce qui concerne la question de la qualité de responsables conjoints du traitement des parties ou du point de contact désigné. Les autorités peuvent donc prendre contact avec n'importe quel responsable conjoint du traitement aux fins d'exercer les pouvoirs que leur confère l'article 58 en matière de traitement conjoint.

Annexe I – Diagramme pour l'application pratique des notions de responsable du traitement, de sous-traitant et de responsables conjoints du traitement

Remarque: afin d'évaluer correctement le rôle de chaque entité concernée, il convient de commencer par identifier le traitement de données à caractère personnel concerné et sa finalité précise. En cas d'entités multiples, il y a lieu d'évaluer si les finalités et les moyens sont déterminés conjointement, ce qui entraîne une responsabilité conjointe.



JE NE SAIS PAS

Je ne sais pas qui décide des finalités ou des moyens du traitement. :

Les facteurs suivants peuvent contribuer à déterminer correctement les rôles:

Facteurs indiquant que vous êtes le responsable du traitement

- Vous tirez un avantage du traitement ou vous avez un intérêt dans celui-ci (autre que la simple rémunération des services reçus d'un autre responsable du traitement)
- Vous prenez des décisions sur les personnes concernées dans le cadre du traitement ou à la suite de celui-ci (par exemple, les personnes concernées sont vos employés)
- Les activités de traitement peuvent être considérées comme étant naturellement liées au rôle ou aux activités de votre entité (par ex., en raison de rôles traditionnels ou d'une expertise professionnelle) qui entraînent des responsabilités en matière de protection des données
- Le traitement concerne votre relation avec les personnes concernées en tant qu'employés, clients, membres, etc.
- Vous disposez d'une totale autonomie pour décider comment les données à caractère personnel sont traitées
- Vous avez confié le traitement de données à caractère personnel à une organisation extérieure pour qu'elle traite ces données pour votre compte

Facteurs indiquant que vous êtes le sous-traitant

- Vous traitez les données à caractère personnel pour les finalités d'un tiers et selon ses instructions détaillées – vous ne poursuivez pas une finalité qui vous est propre pour le traitement.
- Un tiers contrôle vos activités de traitement afin de s'assurer que vous respectez les instructions et les stipulations contractuelles.
- Vous ne poursuivez pas une finalité qui vous est propre pour le traitement en dehors de votre propre intérêt commercial à fournir des services.
- Vous avez été recruté pour effectuer des activités de traitement spécifiques par quelqu'un qui a lui-même été recruté pour traiter des données pour le compte d'un tiers et selon les instructions détaillées de ce tiers (vous êtes un sous-traitant ultérieur)

Responsabilité conjointe – Vous êtes le responsable du traitement et d'autres parties sont impliquées dans le traitement de données à caractère personnel: