EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725

7 novembre 2019

Résumé

Lorsqu'ils traitent des données à caractère personnel, **les institutions et organes de l'Union européenne (IUE) doivent respecter des règles spécifiques en matière de protection des données**. Leurs obligations diffèrent en fonction de leur rôle. **Les lignes directrices qui suivent fournissent des explications et des conseils pratiques aux institutions et organes de l'Union sur la manière de se conformer au règlement (UE) 2018/1725** (ci-après le «règlement»).

À la suite de l'entrée en vigueur du règlement général sur la protection des données (le RGPD) et du règlement 2018/1725, de nombreuses questions ont été soulevées au sujet des modifications apportées aux notions de responsable du traitement, de sous-traitant et de «responsabilité conjointe du traitement», en particulier sur leurs rôles et responsabilités respectifs. **Les présentes lignes directrices visent à fournir aux IUE des conseils pratiques et des instructions permettant de respecter le règlement 2018/1725 en leur apportant des orientations spécifiques sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement à partir des définitions contenues dans le règlement.** Les IUE y verront ainsi plus clair quant au rôle qu'ils peuvent jouer pour des opérations de traitement spécifiques et à ce que ces opérations impliquent en termes d'obligations et de responsabilités au titre du règlement.

Si ces lignes directrices s'adressent aux délégués à la protection des données, aux coordinateurs de la protection des données et à toutes les personnes ayant des responsabilités au sein des IUE en matière de traitement des données à caractère personnel, d'autres organisations externes pourront également les trouver utiles.

Les présentes lignes directrices sont axées sur:

- les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement;

- la répartition de leurs obligations et responsabilités, notamment en ce qui concerne l'exercice des droits des personnes concernées;

- des études de cas précises sur des situations concernant la relation entre responsable du traitement et sous-traitant, la responsabilité séparée du traitement et la responsabilité conjointe du traitement.

Des organigrammes et des listes de contrôle indiquent comment déterminer et évaluer si les IUE peuvent être considérés comme des responsables du traitement, des sous-traitants ou des responsables conjoints du traitement et quelles sont leurs obligations respectives.

Les présentes lignes directrices permettront également aux membres de la direction d'encourager une culture de la protection des données depuis le sommet de l'organisation et d'appliquer le principe de responsabilité.

Leur objectif est d'aider les IUE à remplir leurs obligations. En vertu du principe de responsabilité, les IUE restent en effet responsables du respect de leurs obligations.

TABLE DES MATIÈRES

1. Introduction

À la suite de l'entrée en vigueur du règlement général sur la protection des données[1] (ci-après le «RGPD») et du règlement (UE) 2018/1725[2] (ci-après le «règlement»), de nombreuses questions ont été soulevées au sujet des modifications apportées aux notions de responsable du traitement et de sous-traitant ainsi qu'à leurs rôles respectifs, en particulier aux implications de la notion de «responsabilité conjointe du traitement» (telle que prévue à l'article 28 du règlement).

Lorsqu'ils traitent des données à caractère personnel, les institutions et organes de l'Union européenne (ci-après «IUE») doivent respecter des règles spécifiques en matière de protection des données. Leurs obligations diffèrent en fonction de leur rôle. Les lignes directrices qui suivent visent à fournir aux IUE des conseils pratiques sur la manière de respecter le règlement en leur apportant des explications sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement à partir des définitions contenues dans le règlement. Nous espérons qu'ils y verront ainsi plus clair quant au rôle qu'ils peuvent jouer pour des opérations de traitement spécifiques et à ce que cela implique en termes d'obligations dans le cadre du règlement.

En tant qu'autorité de contrôle indépendante compétente pour le traitement des données à caractère personnel par les IUE, le contrôleur européen de la protection des données (CEPD) peut, entre autres, publier des lignes directrices sur des questions spécifiques relatives au traitement des données à caractère personnel.

Les présentes lignes directrices doivent être prises en considération par les délégués à la protection des données (DPD) et par les coordinateurs ou personnes de contact de la protection des données (CPD) ainsi que par toutes les personnes responsables des IUE agissant en tant que responsables du traitement, sous-traitants ou responsables conjoints du traitement. Elles permettront également aux membres des directions d'encourager une culture de la protection des données depuis le sommet de l'organisation et d'appliquer le principe de responsabilité.

Leur objectif est d'aider les IUE à remplir leurs obligations. En vertu du principe de responsabilité, les IUE restent responsables du respect de leurs obligations. Les IUE pourront choisir d'autres mesures, également efficaces, que celles présentées dans le présent document, en fonction de leurs besoins spécifiques. En pareil cas, ils devront démontrer de quelle manière ils entendent obtenir une protection équivalente des données à caractère personnel à l'aide de ces autres mesures.

[1] 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 (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[2] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

2. Champ d'application et structure des lignes directrices

2.1 Champ d'application des lignes directrices

Le présent document apporte aux IUE des orientations sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement afin de clarifier leur rôle lorsqu'ils traitent des données à caractère personnel, donc de les aider à déterminer leurs responsabilités et à se conformer au règlement.

Il a également pour objet d'illustrer les notions par des exemples grâce à des études de cas et à des listes de contrôle qui expliquent le règlement de manière concrète.

Les présentes lignes directrices portent, en particulier, sur:

- les notions de «responsable du traitement», de «sous-traitant» et de «responsabilité conjointe du traitement» conformément à la législation et à la jurisprudence;

- la répartition des obligations et responsabilités, notamment en ce qui concerne l'exercice des droits des personnes concernées;

- des études de cas précises sur des situations concernant la relation entre responsable du traitement et sous-traitant, la responsabilité séparée du traitement et la responsabilité conjointe du traitement.

Les informations suivantes sont fournies en annexes pour appuyer les orientations:

- un organigramme indiquant si votre institution ou organe peut être considéré comme un responsable du traitement, un sous-traitant ou un responsable conjoint du traitement;

- des listes de contrôle des obligations des responsables du traitement et des sous-traitants.

Ce document ne traite pas/ne tient pas compte:

- des clauses types des contrats entre responsable du traitement et sous-traitant ou des accords entre responsables conjoints du traitement – le CEPD publiera des orientations distinctes à ce sujet;

- des garanties pour les transferts extra-UE/EEE – le CEPD publiera des orientations distinctes à ce sujet.

Le présent document est par ailleurs sans préjudice de toute mise à jour susceptible de s'imposer compte tenu de la future législation de l'UE sur la protection des données, de la future jurisprudence et des futures orientations spécifiques concernant les notions en question et leurs implications en termes de responsabilité.

2.2 Structure des lignes directrices

Les présentes lignes directrices sont structurées comme suit:

- le chapitre 1 présente l'objet des lignes directrices;
- le chapitre 2 définit le champ d'application et la structure du présent document;
- le chapitre 3 explique la notion de «responsable du traitement», définit son rôle et ses responsabilités, et présente ensuite quelques études de cas;
- le chapitre 4 explique la notion de «sous-traitant», définit son rôle et ses responsabilités, et présente ensuite quelques études de cas;
- le chapitre 5 explique la notion de «responsabilité conjointe du traitement», définit le rôle et les responsabilités des responsables conjoints du traitement, et présente ensuite quelques études de cas.
- L'annexe 1 présente un organigramme indiquant comment déterminer si votre institution est responsable du traitement, sous-traitant ou responsable conjoint du traitement;
- l'annexe 2 présente une liste de contrôle énumérant les obligations d'un responsable du traitement;
- l'annexe 3 présente une liste de contrôle énumérant les obligations d'un sous-traitant.

3. La notion de «responsable du traitement»

L'article 3, point 8, du règlement définit le «responsable du traitement» comme «*[...] l'institution ou l'organe de l'Union ou la direction générale ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens dudit traitement sont déterminés par un acte spécifique de l'Union, le responsable du traitement ou les critères spécifiques applicables pour le désigner peuvent être prévus par le droit de l'Union*».

De même qu'à l'article 4, point 7, du RGPD, le «responsable du traitement» est caractérisé par cinq éléments, qui seront analysés séparément dans le présent chapitre. Le RGPD définit le responsable du traitement en des termes légèrement différents comme «*la personne physique ou morale, l'autorité publique ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [...]*». Les deux définitions sont toutefois essentiellement fonctionnelles: l'entité qui décide du «quoi» et du «comment» du traitement sera le responsable du traitement, indépendamment de son statut organisationnel.

3.1 La définition de «responsable du traitement»

3.1.1 «L'institution ou l'organe de l'Union ou la direction générale ou toute autre entité organisationnelle»

La première partie de la définition indique **le type d'acteurs qui peuvent être des responsables du traitement conformément au règlement, à savoir les institutions, les organes de l'Union, les directions générales ou toute autre entité organisationnelle.** Cet élément souligne le fait que toute institution, toute agence, tout organe ou toute direction générale (c'est-à-dire n'importe laquelle des entités organisationnelles généralement présentes dans la majorité des plus grandes IUE) peut être considéré(e) comme un «responsable du traitement» pour l'exécution d'opérations de traitement spécifiques.

Il est donc clair que **les directions générales et les autres entités organisationnelles peuvent jouer le rôle de responsables du traitement (et de responsables conjoints du traitement**, ainsi qu'il sera montré au chapitre 5 des présentes lignes directrices).

3.1.2 «Détermine»

Le deuxième élément de la notion de responsabilité du traitement renvoie à l'**influence de fait qu'a le responsable du traitement sur l'opération de traitement** grâce à l'exercice de son pouvoir de décision[3].

Comment cela peut-il être établi dans la pratique? Pour évaluer l'«influence de fait» d'un responsable du traitement sur l'opération de traitement, il convient d'analyser la totalité des

[3] Voir l'avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», p. 9.

éléments factuels en répondant aux questions ***«pourquoi le traitement a-t-il lieu?»***, ***«qui a entrepris le traitement?»***[4] et ***«à qui le traitement sert-il?»***[5].

Un tel contrôle peut découler:

a) d'une compétence juridique explicite

L'article 3, point 8, du règlement dispose que "(...) *lorsque les finalités et les moyens dudit traitement sont déterminés par un acte spécifique de l'Union, le responsable du traitement ou les critères spécifiques applicables pour le désigner peuvent être prévus par le droit de l'Union*». Lorsque le législateur de l'Union a explicitement désigné le responsable du traitement dans un acte juridique spécifique de l'Union, établir qui est le responsable du traitement devrait en principe être simple.

Le CEPD recommande de définir le responsable du traitement d'une ou plusieurs opération(s) de traitement spécifique(s) dès l'acte législatif de base afin que la détermination de ce responsable soit claire dès le début et pour éviter tout éventuel problème d'interprétation lors de l'analyse de son rôle[6].

- Une telle compétence est par exemple explicitement prévue par le droit aux articles 57 et 58 du règlement ETIAS, où les rôles de responsable et de sous-traitant du traitement des données à caractère personnel sont expressément établis.[7]

b) d'une compétence implicite

En l'absence de compétence explicite, **on peut déterminer qu'une partie est responsable du traitement à partir d'une compétence implicite**. Dans ce cas, le rôle de responsable du traitement n'est pas explicitement prévu par la loi. Toutefois, lorsqu'une partie se voit assigner une tâche spécifique qui nécessite qu'elle exerce certaines fonctions qui supposent le traitement de données à caractère personnel, le rôle de responsable du traitement résulte, en dernière analyse, des tâches et fonctions assignées à cette partie.

- Un exemple de cas où ce rôle est établi par une compétence implicite est le règlement instituant une Agence européenne des médicaments (EMA)[8]: bien que ce règlement ne désigne pas explicitement l'EMA comme «responsable du traitement» (d'ensembles) d'opérations de traitement spécifiques, il lui assigne des missions spécifiques et des

[4] Voir l'avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», p. 8.
[5] Voir l'arrêt dans l'affaire Wirtschaftsakademie Schleswig-Holstein, C-210/16, ECLI:EU:C:2018:388, point 40, et les conclusions de l'avocat général Bot dans l'affaire Wirtschaftsakademie, C-210/16, points 64 et 65.
Arrêt dans l'affaire Fashion ID GmbH & Co.KG/Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629, points 78 à 81, et conclusions de l'avocat général Bobek dans l'affaire Fashion ID, C-40/17, points 68 à 70.
[6] Bien entendu, cette détermination doit être conforme aux responsabilités effectives assignées aux différents acteurs par l'acte législatif.
[7] Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226, articles 57 et 58.
[8] Règlement (CE) nº 726/2004 du Parlement européen et du Conseil du 31 mars 2004 établissant des procédures de l'Union pour l'autorisation et la surveillance en ce qui concerne les médicaments à usage humain et à usage vétérinaire, et instituant une Agence européenne des médicaments, JO L 136 du 30.4.2004, p. 1 à 33, article 24 par exemple.

fonctions connexes. Pour s'acquitter de ces missions (telles que la gestion de certaines bases de données), l'agence doit traiter des données à caractère personnel, ce qui implique également des responsabilités en matière de protection des données. C'est là une indication claire que l'entité en question est un «responsable du traitement».

En l'absence de compétence explicite ou implicite, la responsabilité et le rôle de la partie peuvent être établis en analysant les circonstances factuelles dans lesquelles l'entité opère pour une opération de traitement spécifique[9].

3.1.3 «Les finalités et les moyens»

Le troisième élément de la définition concerne l'essence de l'influence du responsable du traitement, à savoir la détermination des finalités et des moyens de l'opération de traitement. **La détermination du «*pourquoi*» et du «*comment*» d'une opération de traitement est le facteur décisif pour qu'une entité puisse assumer le rôle de «responsable du traitement» au sens de la législation sur la protection des données.** Lorsqu'il exécute une opération de traitement, **le responsable du traitement est celui qui détermine les finalités («*pourquoi*») et les moyens d'une telle opération de traitement («*comment*»)**[10].

Dans cette perspective, le degré d'influence d'une partie dans la détermination tant de la finalité que des moyens peut indiquer son rôle de responsable du traitement. Il convient de souligner que, bien que **les finalités et les moyens** soient liés, il n'est pas nécessaire qu'une partie détermine de la même manière à la fois les uns et les autres pour être considérée comme un responsable du traitement de données à caractère personnel: en fait, cela dépend également du contexte spécifique dans lequel aura lieu l'opération de traitement.

Aussi la question cruciale est-elle de savoir jusqu'à **quel niveau de détail** une partie doit déterminer les finalités et les moyens pour être considérée comme responsable du traitement des données.

Lorsqu'il évalue la **détermination de la finalité**, l'acteur qui détermine la raison pour laquelle un certain traitement aura lieu, à savoir «*pour quoi*» il sera effectué, est le responsable du traitement au sens de la législation sur la protection des données. En d'autres termes, un responsable du traitement est **l'entité qui, de fait, décide de la finalité («*pourquoi*») d'une opération de traitement.**

Pour ce qui est de la **détermination des moyens**, ce terme comprend des éléments divers et renvoie notamment aux mesures techniques et organisationnelles mises en place lors de l'exécution d'une opération de traitement spécifique. Or **la détermination des moyens à utiliser pour une opération de traitement spécifique n'entraîne le rôle de responsable du**

[9] Le plus vraisemblable étant que les institutions et organes de l'Union voient leur rôle établi par une compétence explicite ou implicite, les présentes lignes directrices ne traiteront pas ce cas de figure de manière détaillée. Voir l'avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», p. 11 et 12.

[10] Voir l'arrêt dans l'affaire Wirtschaftsakademie Schleswig-Holstein, C-210/16, ECLI:EU:C:2018:388, points 34 à 36, ainsi que les conclusions de l'avocat général Bot dans l'affaire Wirtschaftsakademie, précitée, points 46 et suivants.

traitement que si la partie décide des éléments essentiels de ces moyens.[11] Selon l'approche adoptée par le groupe de travail «Article 29» dans son avis, ces «éléments essentiels des moyens» sont par exemple: le(s) type(s) de données à traiter, leur période de conservation, les personnes concernées dont les données seraient collectées, les personnes qui auront accès aux données (listes pour le contrôle de l'accès, profils d'utilisateur, etc.) et les destinataires des données, etc., ces éléments étant habituellement réservés à l'appréciation du responsable du traitement.

S'agissant de la détermination des **aspects plus pratiques de la ou des opérations de traitement, autrement dit des «éléments non essentiels des moyens»**, le groupe de travail «Article 29» considère dans le même avis que ce sont le matériel informatique ou le logiciel à utiliser ou les mesures de sécurité technique. Il est tout à fait possible que ces éléments soient identifiés et déterminés par le sous-traitant, dans la mesure où il le fait en suivant les instructions générales données par le responsable du traitement. Le rôle du sous-traitant sera expliqué plus en détail au chapitre suivant.

Par conséquent, **la détermination de la finalité est exclusivement réservée au responsable du traitement d'une opération de traitement.** En revanche, le responsable du traitement **n'est tenu de déterminer que les «éléments essentiels» des moyens des opérations de traitement.** Il est possible qu'un sous-traitant, tout en agissant dans l'intérêt du responsable du traitement, identifie les moyens non essentiels des opérations de traitement, tels que le logiciel à utiliser ou les mesures techniques et organisationnelles qu'il pourrait falloir mettre en place, aidant ainsi le responsable du traitement à respecter les obligations que lui confère la législation sur la protection des données[12].

EXEMPLE:

Conformément aux pouvoirs que lui confère son règlement fondateur, l'Office européen de lutte antifraude (OLAF) décide d'ouvrir une enquête sur des soupçons de fraude dans une institution ou un organe de l'Union, et demande à cette institution ou à cet organe de fournir des informations précises concernant un cas de fraude (informations qui contiennent généralement des données à caractère personnel). L'institution est donc obligée d'obtempérer, mais se demande si elle peut être considérée comme un responsable conjoint du traitement au sens de l'article 28 du règlement.

Ce qui importe pour qu'il existe une situation de responsabilité conjointe du traitement, c'est que la finalité et les moyens des opérations de traitement soient établis conjointement. Si les parties concernées ne déterminent pas conjointement un même objectif (ou une même finalité) général(e) ou si elles n'appuient pas leurs opérations de traitement sur des moyens déterminés conjointement, leur relation semble indiquer une situation de «responsabilité séparée du traitement».

[11] Voir l'avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant»: «*[...] alors que la détermination de la finalité du traitement emporterait systématiquement la qualification de responsable du traitement, la détermination des moyens impliquerait une responsabilité uniquement lorsqu'elle concerne les éléments essentiels des moyens*» (p. 14).

[12] Voir, par exemple, les obligations imposées aux responsables du traitement dans le règlement, aux articles 26, 27 et 33.

Dans ce cas précis, il est évident que les deux institutions ne déterminent pas conjointement la finalité de l'opération de traitement mise en place. L'institution/l'agence/l'organe traite des données à caractère personnel dans une finalité spécifique, par exemple aux fins d'une procédure de passation de marché. Cela ne coïncide pas avec la finalité des opérations de traitement effectuées par l'OLAF, à savoir enquêter sur des soupçons de fraude. En outre, chacune des parties concernées traite des données à caractère personnel indépendamment des moyens utilisés par l'autre responsable du traitement.

Ces faits indiquent donc une situation de responsabilité séparée du traitement.

Une entité n'a pas besoin d'avoir accès à des données à caractère personnel pour être considérée comme un responsable du traitement. Il suffit qu'elle détermine les finalités et les moyens du traitement, qu'elle ait une influence sur le traitement en étant à l'origine du déclenchement du traitement de données à caractère personnel (et en étant en mesure d'y mettre fin), ou qu'elle reçoive les statistiques anonymes fondées sur les données à caractère personnel collectées et traitées par une autre entité[13].

3.1.4 «Seul ou conjointement avec d'autres»

L'article 3, point 8, du règlement (identique à l'article 4, point 7, du RGPD) **établit la possibilité que la finalité et les moyens d'une opération de traitement spécifique soient déterminés par plus d'un acteur**. Cette précision indique clairement et explicitement que la notion de responsabilité du traitement ne suppose pas nécessairement l'existence d'une seule entité, mais qu'elle peut également impliquer que plusieurs parties jouent un rôle dans une opération de traitement. Par conséquent, et comme l'a confirmé la Cour de justice de l'Union européenne (CJUE), chacun des acteurs participants est soumis à des obligations conférées par la législation sur la protection des données[14]. La situation de «responsabilité conjointe du traitement» est analysée de manière détaillée au chapitre 5 des présentes lignes directrices[15].

---

[13] À cet égard, voir l'arrêt dans l'affaire Jehovan todistajat, C-25/17, ECLI:EU:C:2018, points 68 à 72, ainsi que dans l'affaire Wirtschaftsakademie Schleswig-Holstein, C-210/16, et dans l'affaire FashionID & Co.KG/Verbraucherzentrale NRW eV, C-40/17. Il n'est pas non plus nécessaire que le responsable du traitement établisse une distinction, lors du traitement qu'il effectue, entre les données à caractère personnel et les autres types d'information. À cet égard, voir les points 28 et 41 de l'arrêt dans l'affaire Google Spain, C-131/12, où la Cour estime:
- que les moteurs de recherche ne distinguent pas entre les données à caractère personnel et d'autres types d'information qu'ils collectent, indexent et stockent, et
- que le traitement des informations effectué par les moteurs de recherche est un traitement de données à caractère personnel lorsque ces informations contiennent des données à caractère personnel.
Si un acteur détermine les finalités et les moyens d'un traitement, mais que, dans le même temps, ce traitement ne porte pas sur la moindre donnée à caractère personnel à l'un quelconque des stades du traitement, alors ce même acteur ne peut pas être considéré comme un responsable du traitement au sens de la législation sur la protection des données.

[14] Voir l'arrêt dans l'affaire Wirtschaftsakademie Schleswig-Holstein, C-210/16, point 29.

[15] À titre de précision supplémentaire, lorsqu'une institution ou un organe de l'Union doit conclure un accord spécifique avec des organisations internationales, comme ces dernières relèvent d'un statut particulier, il est possible d'adopter un arrangement administratif. Étant donné que la situation relèverait nécessairement du champ d'application des **transferts de données**, l'article 48, paragraphe 3, point b), du règlement précise que «*[...] les garanties appropriées [...] peuvent aussi être fournies, notamment, par [...] des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale [...]* ».

3.1.5 «Du traitement de données à caractère personnel»

Aux termes de l'article 3, point 3, du règlement, «*on entend par [...] "traitement": toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel [...]* ». Cela signifie que **la notion de responsabilité du traitement peut concerner une seule opération ou un ensemble d'opérations de traitement**. Selon une interprétation littérale du règlement, chaque action (collecte, conservation, analyse, communication, etc.) constitue une opération de traitement distincte. Dans la pratique, les opérations de traitement sont groupées en ensembles d'opérations de traitement au service d'une finalité précise. Les responsables du traitement disposent d'une certaine marge d'appréciation pour définir les limites des ensembles d'opérations de traitement.

Par exemple, les responsables du traitement peuvent considérer le processus de recrutement et d'intégration des nouveaux membres du personnel (consistant notamment, pour les IUE, à déterminer les droits statutaires des personnes, à leur donner un badge d'accès physique, un accès aux ressources informatiques, à publier l'information sur l'intranet, etc.) comme un seul ensemble intégré d'opérations de traitement, ou bien le diviser en différents ensembles d'opérations. En règle générale, les responsables du traitement doivent considérer le processus du point de vue des personnes concernées: leur paraît-il constituer un processus intégré? Ainsi, séparer les exercices d'évaluation et les recours pour en faire deux processus semblerait une approche trop étroite, tandis que regrouper tous les processus de gestion des ressources humaines en un seul serait trop large.

L'exercice du contrôle par un acteur donné peut s'appliquer à l'ensemble du traitement, mais peut aussi se limiter à l'une de ses opérations spécifiques[16].

EXEMPLE:

Une institution ou un organe de l'Union décide d'externaliser la surveillance de ses locaux auprès d'une société externe. Cette société gère son propre personnel: l'institution ou organe de l'Union n'intervient pas dans l'établissement du planning, etc.: elle/il exige simplement qu'un nombre défini d'agents de sécurité soient présents à des postes de contrôle définis. Les deux parties peuvent-elles être considérées comme des responsables conjoints du traitement en ce qui concerne le traitement des données à caractère personnel des agents de sécurité dans le cadre de la gestion des ressources humaines par la société externe, par exemple dans le cadre de l'évaluation des performances? La situation changerait-elle si l'institution ou organe de l'Union avait également chargé la société externe d'enregistrer les visiteurs accueillis dans ses locaux?

Il est clair que ni la finalité ni les moyens de l'exécution du traitement des données à caractère personnel des agents de sécurité ne sont déterminés conjointement par les parties concernées: ils sont définis de manière autonome par le prestataire externe. Par conséquent, les parties ne déterminent pas conjointement la finalité et les moyens des opérations de traitement qui concernent le personnel de gestion des ressources humaines de la société externe (les agents de sécurité). Ils peuvent donc être considérés comme des responsables séparés du traitement

[16] À cet égard, voir les conclusions de l'avocat général Bobek dans l'affaire Fashion ID, point 99.

d'opérations différentes dans le cadre du processus global de surveillance des locaux de l'institution ou organe de l'Union.

En revanche, en traitant les données à caractère personnel des visiteurs accueillis dans les locaux de l'institution, la société externe agirait au nom des instructions de l'institution. En d'autres termes, le prestataire externe devrait fournir des garanties de mise en œuvre des moyens techniques et organisationnels en fonction des exigences du responsable du traitement: il agirait alors en tant que sous-traitant de l'institution au sens de l'article 29 du règlement. Cela n'a pas d'incidence sur le rôle de responsable séparé du traitement que joue la société externe pour gérer son propre personnel.

3.2 Obligations et responsabilités du responsable du traitement

L'article 26, paragraphe 1, du règlement dispose que, «*[c]ompte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, 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 présent règlement*». De plus, l'article 26, paragraphe 2, prévoit que «*[…] les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement*». Il est donc clair que **la responsabilité d'assurer le respect des règles incombe au premier chef au responsable du traitement**. **Compte tenu du principe de responsabilité, les responsables du traitement sont par conséquent soumis à l'obligation générale de démontrer le respect du règlement**.

Aux termes de l'article 65 du règlement, «*[t]oute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir de l'institution ou l'organe de l'Union la réparation du dommage subi, sous réserve des conditions prévues dans les traités*».

Cela étant, contrairement à l'article 82 du RGPD, le règlement ne prévoit pas spécifiquement la responsabilité du responsable du traitement (ou du sous-traitant) en cas de non-respect, mais renvoie aux conditions prévues par les traités.

L'article 340 du traité sur le fonctionnement de l'Union européenne (TFUE) dispose que «l'Union doit réparer, conformément aux principes généraux communs aux droits des États membres, les dommages causés par ses institutions». De plus, conformément à la législation sur la protection des données, un responsable du traitement est responsable à l'égard de la personne concernée du total des dommages subis, qu'ils soient matériels ou moraux (article 65 du règlement[17]). Conformément à l'article 268 du TFUE, la Cour de justice de l'Union européenne est compétente pour connaître des litiges relatifs à la réparation des dommages visés à l'article 340 du TFUE.

[17] Voir également l'article 82 du RGPD.

3.3 Protection des personnes concernées

Conformément au règlement (article 4, paragraphe 2, et article 14, paragraphes 1 et 2), il incombe au responsable du traitement de veiller à ce que les personnes concernées puissent exercer les droits qui leur sont conférés par les articles 17 à 24 du règlement. Même si une autre entité est désignée comme point de contact pour les personnes concernées, **le responsable du traitement de l'opération de traitement reste le point de référence ultime soumis à cette obligation**. La jurisprudence la plus récente de la CJUE confirme que la notion de responsable du traitement a été définie de manière large en évitant toute possibilité d'absence de responsabilité à cet égard afin que les personnes concernées puissent bénéficier d'une protection efficace et complète[18].

3.4 Quand une institution ou un organe de l'Union est-il responsable du traitement? Liste de contrôle

Pour résumer le présent chapitre, quand une institution ou un organe de l'Union peut-il être considéré comme un responsable du traitement au sens du règlement? La liste de contrôle suivante pourra aider les IUE à identifier les éléments les plus pertinents pour définir une entité comme responsable du traitement. Si la majorité des réponses aux affirmations est OUI, il est probable que votre institution ou votre organe est responsable du traitement pour un ensemble spécifique d'opérations de traitement au sens du règlement.

	OUI	NON
• Vous avez décidé de traiter des données à caractère personnel ou vous êtes à l'origine de leur traitement par une autre entité.		
• Vous avez décidé quelle finalité ou quel résultat l'opération de traitement doit avoir.		
• Vous avez décidé des éléments essentiels de l'opération de traitement, à savoir quelles données à caractère personnel doivent être collectées, sur quelles personnes, pour quelle période de conservation, qui y a accès, qui en sont les destinataires, etc.		
• Les personnes concernées de vos opérations de traitement sont vos employés.		
• Vous exercez un jugement professionnel lors du traitement des données à caractère personnel.		
• Vous avez un lien direct avec les personnes concernées.		
• Vous disposez d'autonomie et d'indépendance (dans le cadre des missions qui vous sont assignées en tant		

[18] Arrêt dans l'affaire Google Spain SL et Google Inc./Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, C-131/12, ECLI:EU:C:2014:317, point 34. Voir également l'arrêt dans l'affaire Wirtschaftsakademie Schleswig-Holstein, C-210/16, points 27 et 28, et l'arrêt dans l'affaire Jehovan todistajat, C-25/17, point 66.

qu'institution publique) quant à la manière de traiter les données à caractère personnel.		
• Vous avez désigné un sous-traitant afin qu'il exerce des activités de traitement pour votre compte, même si l'entité choisie dans cette finalité met en œuvre des moyens techniques et organisationnels spécifiques (éléments non essentiels).		

Il convient de garder à l'esprit que, pour les IUE, dans la plupart des cas, la responsabilité du traitement est définie par la législation de l'Union, soit parce que cette responsabilité est précisément prévue, soit parce que l'institution ou organe de l'Union a l'obligation ou l'autorisation spécifique de traiter des données conformément à un acte législatif.

4. La notion de «sous-traitant»

L'article 3, point 12, du règlement définit le «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*».

Identique par son libellé à l'article 4, paragraphe 8, du RGPD, la définition du «sous-traitant» est caractérisée par deux éléments, qui seront analysés séparément dans le présent chapitre.

4.1 La définition du «sous-traitant»

4.1.1 La personne physique ou morale, l'autorité publique, le service ou un autre organisme

Comme dans le RGPD, la **définition du «sous-traitant» englobe un large éventail d'acteurs, qu'il s'agisse de personnes physiques ou morales, d'autorités publiques, de services ou d'autres organismes**[19]. L'existence d'un sous-traitant dépend d'une décision prise par le responsable du traitement, qui peut choisir soit d'effectuer lui-même certaines opérations de traitement, soit de déléguer tout ou partie du traitement à un sous-traitant.

L'article 3, point 12, du règlement ne désigne pas spécifiquement les directions générales comme des sous-traitants au sens du droit sur la protection des données. Il est donc clair, d'un point de vue juridique et vis-à-vis des personnes concernées, que l'institution ou organe de l'Union est responsable, en tant que sous-traitant, de toute violation du règlement. Il convient néanmoins de noter que, dans certaines institutions, des directions générales (DG) de l'Union agissent en tant que «DG de soutien», effectuant souvent des opérations de traitement conformément à des instructions strictes et pour le compte d'autres DG (qui sont les responsables du processus opérationnel). Cette situation ne se présente normalement **pas** pour les opérations de traitement effectuées à l'échelle de l'ensemble d'une institution ou d'un organe, mais c'est le cas pour des opérations spécifiques ne relevant que d'une seule DG ou unité particulière. Cette situation est d'ailleurs d'autant plus fréquente qu'il existe des contrats de niveau de service ou d'autres accords pratiques entre directions générales, qui définissent le processus de gouvernance et la répartition des tâches et des responsabilités entre les différentes entités organisationnelles participant au traitement.

Afin d'assurer une répartition efficace des responsabilités et un meilleur niveau de protection des personnes physiques conformément à la législation sur la protection des données, le CEPD recommande de définir, dans les accords internes, les rôles et les responsabilités de ces DG.

Les accords internes à une institution ne doivent pas nécessairement être aussi détaillés que ceux conclus avec les sous-traitants externes, pour autant que les responsabilités soient définies. Cette répartition claire des tâches et des responsabilités entre les différentes entités organisationnelles participant au traitement répond également à la nécessité d'assurer

[19] «Autre organisme» signifiant «toute autre entité» au sens du RGPD, et non organe de l'Union.

pleinement le respect des règles en matière de protection des données et de veiller à ce que le niveau de protection des personnes physiques garanti par le règlement ne soit pas compromis par un manque de clarté quant aux responsabilités.

EXEMPLE:

Dans une institution ou un organe de l'Union, une DG a pour seule responsabilité d'assurer le développement et la gestion technique d'un outil informatique utilisé par une autre direction générale. La direction générale utilisatrice définit les exigences applicables à l'outil informatique. Quel serait le rôle de la DG qui développe l'outil informatique?

Comme cela est expliqué ci-dessus, une DG qui développe, exploite et entretient un outil informatique pour d'autres DG joue un rôle très semblable à celui d'un sous-traitant. Cette DG ne doit pas définir les finalités ou les éléments essentiels des moyens du traitement, c'est-à-dire de l'outil informatique (par exemple, la période de conservation, l'accès aux données et leurs destinataires)[20]. Cela n'empêche pas la DG prestataire de proposer des moyens, à condition que ce soit la DG responsable du traitement qui en décide.

De plus, comme dans le cas du responsable du traitement, le règlement prévoit également la possibilité de désigner un sous-traitant dans un acte juridique spécifique de l'Union:

- voir, par exemple, l'article 58, paragraphe 1, du règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226[21].

4.1.2 Pour le compte du responsable du traitement

L'essence du rôle d'un «sous-traitant» réside dans le fait que **les données à caractère personnel sont traitées pour le compte du responsable du traitement**. Dans la pratique, c'est le responsable du traitement qui détermine la finalité (dans les limites des tâches qui lui sont assignées par la législation) et les éléments essentiels des moyens, tandis que le sous-traitant a un rôle d'exécution. **En d'autres termes, «agir pour le compte du responsable du traitement» signifie que le sous-traitant sert l'intérêt du responsable du traitement en exécutant une tâche spécifique et qu'il suit donc les instructions données par le responsable du traitement, au moins en ce qui concerne la finalité et les éléments essentiels des moyens.**

[20] Si tel était le cas, les entités seraient des responsables conjoints du traitement.

[21] JO L 236 du 19.9.2018, p. 1. «*Article 58* **Sous-traitant** 1. L'eu-LISA est considérée comme un sous-traitant au sens de l'article 2, point e), du règlement (CE) nº 45/2001 en ce qui concerne le traitement de données à caractère personnel dans le système d'information ETIAS.»

L'obligation de respecter les règles incombe au premier chef au responsable du traitement. Il importe néanmoins de comprendre que le sous-traitant n'est pas nécessairement le «subordonné» du responsable du traitement. Le fait que le sous-traitant agisse «pour le compte du responsable du traitement» ne met pas nécessairement en cause son indépendance dans l'exécution des tâches spécifiques qui lui ont été confiées. Le sous-traitant peut jouir d'un degré élevé d'autonomie dans la prestation de ses services et peut définir les éléments non essentiels de l'opération de traitement.

Par exemple, un service ou un organe qui fournit des services d'enquête et qui agit pour le compte d'une autre institution ou d'un autre organe de l'Union (et qui a donc mis en place des procédures de fonctionnement) conformément à un contrat spécifique ou à un autre acte juridique est en droit de conserver son indépendance opérationnelle et organisationnelle dans le cadre de l'exécution de ses principales tâches, car la nature de son mandat requiert un certain degré d'indépendance. Cela est toutefois dû au fait que le responsable du traitement a choisi de donner cette indépendance opérationnelle au sous-traitant. Il appartient aux deux parties concernées de s'entendre sur l'approbation des procédures établies ainsi que sur les rôles et sur les modalités de mise en place de certaines opérations de traitement. Le sous-traitant peut conseiller ou proposer certaines mesures (notamment dans son domaine d'expertise), mais c'est au responsable du traitement qu'il revient de décider d'accepter ou non ces conseils ou ces propositions, une fois qu'il a été pleinement informé des raisons de ces mesures, de leur nature et de la façon dont elles seraient mises en œuvre. En d'autres termes, pour qu'une organisation agisse «pour le compte» d'un responsable du traitement et soit donc définie comme un sous-traitant, il n'est pas nécessaire que le responsable du traitement «impose» la totalité des modalités d'exécution d'une opération de traitement donnée.

Cela étant, lorsqu'**un sous-traitant agit en dehors du mandat qui lui a été donné en violant le contrat ou un autre acte juridique ou en prenant des décisions quant à la finalité et aux éléments essentiels des moyens d'une certaine opération de traitement, il peut être considéré comme un responsable du traitement (ou comme un responsable conjoint du traitement)**.

Dans la pratique, il est possible que le sous-traitant outrepasse son rôle, c'est-à-dire agisse en dehors du cadre de l'accord ou prenne des décisions relatives à la finalité et aux éléments essentiels des moyens d'une opération de traitement spécifique. La question de savoir si une telle situation signifie qu'un sous-traitant devrait automatiquement être qualifié de responsable du traitement (avec toutes les responsabilités que cela implique) dépend, entre autres, de la portée de l'écart de comportement, notamment lorsqu'il sert à assurer le respect des principes de protection des données. En revanche, si le sous-traitant réutilise des données à ses propres fins, outrepassant ainsi clairement le principe de gouvernance générale et les finalités définis dans l'accord conclu avec le responsable du traitement, cela constitue à l'évidence un manquement à ses obligations.

EXEMPLES:

1**. Une directive crée un réseau à participation volontaire d'autorités responsables d'une question spécifique désignée par les États membres. La directive prévoit également que l'institution A fasse fonction de secrétariat du réseau. L'un des principaux objectifs du**

réseau est d'améliorer l'interopérabilité entre les systèmes informatiques nationaux liés à ce domaine en échangeant des données à caractère personnel. Afin de faciliter ces échanges, le réseau a décidé de mettre en place un outil informatique, conçu et mis en œuvre par l'institution A. À la demande des points de contact nationaux des États membres, des données à caractère personnel sont transmises à un ou plusieurs États membres. Le type de données à échanger dans le cadre de l'outil informatique interopérable est déterminé par les lignes directrices adoptées par le réseau et par le recours à des accords spécifiques conclus entre les points de contact des États membres. L'institution A, en tant que secrétariat du réseau, n'est pas associée au processus décisionnel concernant la conception et les fonctions du système en tant que telles, et fournit exclusivement des conseils relatifs à la faisabilité technique et juridique de l'option choisie.

Comme indiqué dans l'exposé du cas, la finalité du traitement de données à caractère personnel dans le cadre de l'outil informatique d'interopérabilité est définie dans la directive. En outre, cette même directive établit aussi l'institution A secrétariat du réseau. Les décisions relatives aux types de données à échanger et au système à utiliser sont fournies par les lignes directrices adoptées par le réseau et par des accords spécifiques conclus entre les points de contact nationaux des États membres. Supposons de surcroît qu'un autre acte d'exécution prévoie les rôles précis de l'institution A, à savoir la tâche de gérer et de garantir la sécurité de l'outil informatique, ainsi que la tâche de fournir aux responsables du traitement les informations nécessaires pour démontrer le respect de leurs obligations.

Conformément à ce qu'indique l'exposé présenté jusqu'ici, la plateforme informatique grâce à laquelle des données à caractère personnel sont échangées est en fait un moyen de communication entre les bases de données des États membres. Vu le cadre juridique relatif à la définition des finalités et des moyens de l'infrastructure, et vu les limites strictes des tâches de l'institution A pour assurer la sécurité des principaux services fournis par la plateforme informatique interopérable, dans cet exemple, l'institution A peut être considérée comme un sous-traitant agissant pour le compte des États membres.

4.2 Le choix du sous-traitant par le responsable du traitement

L'article 29, paragraphe 1, du règlement prévoit que «*[le] responsable du traitement [...] fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du présent règlement et garantisse la protection de la personne concernée*». Cette disposition **oblige le responsable du traitement à évaluer si les garanties offertes par le sous-traitant sont suffisantes. Compte tenu du principe de responsabilité, le responsable du traitement doit être en mesure de prouver qu'il a pris sérieusement en considération tous les éléments visés dans le règlement.**

Le responsable du traitement peut examiner si le sous-traitant fournit des **documents appropriés** attestant d'un tel respect des règles, tels que des politiques de confidentialité, des politiques de gestion des documents, des politiques de sécurité de l'information, des rapports d'audit externe, des certifications, etc. **Le responsable du traitement doit tenir compte des**

connaissances spécialisées du sous-traitant (par exemple de sa compétence technique en cas de violations de données et de mesures de sécurité), de sa fiabilité et de ses ressources. Ce n'est que lorsque le responsable du traitement peut démontrer que le sous-traitant est approprié qu'il peut ensuite conclure un accord conforme aux exigences de l'article 29 du règlement. Le responsable du traitement n'en doit pas moins respecter le principe de responsabilité et vérifier régulièrement si le sous-traitant respecte les règles et quelles mesures il emploie.

Avant d'externaliser le traitement et afin d'éviter tout problème éventuel, **le responsable du traitement doit conclure avec l'autre entité un contrat, un autre acte juridique ou un accord contraignant qui définisse en amont, de manière claire et précise, les obligations en matière de protection des données.**

Aussi le CEPD tient-il à adresser les recommandations suivantes aux IUE:

- faites uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour que le traitement réponde aux exigences du règlement et garantisse la protection des droits des personnes concernées;
- assurez-vous que le sous-traitant n'externalise/ne sous-traite pas les opérations de traitement sans l'autorisation écrite préalable du responsable du traitement;
- veillez à ce que le sous-traitant tienne le responsable du traitement informé de tout changement, en vous donnant la possibilité d'émettre des objections;
- signez avec le sous-traitant un contrat écrit ou un autre accord juridique (contraignant) contenant des clauses spécifiques de protection des données;
- assurez-vous que des obligations contractuelles identiques soient transmises à tout sous-traitant choisi;
- dans le cas des sous-traitants soumis au RGPD, veillez à ce que ces obligations définissent le respect du RGPD comme l'un des éléments à utiliser pour démontrer l'existence des garanties suffisantes.

En suivant ces recommandations et l'évaluation du sous-traitant éventuel et conformément à l'article 29 du règlement, **le responsable du traitement conclut un accord contraignant avec le sous-traitant, qui doit respecter les mêmes obligations que celles qui sont énoncées dans le règlement et dans le RGPD.**

Le sous-traitant ne doit traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit d'un État membre. Le sous-traitant a également l'obligation d'aider le responsable du traitement:

- à s'acquitter de l'obligation incombant au responsable du traitement de garantir les droits des personnes concernées; et
- à remplir les obligations conférées au responsable du traitement par les articles 33 à 41 du règlement (notification des violations de la sécurité et de données, analyse d'impact relative à la protection des données et consultation préalable, confidentialité des communications électroniques, information et consultation du CEPD).

Le responsable du traitement doit donc fixer clairement les modalités de cette aide et donner au sous-traitant des instructions précises sur la manière de les appliquer, par exemple dans le contrat ou dans un autre accord (contraignant).

Ainsi, lorsque le sous-traitant est la seule entité susceptible, en pratique, d'être en mesure de permettre l'exercice des droits des personnes concernées, il devra fournir au responsable du traitement toutes les informations nécessaires pour que ce dernier réponde à la personne concernée. De plus, étant donné que le responsable du traitement et le sous-traitant ont connaissance de leurs responsabilités respectives et qu'ils se sont entendus à cet égard en concluant un contrat spécifique, un autre acte juridique ou un autre accord contraignant, le responsable du traitement peut également avoir la possibilité de transmettre toute demande au sous-traitant lorsque celui-ci est la seule entité à accorder des droits à la personne concernée. Nous recommandons que, dans l'accord en vigueur entre les responsables du traitement et les sous-traitants, les deux parties s'entendent sur les modalités à appliquer pour permettre aux personnes concernées le plein exercice de leurs droits, et que ces modalités soient reflétées dans la déclaration relative à la protection des données qu'il convient de fournir aux personnes concernées.

S'agissant des contrats entre responsable du traitement et sous-traitant, notamment des clauses contractuelles types, le CEPD publiera d'autres orientations.

4.3 La responsabilité du sous-traitant et l'exercice des droits conférés à la personne concernée

Par rapport au cadre juridique antérieur de protection des données, le règlement (considérants 45 et 50 et article 29)[22] **renforce les responsabilités du sous-traitant.**

Toutefois, nonobstant les obligations de ce dernier, l'article 29 du règlement semble indiquer que **la responsabilité du sous-traitant demeure d'une portée plus limitée que la responsabilité du responsable du traitement.** En d'autres termes, bien que les responsables du traitement puissent en principe être tenus responsables des dommages résultant de toute infraction liée au traitement de données à caractère personnel (y compris de toute infraction commise par le sous-traitant) ou de toute violation du contrat ou d'un autre accord (contraignant), le sous-traitant peut être tenu responsable lorsqu'il a agi en dehors du mandat que lui a donné le responsable du traitement, ou s'il n'a pas rempli les obligations que lui confère le règlement[23]. Le sous-traitant peut être tenu entièrement ou partiellement responsable de la «partie» de l'opération de traitement à laquelle il participe[24]. Il ne peut être tenu pleinement responsable que s'il est entièrement responsable du dommage subi.

[22] Pour le RGPD, voir les considérants 79 et 146 ainsi que l'article 82.
[23] De nombreux articles du règlement énoncent les obligations des sous-traitants, et non pas seulement l'article 29.
[24] Par exemple en cas de violation de données au centre de données du sous-traitant due au fait que celui-ci n'a pas mis en œuvre les mesures de sécurité appropriées. Cela étant, le responsable du traitement n'a pas vérifié si des mesures de sécurité étaient en place, ni lesquelles, ni si elles étaient appropriées pour atténuer les risques. Ils sont donc tous deux responsables de la violation de données et des dommages subis.

Un sous-traitant qui suit des instructions spécifiques données par le responsable du traitement peut-il être tenu responsable de suivre ces instructions? L'article 29, paragraphes 3 et 4, du règlement définit les obligations du sous-traitant en ce qui concerne l'accord à conclure avec le responsable du traitement. Dans la pratique, un sous-traitant effectuant des opérations de traitement spécifiques selon des instructions strictes données par le responsable du traitement n'est pas tenu responsable d'une quelconque violation du règlement lorsqu'il suit strictement les instructions du responsable du traitement[25]. Toutefois, s'il est constaté que le sous-traitant a outrepassé les instructions et le mandat donnés par le responsable du traitement, ou s'il a manqué à ses obligations, il peut être tenu responsable de la violation du règlement et/ou du dommage. Il convient également de noter que, lorsque le responsable du traitement est une institution ou un organe de l'Union et que le sous-traitant est un acteur extérieur, ce dernier est soumis à la fois au règlement (notamment en ce qui concerne le respect des conditions visées à l'article 29 du règlement) et au RGPD (en ce qui concerne les exigences relatives à son organisation interne et au respect des règles).

Conformément à l'article 29, paragraphe 1, du règlement, **vis-à-vis de la personne concernée**, le responsable du traitement porte la responsabilité principale de l'opération de traitement et peut être tenu responsable de dommages. La personne concernée peut néanmoins tenir le sous-traitant responsable si elle a des raisons spécifiques de croire que l'infraction qui lui a causé préjudice a été commise par celui-ci.

4.4 Quand une institution ou un organe de l'Union est-il sous-traitant? Liste de contrôle

Pour résumer le présent chapitre, quand une institution ou un organe de l'Union peut-il être considéré comme un sous-traitant au sens du règlement? La liste de contrôle suivante a pour but d'aider les IUE à identifier les éléments les plus pertinents qui justifient de définir une entité comme sous-traitant. Si la majorité des réponses aux affirmations est OUI, il est probable que votre institution ou votre organe soit sous-traitant pour un ensemble spécifique d'opérations de traitement au sens du règlement.

	OUI	NON
• Pour le traitement des données à caractère personnel, vous suivez les instructions d'une autre partie.		
• Ce n'est pas vous qui décidez de collecter des données à caractère personnel auprès des personnes.		
• Ce n'est pas vous qui décidez de la base juridique de la collecte et de l'utilisation de ces données.		
• Ce n'est pas vous qui décidez de la ou des finalités de l'utilisation des données.		
• Ce n'est pas vous qui décidez s'il convient ou non de communiquer ces données, ni à qui.		
• Ce n'est pas vous qui décidez de la période de conservation des données.		

[25] Sans préjudice de la responsabilité de tout manquement à l'une quelconque de ses propres obligations commis simultanément par le sous-traitant.

• Vous prenez certaines décisions sur la manière dont les données sont traitées, mais vous mettez en œuvre ces décisions dans le cadre d'un contrat ou d'un autre acte juridique ou accord contraignant conclu avec le responsable du traitement.		
• Vous n'êtes pas intéressé au résultat final du traitement.		

5. La notion de «responsabilité conjointe du traitement»

La distinction entre les notions de «responsable du traitement» et de «sous-traitant» ne rend pas compte de toutes les relations possibles. Il peut arriver que davantage d'acteurs partagent les responsabilités du responsable du traitement. Comme indiqué dans l'avis 1/2010 du groupe de travail «Article 29», «*[...] l'article 2, point b), de la directive n'exclut pas la possibilité que différents acteurs participent à plusieurs opérations ou ensembles d'opérations appliquées à des données à caractère personnel*»[26].

La notion de responsabilité conjointe du traitement avait déjà été prévue dans la définition du «responsable du traitement» donnée à l'article 2, point d), du règlement (CE) nº 45/2001. En conséquence, l'article 2, point d), de la directive 95/46/CE avait englobé la notion de «responsable conjoint du traitement» dans la définition plus large du terme «responsable du traitement». De même, l'article 26 du RGPD prévoit que lorsque deux responsables du traitement ou plus déterminent les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Par conséquent, **la «responsabilité conjointe du traitement» n'est pas une notion nouvelle**.

L'article 28, paragraphe 1, du règlement prévoit que «*[l]orsque deux ou plusieurs responsables du traitement ou un ou plusieurs responsables du traitement avec un ou plusieurs responsables du traitement autres que les institutions et organes de l'Union, déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement [...]*».

Que cela signifie-t-il dans la pratique?

Le présent chapitre vise à répondre à deux questions générales: quand une situation de responsabilité conjointe du traitement se présente-t-elle et quelles sont les obligations des responsables conjoints du traitement? Il traite également des droits des personnes concernées et de la responsabilité des parties dans une situation de responsabilité conjointe du traitement. Nous donnons ci-dessous quelques orientations en indiquant les éléments susceptibles d'être utiles pour analyser une situation de responsabilité conjointe du traitement.

5.1 Quand une situation de responsabilité conjointe du traitement se présente-t-elle et quels en sont les éléments déterminants?

L'élément crucial de la définition donnée à l'article 28, paragraphe 1, du règlement est que les responsables du traitement «*déterminent conjointement les finalités et les moyens du traitement*». Le chapitre suivant présentera les conséquences de cette définition et se penchera sur les problèmes d'interprétation qu'elle est susceptible d'engendrer.

Premièrement, l'article 28, paragraphe 1, précise qu'une telle situation ne se présente pas uniquement entre deux responsables du traitement ou plus à l'intérieur des IUE. La responsabilité conjointe du traitement peut également se présenter entre une institution ou un organe de l'Union et un acteur extérieur (tel que le prestataire externe d'un portail de gestion

[26] Avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant», p. 18.

ou une autorité publique nationale, etc.). Il est par conséquent essentiel de garder à l'esprit qu'une situation de responsabilité conjointe du traitement peut effectivement se présenter entre une institution ou un organe de l'Union et un ou plusieurs acteurs extérieurs liés par le RGPD[27]. Dans ce cas, **les obligations découlant de l'article 28 du règlement s'appliquent pleinement**.

Une institution ou un organe de l'Union peut se trouver dans une situation de responsabilité conjointe du traitement avec une entité soumise au RGPD. Par exemple, les IUE, en accomplissant leurs missions d'intérêt public, peuvent être responsables du traitement conjointement avec des autorités des États membres (comme ce sera expliqué plus avant dans les études de cas).

Cela étant, le CEPD encourage les IUE utilisant des services fournis par des sociétés privées à s'assurer que ces sociétés privées agissent uniquement en tant que sous-traitants de ces opérations de traitement. Si les IUE peuvent recourir à des services externes lorsqu'ils accomplissent les missions que la législation leur a attribuées dans l'intérêt public, il ne serait pas approprié qu'une partie privée exerce le type d'influence qui ferait d'elle un responsable conjoint du traitement.

- Prenons l'exemple d'une institution ou d'un organe qui ferait appel à un prestataire de services informatiques. Dans cette situation, l'institution ou organe de l'Union doit en effet avoir pour objectif de décider de la finalité et des éléments essentiels de l'opération de traitement, donc de garder le contrôle de l'opération de traitement mise en place, et de ne déléguer au prestataire de services que les éléments non essentiels du traitement.

Deuxièmement, il convient de comprendre la notion de détermination conjointe comme toute situation dans laquelle chaque responsable du traitement a la possibilité/le droit de déterminer les finalités et les éléments essentiels des moyens d'une opération de traitement. Cela signifie que, avant de conclure un accord spécifique avec une partie ou plus, chaque responsable du traitement a connaissance de la finalité générale et (des éléments essentiels) des moyens du traitement. En d'autres termes, **par le simple fait de conclure un tel accord, les parties déterminent en commun (ou convergent sur) la finalité et les éléments essentiels des moyens d'effectuer une opération de traitement: cela suffit, en soi, pour provoquer une situation de responsabilité conjointe du traitement.**

Troisièmement, il faut que soient déterminés à la fois les finalités et les (éléments essentiels des) moyens de l'opération de traitement. La notion de moyens et de finalités a été expliquée au chapitre 2 des présentes lignes directrices[28].

[27] Ou par la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

[28] Conclusions de l'avocat général Bobek dans l'affaire Fashion ID, C-40/17, point 105. Cela a été confirmé par la CJUE dans l'affaire Fashion ID GmbH & Co.KG/Verbraucherzentrale NRW eV, C-40/17.

En résumé, **lorsque les finalités et les (éléments essentiels des) moyens de l'opération de traitement sont déterminés conjointement, un niveau «général» de complémentarité et d'unité de finalité peut suffire à provoquer une situation de responsabilité conjointe du traitement[29].**

Certaines situations font régulièrement naître des doutes quant à l'existence d'une situation de responsabilité conjointe du traitement.

- Il a été avancé que le fait de ne pas avoir accès aux données à caractère personnel dans le cadre d'une opération de traitement suffit à exclure une situation de responsabilité conjointe du traitement. Toutefois, la CJUE, dans son arrêt dans l'affaire Wirtschaftsakademie, C-201/16 (fondé sur la directive 95/46/CE[30]), a jugé que la directive «*[…] n'exige pas, lorsqu'il y a une responsabilité conjointe de plusieurs opérateurs pour un même traitement, que chacun ait accès aux données à caractère personnel concernées*»[31]. De plus, dans l'affaire Témoins de Jéhovah, la CJUE a confirmé cette approche en définissant les parties impliquées dans une activité de prédication de porte-à-porte comme des responsables conjoints du traitement «*[…] sans qu'il soit nécessaire que ladite communauté ait accès aux données […]*»[32].

Ces arrêts soulignent que ce qui importe pour qu'il existe une situation de responsabilité conjointe du traitement, c'est la détermination de la finalité et (d'éléments essentiels) des moyens des opérations de traitement. Le fait qu'une partie n'ait accès qu'à des informations ne concernant pas une personne physique identifiée ou identifiable, ou à des données à caractère personnel rendues anonymes de telle manière que la personne concernée n'est pas ou n'est plus identifiable, comme c'était le cas dans l'affaire Wirtschaftsakademie, n'a pas d'incidence sur la situation de responsabilité conjointe du traitement. Cela peut néanmoins importer lorsqu'il s'agit d'établir le degré de responsabilité des parties concernées.

Dans la pratique, il peut être difficile de distinguer une situation de responsabilité conjointe du traitement d'une situation dans laquelle deux responsables du traitement agissent séparément. En fait, plusieurs responsables du traitement peuvent interagir dans différentes opérations du traitement sans nécessairement partager l'ensemble des finalités et des moyens en tant que tels.

Il est clair que **si les parties concernées ne déterminent pas conjointement un même objectif (ou une même finalité) général(e) ou ne convergent pas sur un tel objectif (ou une telle finalité), ou si elles n'appuient pas leurs opérations de traitement sur (des éléments essentiels) des moyens déterminés conjointement, leur relation semble indiquer une situation de «responsabilité séparée du traitement».**

[29] Arrêt dans l'affaire Fashion ID GmbH & Co.KG/Verbraucherzentrale NRW eV, C-40/17, point 85.
[30] Il ne semble exister aucune raison de croire qu'il aurait été statué différemment sur le fondement du règlement ou du RGPD.
[31] Arrêt dans l'affaire Wirtschaftsakademie Schleswig-Holstein, C-210/16, point 38.
[32] Arrêt dans l'affaire Jehovan todistajat, C-25/17, points 69 et 75. Cela a été réaffirmé dans l'affaire Fashion ID GmbH & Co.KG/Verbraucherzentrale NRW eV, C-40/17, point 69.

- Par exemple, les IUE disposent généralement de caméras de télévision en circuit fermé (CCTV), installées pour préserver la sécurité des locaux. En cas d'incident, qui peut nécessiter une enquête des autorités répressives nationales, il peut être indispensable de transférer les données de la CCTV aux autorités chargées de l'enquête. En pareil cas, les deux parties concernées ne déterminent pas conjointement la finalité et les moyens du traitement. Par conséquent, elles ne sont pas des responsables conjoints du traitement.

EXEMPLES:

1. Deux directions générales ou plus ont décidé de développer une application informatique pour gérer des projets de recherche, y compris leur programmation, les appels à projets, les évaluations, les attributions et la signature des contrats, les paiements et les informations sur les contrats en cours. Les deux DG seront-elles considérées comme des responsables conjoints du traitement?

Conformément à la définition du responsable du traitement donnée à l'article 3, point 8, du règlement, deux ou plusieurs directions générales (DG) utilisant la même application informatique pour la gestion de projets de recherche peuvent être considérées en interne comme des responsables conjoints du traitement au sein d'une institution ou d'un organe de l'Union, étant donné que la finalité a été décidée d'un commun accord et l'application conçue pour gérer les projets de recherche, sélectionner leurs propres experts et les bénéficiaires de subventions.

Comme indiqué ci-dessus dans les scénarios concernant la relation entre responsable du traitement et sous-traitant, la DG qui développe et entretient l'application informatique est le sous-traitant, qui exécute les instructions des autres DG. Dans la pratique, certaines IUE, pour clarifier les responsabilités internes, utilisent les notions de «responsable du traitement interne» (ou de «responsable du traitement en pratique») et de «sous-traitant interne» pour qualifier les départements ou entités internes à l'institution ou organe de l'Union.

Si d'autres organes de l'Union, tels que des agences exécutives ou d'un autre type ou des entreprises communes de l'Union, utilisent l'outil informatique susmentionné pour gérer les projets de recherche qui leur sont délégués, quel sera le rôle de ces organes? Dans ses avis de contrôle préalable conjoint sur la gestion des experts et sur la gestion des subventions sur le Portail des participants, le CEPD a déjà conclu qu'il s'agissait d'un cas de responsabilité conjointe du traitement entre la Commission et les agences et organes utilisant le Portail des participants[33].

2. Une application en ligne est mise au point pour soutenir un réseau de points de contact virtuels des États membres afin de partager des informations et des données de la recherche médicale concernant des maladies rares et complexes sur le territoire de l'Union. Le réseau a été mis en place conformément à une directive, et ce même acte donne mandat à l'institution A pour soutenir le réseau par l'adoption d'actes délégués et d'actes d'exécution. Ce logiciel permet l'échange d'informations entre des prestataires

[33] Joint Prior-checking Opinion regarding Grants Award and Management in the in the Participant Portal (under H2020 ÏT tools) in a number of European Union institutions - EDPS cases: C-2017-1080 REA, C- 2017-1076 SESAR, C-2017-1037 INEA, C- 2017-1068 CHAFEA, C-2017-0977 EASME and C-2017-1070 EIT.

de soins d'Europe et contient les données médicales de patients atteints de maladies rares. L'institution A a mis en place et gère l'application, qui a été mise au point par un sous-traitant. Cette plateforme contient donc, dans un répertoire central, des données médicales de patients atteints de maladies rares. L'institution A décide des catégories de données à caractère personnel qui sont traitées sur la plateforme, tandis que les prestataires de soins nationaux traitent ces données en dehors de la plateforme afin d'utiliser le système. Si l'institution A n'avait pas accès au répertoire central, cela aurait-il de l'importance?

L'institution A et les prestataires de soins déterminent conjointement la finalité et les moyens de l'application. L'institution A est légalement mandatée pour définir les mesures techniques et non techniques qui peuvent être mises en place pour les opérations de traitement des données des patients au sein de la plateforme. Elle a également mis en place la plateforme, et la gère elle-même. À l'autre bout, et conformément à la finalité et aux moyens déterminés conjointement, les prestataires de soins nationaux traitent eux aussi les données sur la santé des patients, au niveau national, afin d'utiliser le système, en veillant donc également à en informer les patients et à garantir leurs droits.

L'institution A et les prestataires de soins nationaux déterminent conjointement la finalité et les moyens des opérations de traitement, agissant ainsi en tant que responsables conjoints du traitement au sens de l'article 28 du règlement. L'important est le fait de «définir conjointement» les finalités et les moyens: même si l'institution A elle-même n'avait pas accès aux données, en raison de son rôle dans la définition du système, elle n'en resterait pas moins un responsable conjoint du traitement.

3. Un règlement crée un système d'information permettant à des autorités désignées des États membres d'échanger des informations, notamment des données à caractère personnel, en utilisant un répertoire central géré par une agence de l'Union pour faciliter la reconnaissance transfrontière de décisions prises dans un domaine d'action donné. Le même règlement attribue spécifiquement certaines tâches aux différentes parties concernées: l'agence de l'Union sera chargée de veiller à la sécurité de l'information dans le répertoire central et de fournir certaines analyses des données qui se trouvent dans le système. Les autorités des États membres, qui alimentent quant à elles le système en données, sont responsables de l'exactitude de ces données. L'agence et les autorités des États membres décident de continuer à développer le système dans le cadre d'un comité de pilotage. Le règlement ne dit pas qui informera les personnes concernées.

Il est clair qu'aucune des parties aux opérations de traitement ne serait en mesure de réaliser la finalité de façon indépendante. En outre, ce sont les parties elles-mêmes qui développent conjointement les moyens. La finalité et les moyens des opérations de traitement étant déterminés conjointement par les parties, il semble à l'évidence s'agir d'une situation de responsabilité conjointe du traitement. Le règlement portant création du système ne prévoit pas spécifiquement laquelle des parties informera les personnes concernées du traitement des données à caractère personnel en cours: les responsables conjoints du traitement doivent en décider dans l'accord conclu entre eux. Dans ce cas précis, il serait judicieux que ce soient les autorités nationales qui informent les personnes concernées du traitement de données à caractère personnel dans la base de données européenne, au moment où elles rendent leur décision et en informent ces personnes.

5.2 Quelles sont les obligations des responsables conjoints du traitement?

Une situation de responsabilité conjointe du traitement entraîne des obligations spécifiques pour les parties concernées. L'article 28, paragraphe 1, du règlement prévoit que les responsables conjoints du traitement «*[...] définissent de manière transparente leurs responsabilités respectives aux fins d'assurer le respect des obligations qui leur incombent en matière de protection des données, notamment en ce qui concerne l'exercice des droits de la personne concernée [...], par voie d'accord entre eux, sauf si, et dans la mesure où, leurs responsabilités respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables conjoints du traitement sont soumis [...]*».

Si l'étendue des obligations qui découlent de la responsabilité conjointe du traitement est vaste, le considérant 50 du règlement définit également la **«répartition claire des responsabilités» comme une condition sine qua non de la *protection des droits et libertés des personnes concernées***. Ce point de vue centré sur les personnes concernées ressort également de l'article 28, qui évoque en particulier les règles relatives à l'exercice des droits des personnes concernées et le droit à l'information. L'approche axée sur les droits fondamentaux qui est celle du règlement apparaît également dans la possibilité spécifique donnée aux responsables conjoints du traitement de créer un point de contact unique afin de faciliter l'exercice des droits des personnes concernées.

5.2.1 Les responsabilités des responsables conjoints du traitement

Comme pour les responsabilités du responsable du traitement prévues par le règlement, **la première obligation consiste donc à définir les responsabilités à l'égard du respect des obligations en matière de protection des données**.

Par conséquent, lorsque deux ou plusieurs parties agissent en tant que responsables conjoints du traitement, elles doivent clairement identifier et définir leurs responsabilités respectives en ce qui concerne les obligations spécifiques qui découlent du règlement. Dans ce contexte, il est important de ne pas oublier que **le règlement n'oblige pas les responsables conjoints du traitement à partager leurs responsabilités de façon égale**. Au sujet de la responsabilité des parties, la CJUE, dans l'affaire Wirtschaftsakademie, précise 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. Au contraire, 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*»[34].

[34] Arrêt dans l'affaire Wirtschaftskademie Schleswig-Holstein, C-210/16, point 43; arrêt dans l'affaire Jehovan todistajat, C-25/17, point 66; arrêt dans l'affaire Fashion ID GmbH & Co.KG/Verbraucherzentrale NRW eV, C-40/17, points 70 et 85.

Dès lors, **les parties impliquées dans les opérations de traitement doivent évaluer leurs rôles et leurs responsabilités en tenant compte des différents stades auxquels elles opèrent**.

La répartition claire des responsabilités peut cependant ne pas être toujours immédiatement apparente. Il est donc nécessaire de procéder à une analyse au cas par cas afin d'identifier les obligations qui incombent à chacun des responsables conjoints du traitement. Bien comprendre qui fait quoi permettra une répartition des responsabilités judicieuse – par exemple, si certains des responsables conjoints du traitement, contrairement à d'autres, doivent interagir avec les personnes concernées, il est logique d'attribuer aux premiers des responsabilités relatives à l'information des personnes concernées et au traitement de leurs demandes.

Si l'un des responsables conjoints du traitement (ou les deux) décide(nt) de recruter un sous-traitant, quelle incidence cela a-t-il sur la situation de responsabilité conjointe du traitement et sur les responsabilités établies? En bref, aucune: le fait que l'un des responsables conjoints du traitement choisisse de faire exécuter certaines opérations de traitement par un sous-traitant n'a pas d'effet sur ses obligations en tant que responsable conjoint du traitement. Dans la pratique, **les responsables conjoints du traitement peuvent souhaiter instaurer, dans l'accord conclu entre eux, des procédures spécifiques concernant le recours aux sous-traitants.** Ces procédures peuvent prévoir que, si l'une des parties décide de recruter un sous-traitant, elle doit consulter le ou les autre(s) responsable(s) du traitement sur la partie du traitement qui sera confiée à un sous-traitant et sur les aspects du contrat qui sera mis en place avec le sous-traitant. Ce n'est qu'une fois que les responsables conjoints du traitement se sont entendus sur ces points que le responsable du traitement qui recrute le sous-traitant peut conclure un contrat spécifique avec ce dernier.

5.2.2 L'accord entre les responsables conjoints du traitement

Les responsables conjoints du traitement doivent conclure un accord spécifique précisant leurs rôles et leurs responsabilités, en particulier à l'égard des personnes concernées. Il s'agit d'une obligation découlant de l'article 28 du règlement, sauf si et dans la mesure où un droit définit déjà ces rôles et ces responsabilités.

Dans certains cas, ces rôles et ces responsabilités sont déjà définis (en partie) par le droit, par exemple dans l'acte portant création d'un système d'information. En fait, l'article 28 du règlement confirme que **la législation de l'Union peut directement prévoir une répartition des rôles et des responsabilités entre les parties**. Si tel est le cas, il n'y a aucune obligation de conclure un accord, dans la mesure où les responsabilités respectives des responsables conjoints du traitement sont déterminées par le droit de l'Union ou par le droit d'un État membre. Il convient dès lors de procéder à une répartition claire des responsabilités dans le dispositif de l'acte législatif concerné (ou, pour ce qui est du droit de l'Union, au plus tard dans un acte d'exécution ou un acte délégué, lorsque l'acte de base le prévoit).

Le CEPD recommande vivement de prévoir dans les actes législatifs pertinents une répartition claire des responsabilités afin d'assurer une répartition claire des tâches entre les responsables conjoints du traitement.

Lorsque les rôles et les responsabilités des responsables conjoints du traitement ne sont que partiellement déterminés par le droit, il est nécessaire que l'accord comble toute lacune qui subsiste.

Sauf si le droit de l'Union **répartit déjà leurs responsabilités, les responsables conjoints du traitement doivent conclure un accord spécifique, prévoyant une répartition claire et transparente des responsabilités**. Un tel accord peut prendre la forme d'un protocole d'accord ou d'un contrat. En complément du protocole d'accord, il peut être recouru à un accord de niveau de service (ci-après «ANS») contenant des spécifications techniques. Un ANS peut d'ailleurs être considéré comme un accord suffisant entre les responsables conjoints du traitement, pour autant qu'il contienne tous les éléments exigés par le règlement.

S'assurer que toutes les parties concernées comprennent bien et de la même manière leurs tâches respectives est non seulement important dans le domaine de la protection des données, mais aussi en termes de bonne administration en général[35]: cela permet que les questions arrivent aux bonnes personnes et que les IUE continuent à rendre des comptes.

Aussi est-il essentiel, maintenant que nous avons circonscrit les différentes possibilités dont résulte la nécessité de conclure un accord spécifique (à moins qu'elle ne découle du droit lui-même), de souligner que cet accord:

- doit être débattu et approuvé par TOUS les responsables conjoints du traitement;
- ne peut pas être adopté unilatéralement par une seule institution ou un seul organe de l'Union;
- ne doit couvrir que les opérations de traitement pertinentes et avoir un champ d'application clairement défini (surtout lorsqu'il concerne un processus à l'interface d'autres processus que les responsables conjoints du traitement peuvent avoir mis en place);
- doit couvrir l'objet, la durée, la nature et la finalité des opérations de traitement;
- doit couvrir les catégories de données à caractère personnel et les personnes concernées par les opérations de traitement.

[35] Voir le droit à une bonne administration consacré à l'article 41 de la Charte, ainsi que le Code européen de bonne conduite administrative.

Pour ce qui est de la **substance des accords**, ceux-ci doivent au minimum couvrir les points suivants:

- les responsabilités, rôles et relations respectifs, de sorte que la licéité, la loyauté et la proportionnalité des opérations de traitement mises en place puissent être mises en évidence;
- les obligations respectives des responsables conjoints du traitement quant à la communication des informations énumérées aux articles 15 et 16 du règlement (article 28, paragraphe 1);
- les responsabilités en matière de sécurité de l'information, notamment de signalement des violations de données à caractère personnel;
- un point de contact pour les demandes des personnes concernées;
- la coopération entre les responsables conjoints du traitement en ce qui concerne les réponses aux demandes de personnes concernées et l'exercice des autres droits des personnes concernées;
- la coopération entre les responsables conjoints du traitement lors des analyses d'impact relatives à la protection des données[36];
- le ou les éventuel(s) sous-traitant(s) recruté(s) par un (ou plusieurs) des responsables du traitement.

Dans la pratique, un tel accord écrit est l'instrument juridique qui établit la relation entre les différentes parties concernées par la responsabilité conjointe du traitement. Conformément à l'article 31, paragraphe 1, point a), du règlement, la responsabilité conjointe du traitement doit être évoquée dans la partie publique du registre des activités de traitement. Nous recommandons en outre de lier le protocole d'accord ou tout autre instrument utilisé à la partie interne du registre.

5.2.3 Informer les personnes concernées des grandes lignes de l'accord

Conformément à l'article 28, paragraphe 2, du règlement, «*[l]es grandes lignes de l'accord sont mises à la disposition de la personne concernée*».

Cette disposition souligne l'importance d'identifier les rôles et les responsabilités entre les responsables conjoints du traitement, avant tout pour que les personnes concernées soient en

[36] En cas de situation de responsabilité conjointe du traitement, pour une analyse d'impact relative à la protection des données (ci-après «AIPD»), les responsables du traitement doivent convenir d'une méthode commune et réaliser cette AIPD conjointement. Dans le cas probable où les responsables du traitement ne peuvent pas être associés aux mêmes étapes de l'opération de traitement mise en place, les parties peuvent convenir d'une méthode commune tout en réalisant une AIPD séparée de l'étape particulière de l'opération de traitement à laquelle elles participent.

mesure de bien comprendre comment les responsabilités sont réparties et à qui s'adresser en premier. **Il convient de communiquer ces informations aux personnes concernées dans la déclaration relative à la protection des données.** Chacun des responsables du traitement peut avoir une déclaration relative à la protection des données distincte. Toutefois, les responsables conjoints du traitement peuvent aussi se coordonner pour établir une déclaration commune relative à la protection des données qui sera fournie aux personnes concernées. Conformément à l'article 15, paragraphe 4, et à l'article 16, paragraphe 5, point a), du règlement, il suffit d'informer une seule fois les personnes concernées par une déclaration relative à la protection des données. L'accord peut également attribuer la tâche d'informer les personnes concernées à un seul des responsables conjoints du traitement.

EXEMPLE:

Une agence de l'Union décide d'organiser un événement sur un thème donné avec une autre institution. L'agence et cette autre institution décident de répartir leurs tâches et leurs responsabilités, en particulier en ce qui concerne le traitement des données à caractère personnel des participants à l'événement.

Il est clair que la finalité globale est déterminée conjointement par les parties concernées. Le fait que les responsabilités et les tâches puissent différer pour ce qui est de l'exécution des opérations de traitement mises en place n'a pas d'incidence sur la détermination conjointe de la finalité générale. De plus, les moyens aussi peuvent être considérés comme déterminés conjointement, car les deux parties concernées s'entendent sur la manière de les employer dans le cadre de l'organisation de l'événement et du traitement des données à caractère personnel des participants. Chaque partie exécutera des tâches particulières (telles que la tenue d'une liste de diffusion, le contrôle de l'accès, etc.), mais ces mesures ne sont en place que parce qu'une finalité d'ensemble a été déterminée conjointement (l'organisation de l'événement en tant que telle). Il est donc évident que les parties concernées sont des responsables conjoints du traitement au sens de l'article 28 du règlement. En outre, dans l'accord mis en place par les parties, l'exercice des droits des personnes concernées sera clairement abordé, en prévoyant notamment les obligations de coopération entre ces parties pour répondre aux demandes des personnes concernées exerçant leurs droits. Ces obligations de coopération peuvent par exemple prévoir l'établissement d'un point de contact auquel les personnes concernées peuvent adresser leurs demandes.

5.3 Que signifie une situation de responsabilité conjointe du traitement pour l'exercice des droits des personnes concernées?

Les grandes lignes de l'accord doivent être mises à la disposition des personnes concernées pour qu'elles comprennent clairement les rôles et les responsabilités des responsables conjoints du traitement. À l'instar du RGPD, le règlement va plus loin en prévoyant qu'«*[i]ndépendamment des termes de l'accord [...], la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du*

traitement»[37]. Autrement dit, les termes de l'accord ne peuvent pas empêcher les personnes concernées d'exercer les droits qui leur sont conférés par le règlement, et qui sont spécifiquement définis au chapitre III (notamment le droit d'accès et le droit de rectification, le droit à l'effacement, à la portabilité des données et le droit de s'opposer au traitement de données).

Toutefois, dans la pratique, lorsqu'un accord en place entre les responsables conjoints du traitement prévoit des rôles et des responsabilités spécifiques, il peut être complexe pour les deux parties (ou plus) de permettre le plein exercice des droits des personnes concernées. En fait, il est fort probable que les rôles et les responsabilités définis n'octroient pas aux responsables conjoints du traitement les mêmes moyens pour permettre aux personnes concernées d'exercer leurs droits au sens du règlement (tels que le droit d'accès, d'effacement ou de limitation). À cet égard, **si les rôles et les responsabilités sont définis dans l'accord passé entre les responsables conjoints du traitement, celui-ci doit également inclure des obligations de coopération entre eux pour répondre aux demandes des personnes concernées exerçant leurs droits.** Ces obligations de coopération peuvent par exemple prévoir l'établissement d'un point de contact auquel les personnes concernées pourront adresser leurs demandes, tel qu'une adresse électronique commune. Dans la pratique, les modalités relatives aux responsabilités générales doivent être incluses dans l'accord, tandis que les détails concrets des instructions peuvent figurer dans les documents sous-jacents.

Dès lors, il est essentiel de **s'assurer qu'une personne concernée puisse toujours contacter chaque responsable conjoint du traitement pour demander l'accès aux données à caractère personnel, l'effacement de celles-ci ou une limitation**. Afin que de tels droits soient exercés, déterminer les rôles et les responsabilités exacts des responsables conjoints du traitement est donc essentiel à l'organisation adéquate de l'exercice de ces droits.

Nonobstant la possibilité qu'ont les personnes concernées d'adresser leurs demandes à chaque responsable conjoint du traitement, le CEPD recommande d'établir un point de contact unique auquel ces personnes puissent transmettre leurs demandes lorsqu'ils exercent leurs droits.

5.4 Quelles sont les responsabilités des parties impliquées dans une situation de responsabilité conjointe du traitement?

L'article 65 du règlement prévoit le droit à réparation. Il dispose que toute personne ayant subi tout dommage matériel ou moral spécifique résultant d'une violation du règlement a le droit d'obtenir la réparation du dommage subi auprès de l'institution ou de l'organe de l'Union, «*[...] sous réserve des conditions prévues par les traités*». Au sujet de ces conditions, l'article 340, deuxième alinéa, du traité sur le fonctionnement de l'Union européenne (TFUE) prévoit qu'«*[e]n matière de responsabilité non contractuelle, l'Union doit réparer,*

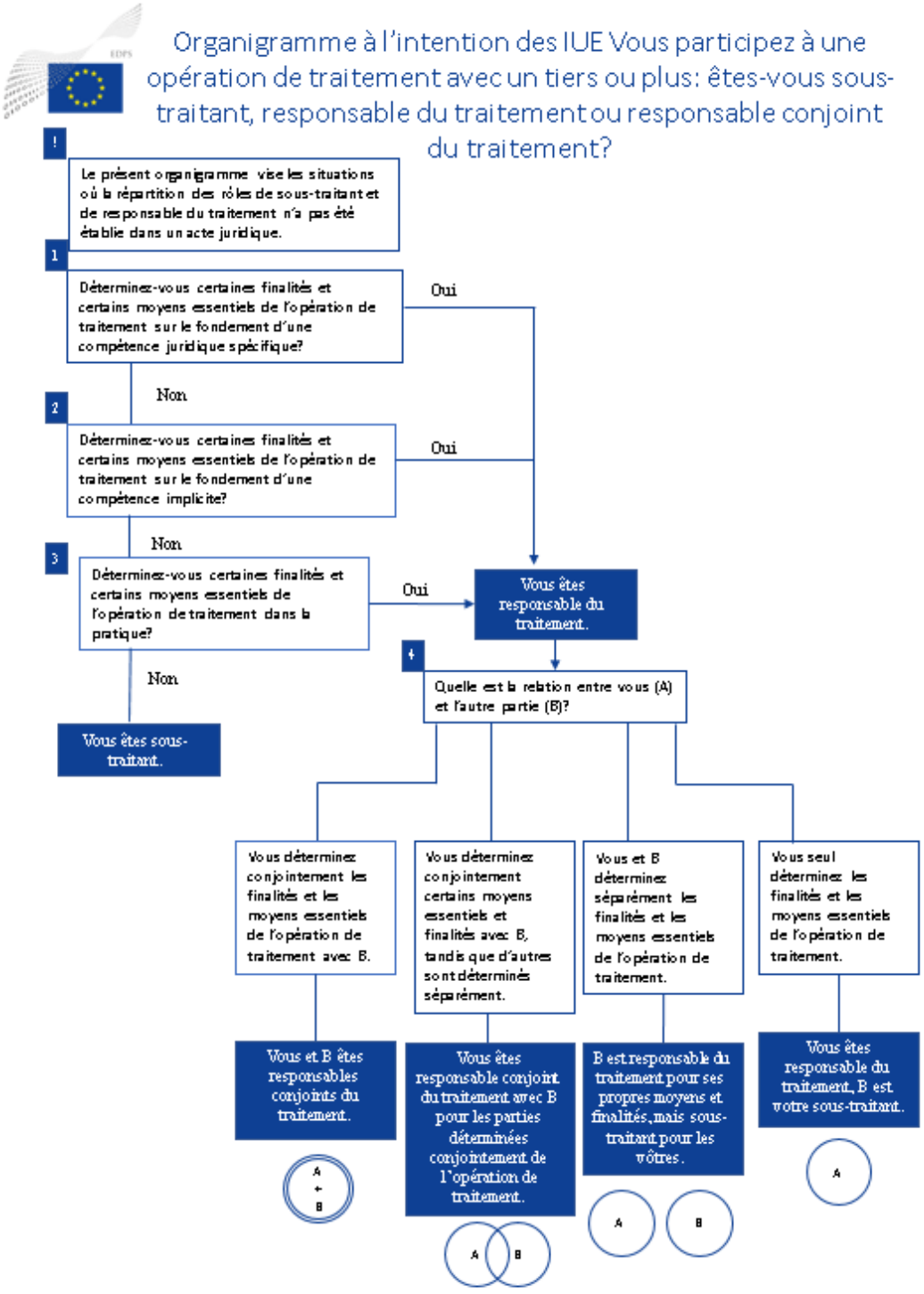
[37] Article 28, paragraphe 3, du règlement.

conformément aux principes généraux communs aux droits des États membres, les dommages causés par ses institutions ou par ses agents dans l'exercice de leurs fonctions»[38].

Contrairement aux articles 26 et 82 du RGPD, **le règlement ne traite pas spécifiquement de la responsabilité en cas de manquement**. L'article 340 du TFUE fait référence aux «principes généraux communs aux droits des États membres». Comme cela a déjà été indiqué dans le chapitre consacré à la responsabilité du traitement, l'article 268 du TFUE dispose que la Cour de justice de l'Union européenne est compétente pour connaître des litiges relatifs à la réparation des dommages visés à l'article 340 du TFUE. Les principes qui régissent la responsabilité des parties dans le cadre d'une responsabilité conjointe du traitement diffèrent donc du régime du RGPD.

[38] Article 340, paragraphe 2, TFUE.

6. Annexe 1



Remarque: l'objectif du présent organigramme est de faire apparaître clairement les conditions à remplir au départ pour être considéré comme responsable du traitement ou comme sous-traitant, et non d'expliquer ce qui se passe lorsqu'un sous-traitant outrepasse son mandat/rôle en participant à la détermination des moyens essentiels du traitement.

7. Annexe 2

Liste de contrôle 1: Quelles sont les obligations du responsable du traitement?

Le traitement de données à caractère personnel doit respecter les principes suivants:

- l'opération de traitement doit être licite, loyale et transparente («**licéité**», «**loyauté**», «**transparence**»);
- l'opération de traitement doit être liée à des finalités spécifiques («**limitation des finalités**»);
- les données à caractère personnel traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire («**minimisation des données**»);
- les données à caractère personnel doivent être exactes («**exactitude**»);
- les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire («**limitation de la conservation**»);
- les données à caractère personnel doivent rester bien sécurisées et confidentielles («**intégrité et confidentialité**»).

Voir les orientations intitulées EDPS "accountability on the ground" guidance, première partie, p. 20 à 22, ainsi que leur deuxième partie, p. 11 à 15, où figurent des questions destinées à guider le lecteur sur ces principes de protection des données.

Le responsable du traitement est responsable du respect de ces principes et doit être en mesure de démontrer ce respect («principe de responsabilité»). À cet effet, les responsables du traitement en pratique doivent, en particulier:

- documenter leurs opérations de traitement à l'aide de **registres**
  (remarque: le CEPD recommande vivement de conserver ces registres dans un **registre central à la disposition du public**);
- procéder à une analyse d'impact relative à la protection des données (**AIPD**) avant les opérations présentant un risque élevé pour les droits et libertés des personnes concernées;
- dans certaines circonstances, **consulter le CEPD** avant d'effectuer ces opérations de traitement à haut risque;
- lors de la conception des opérations de traitement, garder à l'esprit les principes de «**protection de la vie privée dès la conception**» et de «**protection de la vie privée par défaut**»;
- prendre des **mesures de sécurité adéquates** pour protéger les données à caractère personnel;
- en cas de **violation de données à caractère personnel**, la notifier au CEPD ainsi que, dans certaines circonstances, aux personnes concernées;
- conclure des **accords/contrats avec les sous-traitants** (uniquement avec ceux qui présentent des garanties suffisantes);
- en cas de **responsabilité conjointe du traitement**, conclure des accords avec les autres responsables du traitement;
- ne **transférer** des données à caractère personnel à l'intérieur de l'institution ou organe de l'Union, vers d'autres IUE, vers des pays tiers ou vers des organisations internationales que lorsque les conditions du règlement sont respectées;
- **coopérer avec le CEPD**.

Voir les orientations intitulées EDPS accountability on the ground, qui fournissent des conseils concernant les registres, les AIPD, la consultation préalable, etc.

Enfin, le responsable du traitement doit fournir **aux personnes concernées des informations claires et accessibles** sur le traitement, **respecter les droits de ces personnes** et veiller à la disponibilité des données dans la pratique.

Voir les lignes directrices du CEPD sur la transparence et les autres droits et obligations (en anglais).

8. Annexe 3

Liste de contrôle 2: Quelles sont les obligations du sous-traitant?

Pour respecter le règlement, les sous-traitants doivent, en particulier:

- ne traiter les données à caractère personnel que sur **instruction documentée du responsable du traitement**, à moins qu'ils ne soient tenus d'y procéder en vertu du droit de l'Union ou du droit d'un État membre;

- traiter les données à caractère personnel **régies par un contrat ou un acte juridique** qui lie le sous-traitant et qui énonce les conditions préalables nécessaires à l'exercice de l'activité de traitement;

- **NE PAS effectuer un traitement ultérieur** des données pour une autre finalité incompatible;

- **aider le responsable du traitement** à respecter l'obligation de garantir les **droits des personnes concernées** et à remplir les **obligations** conférées au responsable du traitement par les **articles 33 à 41** du règlement (notification des violations de la sécurité et de données, analyse d'impact relative à la protection des données et consultation préalable, confidentialité des communications électroniques, information et consultation du CEPD);

- **notifier** toute **demande** juridiquement contraignante **de communication** des données à caractère personnel traitées pour le compte du responsable du traitement et ne donner accès aux données qu'avec l'autorisation écrite préalable du responsable du traitement;

- **externaliser/sous-traiter UNIQUEMENT avec l'autorisation écrite préalable** du responsable du traitement; tenir ce dernier informé de tout changement, en lui donnant la possibilité d'émettre des objections; transmettre des obligations contractuelles identiques à tout sous-traitant;

- **tenir un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement;

- prendre des **mesures de sécurité adéquates** pour protéger les données à caractère personnel;

- en cas de **violation de données**, en informer le responsable du traitement dans les meilleurs délais;

- **coopérer** avec le CEPD, à la demande de celui-ci, dans l'exécution de ses missions.

Bruxelles, le 7 novembre 2019

Wojciech Wiewiorowski

Contrôleur européen adjoint de la protection des données