Avis du comité (article 64)

Avis 22/2024 relatif à certaines obligations découlant du recours à un ou plusieurs sous-traitant(s) ou sous-traitant(s) ultérieur(s)

Adopté le 7 octobre 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Résumé

L'autorité de contrôle (ci-après «AC») danoise a demandé au comité européen de la protection des données (ci-après «le comité» ou «l'EDPB») d'émettre un avis sur des questions d'application générale conformément à l'article 64, paragraphe 2, du règlement général de l'UE sur la protection des données (ci-après «RGPD»). L'avis contribue à une interprétation harmonisée par les autorités de contrôle nationales de certains aspects de l'article 28 du RGPD, le cas échéant lu conjointement avec le chapitre V du RGPD. En particulier, l'avis porte sur les questions relatives à l'interprétation de certaines obligations incombant aux responsables du traitement qui ont recours à des sous-traitants et sous-traitants ultérieurs, découlant notamment de l'article 28 du RGPD, ainsi que sur le libellé du contrat signé entre le responsable du traitement et le sous-traitant. Les questions portent sur le traitement des données à caractère personnel dans l'EEE ainsi que sur le traitement à la suite d'un transfert de ces données vers un pays tiers.

Le comité conclut dans cet avis que les responsables du traitement devraient disposer à tout moment des informations sur l'identité (c'est-à-dire le nom, l'adresse, la personne de contact) de tous les sous-traitants, sous-traitants ultérieurs, etc., afin qu'ils puissent remplir au mieux les obligations qui leur incombent en vertu de l'article 28 du RGPD, indépendamment du risque associé à l'activité de traitement. À cette fin, le sous-traitant devrait fournir de manière proactive au responsable du traitement toutes ces informations et les tenir à jour en permanence.

L'article 28, paragraphe 1, du RGPD prévoit que les responsables du traitement ont l'obligation de faire appel à des sous-traitants présentant des «garanties suffisantes» pour mettre en œuvre des mesures «appropriées» de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes concernées. Dans son avis, l'EDPB considère que, lors de l'évaluation du respect, par les responsables du traitement, de cette obligation et du principe de responsabilité (article 24, paragraphe 1, du RGPD), les autorités de contrôle devraient considérer que le recours à des sous-traitants ne devrait pas abaisser le niveau de protection des droits des personnes concernées. L'*obligation* du responsable du traitement de vérifier si les sous-traitants (ultérieurs) présentent des «garanties suffisantes» pour mettre en œuvre les mesures appropriées déterminées par le responsable du traitement devrait s'appliquer indépendamment du risque pesant sur les droits et libertés des personnes concernées. Toutefois, *l'étendue* de cette vérification variera, dans la pratique, en fonction de la nature de ces mesures techniques et organisationnelles, et peut donc être plus restreinte ou plus étendue en fonction du niveau de risque.

Le comité précise en outre dans son avis que, même si le sous-traitant initial doit veiller à proposer des sous-traitants ultérieurs fournissant des garanties suffisantes, la décision finale de faire appel à un sous-traitant ultérieur et la responsabilité correspondante, y compris en ce qui concerne la vérification des garanties, restent du ressort du responsable du traitement. Les AC devraient évaluer si le responsable du traitement est en mesure de démontrer que la vérification du caractère suffisant des garanties fournies par ses sous-traitants (ultérieurs) a eu lieu à la satisfaction du responsable du traitement. Le responsable du traitement peut choisir de s'appuyer sur les informations reçues de son sous-traitant et de les compléter si nécessaire (par exemple, lorsqu'elles semblent incomplètes, inexactes ou qu'elles soulèvent des questions). Plus précisément, pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait

augmenter son niveau de vérification en ce qui concerne le contrôle des informations fournies. À cet égard, le comité considère qu'en vertu du RGPD, le responsable du traitement n'a pas l'obligation de demander la présentation systématique des contrats de sous-traitance ultérieure afin de vérifier si les obligations en matière de protection des données prévues dans le contrat initial ont été transmises en aval de la chaîne de traitement. Le responsable du traitement devrait évaluer, au cas par cas, s'il est nécessaire de demander une copie des contrats précités ou de les réexaminer lorsque cela est nécessaire pour être en mesure de démontrer la conformité à la lumière du principe de responsabilité.

Lorsque des transferts de données à caractère personnel en dehors de l'EEE ont lieu entre deux sous-traitants (ultérieurs), conformément aux instructions du responsable du traitement, ce dernier reste soumis aux obligations découlant de l'article 28, paragraphe 1, du RGPD concernant les «garanties suffisantes», en plus de celles prévues à l'article 44, pour veiller à ce que le niveau de protection garanti par le RGPD ne soit pas amoindri par les transferts de données à caractère personnel. Le sous-traitant/l'exportateur devrait préparer la documentation pertinente, conformément à la jurisprudence et comme expliqué dans les recommandations 01/2020 de l'EDPB. Le responsable du traitement devrait évaluer et être en mesure de présenter ladite documentation pertinente à l'autorité de contrôle compétente. Le responsable du traitement peut s'appuyer sur la documentation ou les informations reçues du sous-traitant/de l'exportateur et, si nécessaire, les compléter. L'étendue et la nature de l'obligation du responsable du traitement d'évaluer cette documentation peuvent dépendre du motif du transfert et du caractère initial ou ultérieur du transfert.

Le comité a également abordé, dans son avis, une question sur le libellé du contrat entre le responsable du traitement et le sous-traitant. À cet égard, un élément fondamental est l'engagement du sous-traitant à ne traiter des données à caractère personnel que sur instruction documentée du responsable du traitement, à moins que le sous-traitant ne soit «*soit tenu [de procéder au traitement] en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» [article 28, paragraphe 3, point a), du RGPD], rappelant le principe général selon lequel les contrats ne peuvent pas prévaloir sur la loi. Compte tenu de la liberté contractuelle accordée aux parties pour adapter le contrat entre le responsable du traitement et le sous-traitant à leur situation, dans les limites de l'article 28, paragraphe 3, du RGPD, le comité estime que l'inclusion des mots «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» (soit textuellement, soit dans des termes très similaires) est fortement recommandée, mais pas obligatoire.

En ce qui concerne les variantes similaires à «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*», le comité estime que cela reste de la prérogative de la liberté contractuelle des parties et ne viole pas, en soi, l'article 28, paragraphe 3, point a), du RGPD. Dans le même temps, le comité recense un certain nombre de problèmes dans son avis, étant donné qu'une telle clause n'exonère pas le sous-traitant du respect des obligations qui lui incombent en vertu du RGPD.

En ce qui concerne les données à caractère personnel transférées en dehors de l'EEE, l'EDPB considère qu'il est peu probable que les termes «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» suffisent en soi à assurer le respect de l'article 28, paragraphe 3, point a), lu conjointement avec le chapitre V, du RGPD. Comme l'illustrent les clauses contractuelles types (CCT) de la Commission européenne pour le transfert de données à

caractère personnel vers des pays tiers et les recommandations relatives aux règles d'entreprise contraignantes pour les responsable du traitement (les «recommandations BCR-C», l'article 28, paragraphe 3, point a), du RGPD ne s'oppose pas — en principe — à l'inclusion dans le contrat de dispositions relatives aux exigences légales de pays tiers en matière de traitement des données à caractère personnel transférées. Toutefois, comme c'est le cas dans ces documents, il convient d'établir une distinction entre les lois des pays tiers qui porteraient atteinte au niveau de protection garanti par le RGPD et celles qui ne le feraient pas. Enfin, le comité rappelle que la possibilité que le droit d'un pays tiers entrave le respect du RGPD devrait être un facteur pris en considération par les parties avant la conclusion du contrat (entre le responsable du traitement et le sous-traitant ou entre le sous-traitant et le sous-traitant ultérieur).

Lorsque le sous-traitant traite des données à caractère personnel dans l'EEE, il peut toujours être confronté, dans certaines circonstances, au droit d'un pays tiers. Le comité souligne que l'ajout dans le contrat d'un libellé signifiant «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» n'a pas pour effet de libérer le sous-traitant de ses obligations au titre du RGPD.

Enfin, le comité est d'avis que le fait de faire suivre l'engagement du sous-traitant de ne procéder au traitement que sur instruction documentée de la mention «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» (soit textuellement, soit dans des termes très similaires) ne saurait être interprété comme une instruction documentée fournie par le responsable du traitement.

Table des matières

Le comité européen de la protection des données

vu l'article 63 et l'article 64, paragraphe 2, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

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

vu les articles 12 et 22 de son règlement intérieur,

considérant ce qui suit:

(1) La mission principale du comité européen de la protection des données (ci-après «le comité» ou «EDPB») est de veiller à l'application cohérente du RGPD dans l'ensemble de l'Espace économique européen (ci-après «EEE»). Conformément à l'article 64, paragraphe 2, du RGPD, toute autorité de contrôle (ci-après «AC»), la présidente de l'EDPB ou la Commission peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres de l'EEE soit examinée par l'EDPB en vue d'obtenir un avis. Le présent avis vise à examiner une question d'application générale ou qui produit des effets dans plusieurs États membres de l'EEE.

(2) L'avis de l'EDPB est adopté conformément à l'article 64, paragraphe 3, du RGPD, lu conjointement avec l'article 10, paragraphe 2, du règlement intérieur de l'EDPB, dans un délai de huit semaines à compter du premier jour ouvrable suivant la date à laquelle la présidente de l'EDPB et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision de la présidente, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

A ADOPTÉ LE PRÉSENT AVIS:

1 INTRODUCTION

1.1 Résumé des faits

1. Le 5 juillet 2024, l'autorité de contrôle danoise (ci-après «l'AC danoise») a demandé au comité européen de la protection des données (ci-après «le comité» ou «l'EDPB») d'émettre un avis sur les obligations de responsabilité des responsables du traitement en ce qui concerne la chaîne de traitement et la relation entre les responsables du traitement et leurs sous-traitants (ultérieurs) (ci-après «la demande»).

2. L'AC danoise a déclaré le dossier complet le 8 juillet 2024. La présidente de l'EDPB a considéré que le dossier était complet le 9 juillet 2024. À la même date, le dossier a été diffusé par le secrétariat de

[1] Dans le présent avis, on entend par «États membres» les «États membres de l'EEE». Dans le présent avis, on entend par «Union» l'«EEE».

l'EDPB. La présidente de l'EDPB, compte tenu de la complexité de la question, a décidé de prolonger le délai légal conformément à l'article 64, paragraphe 3, du RGPD et à l'article 10, paragraphe 4, du règlement intérieur de l'EDPB.

3. L'AC danoise renvoie également, dans sa demande, au rapport adopté par l'EDPB en janvier 2023 sur les conclusions de sa première action coordonnée de mise en application[2] au sein du cadre d'application coordonné (Coordinated Enforcement Framework, ci-après «CEF»)[3]. Cette action coordonnée s'est concentrée sur l'utilisation de services en nuage par le secteur public. Dans le rapport de l'EDPB, les autorités de contrôle participant à l'action coordonnée ont recensé huit défis, en particulier en ce qui concerne l'utilisation des services en nuage par les organismes publics, et ont fourni une liste de points saillants que les parties prenantes concernées doivent prendre en considération lors de l'évaluation de services en nuage et de l'engagement de fournisseurs de services en nuage[4]. Si, pour la plupart de ces points, l'étendue des obligations imposées par le RGPD est claire tant pour les responsables du traitement que pour les sous-traitants, l'étendue précise de certaines obligations au titre du RGPD reste floue selon l'AC danoise[5].

Les questions suivantes ont été posées par l'AC danoise:

4. Question 1.1: Compte tenu de l'article 5, paragraphe 2, et de l'article 24, paragraphe 1, du RGPD, lorsqu'il est fait appel à un sous-traitant pour effectuer un traitement pour le compte du responsable du traitement, afin de démontrer le respect *notamment* de l'article 28, paragraphe 1, et de l'article 28, paragraphe 2 (y compris lors de la présentation des documents à l'autorité de contrôle lors de l'inspection):

   a. Le responsable du traitement doit-il identifier tous les sous-traitants ultérieurs du sous-traitant, leurs sous-traitants respectifs, etc. tout au long de la chaîne de traitement, ou seulement la première ligne de sous-traitants ultérieurs engagés par le sous-traitant?

   b. dans quelle mesure et à quel niveau de détail le responsable du traitement doit-il vérifier et documenter:

      i. le caractère suffisant des garanties fournies par les sous-traitants, leurs sous-traitants ultérieurs, etc. ;
      ii. le contenu des contrats conclus entre le sous-traitant initial et les sous-traitants supplémentaires afin de déterminer si les mêmes obligations ont été imposées aux sous-traitants supplémentaires conformément à l'article 28, paragraphe 4, du RGPD; et
      iii. si les sous-traitants, leurs sous-traitants ultérieurs, etc. satisfont aux exigences du responsable du traitement au titre de l'article 28, paragraphe 1, du RGPD?

5. Question 1.2: En cas de transferts ou de transferts ultérieurs d'un sous-traitant (ultérieur) vers un autre sous-traitant (ultérieur) conformément aux instructions du responsable du traitement: dans quelle mesure le responsable du traitement doit-il, dans le cadre de son obligation au titre de l'article 28, paragraphe 1, du RGPD, lu conjointement avec l'article 44 du RGPD, évaluer et être en mesure de

[2] Rapport sur l'action coordonnée de mise en application de 2022 — Utilisation des services en nuage par le secteur public, 17 janvier 2023 (ci-après le «rapport CEF sur les services en nuage»).
[3] Le cadre d'application coordonné (CEF) a été mis en place par l'EDPB en octobre 2020 en vue de rationaliser l'application de la législation et la coopération entre les autorités de contrôle. Voir le document du Comité européen de la protection des données sur le cadre d'application coordonné en vertu du règlement (UE) 2016/679, adopté le 20 octobre 2020, version 1.1.
[4] Rapport CEF sur les services en nuage, p. 10-20.
[5] Demande, p. 1.

produire des documents provenant de sous-traitants (ultérieurs) attestant que le niveau de protection des données à caractère personnel n'est pas compromis par les transferts (ultérieurs)?

6. Question 1.3: L'étendue des obligations découlant de l'article 28, paragraphe 1, et de l'article 28, paragraphe 2, du RGPD, lus conjointement avec l'article 5, paragraphe 2, et l'article 24 du RGPD, comme indiqué à la question 1.1 et à la question 1.2, varie-t-elle en fonction du risque associé à l'activité de traitement? Dans l'affirmative, quelle est l'étendue de ces obligations pour les activités de traitement à faible risque et quelle est l'étendue de ces obligations pour les activités de traitement à haut risque?

7. Question 2: Un contrat ou un autre acte juridique en vertu du droit de l'Union ou de l'État membre conformément à l'article 28, paragraphe 3, du RGPD doit-il contenir l'exception prévue à l'article 28, paragraphe 3, point a): «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» (que ce soit textuellement ou dans des termes très similaires) afin d'être conforme au RGPD?

8. Question 2a: si la réponse à la question 2 est négative, lorsqu'un contrat ou un autre acte juridique en vertu du droit de l'Union ou de l'État membre élargit l'exception prévue à l'article 28, paragraphe 3, point a), du RGPD pour couvrir également le droit des pays tiers en général (par exemple, avec la mention «à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental»), cela constitue-t-il en soi une violation de l'article 28, paragraphe 3, point a), du RGPD?

9. Question 2b: Si la réponse à la question 2a est négative, cette exception élargie doit-elle être interprétée comme une instruction documentée émise par le responsable du traitement au sens de l'article 28, paragraphe 3, point a), du RGPD?

1.2 Recevabilité de la demande d'avis au titre de l'article 64, paragraphe 2, du RGPD

10. Conformément à l'article 64, paragraphe 2, du RGPD, toute autorité de contrôle peut demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité en vue d'obtenir un avis.

11. Les premières questions posées par l'AC danoise concernent les obligations de responsabilité des responsables du traitement au titre de l'article 28 du RGPD (questions 1.1, 1.2 et 1.3), tandis que la dernière question porte sur le contenu spécifique du contrat entre le responsable du traitement et le sous-traitant ou de l'acte juridique au titre de l'article 28, paragraphe 3, point a), du RGPD (question 2).

12. Le comité estime que ces questions sont liées à l'interprétation du RGPD, en particulier en ce qui concerne la relation entre les responsables du traitement et ses sous-traitants (ultérieurs) et à l'interprétation de l'article 5, paragraphe 2, de l'article 24 et de l'article 28 du RGPD. La demande est liée, d'une part, aux obligations de responsabilité des responsables du traitement et au niveau de documentation que les autorités de contrôle devraient attendre de tout responsable du traitement faisant appel à des sous-traitants (ultérieurs) pour effectuer des activités de traitement en leur nom et, d'autre part, au contenu des contrats ou des actes juridiques entre le responsable du traitement et le sous-traitant. Par conséquent, la présente demande concerne une «*question d'application générale*» au sens de l'article 64, paragraphe 2, du RGPD.

13. En outre, le comité considère que la demande de l'autorité de contrôle danoise est motivée conformément à l'article 10, paragraphe 3, du règlement intérieur de l'EDPB, étant donné que l'autorité de contrôle danoise a avancé des arguments en faveur de la nécessité d'une interprétation cohérente des questions abordées dans la demande.

14. Conformément à l'article 64, paragraphe 3, du RGPD, l'EDPB n'émet pas d'avis s'il a déjà émis un avis sur la question[6]. L'EDPB n'a pas encore répondu aux questions soulevées par la demande de l'autorité de contrôle danoise. En outre, même si les lignes directrices disponibles de l'EDPB, y compris en particulier les lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant[7] (ci-après les «lignes directrices 07/2020 de l'EDPB»), fournissent certaines orientations sur l'étendue des obligations de responsabilité du responsable du traitement au titre de l'article 28 du RGPD, les orientations existantes ne répondent pas pleinement à toutes les questions énoncées dans la demande[8]. Plus précisément, par exemple, les orientations disponibles concernant l'article 28, paragraphe 3, point a), du RGPD ne répondent pas spécifiquement à la question incluse dans la demande de l'AC danoise, à savoir si les termes «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» doivent être inclus dans les contrats ou les actes juridiques entre le responsable du traitement et le sous-traitant.

15. Pour ces raisons, le comité estime que la demande de l'AC danoise est recevable et que les questions soulevées par la demande de l'AC danoise devraient être analysées dans un avis adopté conformément à l'article 64, paragraphe 2, du RGPD.

2 SUR LE FOND DE LA DEMANDEERROR! BOOKMARK NOT DEFINED.

2.1 Sur l'interprétation de l'article 28, paragraphes 1, 2, et 4 du RGPD, lus conjointement avec l'article 5, paragraphe 2, et l'article 24, paragraphe 1, du RGPD (questions 1.1 et 1.3)

16. Cette section traite des questions 1.1 et 1.3 adressées au comité, telles que reproduites dans la section «recevabilité» ci-dessus.

17. L'article 28 du RGPD définit la relation entre le responsable du traitement et le sous-traitant et impose des obligations directes aux responsables du traitement et aux sous-traitants. À titre préliminaire, il convient de noter que le RGPD définit le «sous-traitant» à l'article 4, paragraphe 8, d'une manière générale qui inclut à la fois le sous-traitant initial engagé directement par le responsable du traitement et le sous-traitant du sous-traitant, et ainsi de suite tout au long de la chaîne de traitement.

18. L'EDPB souligne que l'évaluation du rôle des parties (et la question de savoir si elles agissent en tant que responsables uniques ou conjoints du traitement ou en tant que sous-traitants) ne relève pas du champ d'application de la demande. L'EDPB rappelle qu'il appartient principalement aux parties d'évaluer leur rôle effectif en fonction d'éléments factuels ou de circonstances de l'espèce[9], sans préjudice de la compétence de l'AC de vérifier si leur évaluation est juste.

19. À la lumière des questions qui précèdent, le présent avis se concentre uniquement sur la portée et l'étendue des obligations qui incombent au responsable du traitement en vertu de l'article 28,

[6] Article 64, paragraphe 3, du RGPD et article 10, paragraphe 4, du règlement intérieur de l'EDPB.
[7] Voir les lignes directrices 07/2020 de l'EDPB concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.1, adoptées le 7 juillet 2021.
[8] Voir notamment les lignes directrices 07/2020 de l'EDPB, section 1.1 «Choix du sous-traitant» à la page 35, section 1.3.4 «*Le sous-traitant doit respecter les conditions visées à l'article 28, paragraphes 2 et 4, pour recruter un autre sous-traitant [article 28, paragraphe 3, point d), du RGPD]*» à la page 43, section 1.6 «Sous-traitants ultérieurs», à la page 48.
[9] Lignes directrices 07/2020 de l'EDPB, paragraphe 12.

paragraphe 1, du RGPD, de vérifier si les sous-traitants (ultérieurs) fournissent des «garanties suffisantes», en vertu de l'article 28, paragraphe 2, et sur les obligations de responsabilité qui incombent au responsable du traitement en vertu de l'article 5, paragraphe 2, et de l'article 24, paragraphe 1, du RGPD[10].

20. En outre, le comité note que les questions ci-dessus ne concernent pas la responsabilité du responsable du traitement à l'égard des personnes concernées pour les activités de traitement menées pour son compte, par exemple en ce qui concerne le droit à réparation des personnes concernées au titre de l'article 82 du RGPD. La présente section s'attachera donc à fournir des précisions aux autorités de contrôle en ce qui concerne l'interprétation de l'article 28, paragraphes 1 et 2, du RGPD, lu conjointement avec l'article 5, paragraphe 2, et l'article 24 du RGPD, sur certaines obligations découlant du recours à des sous-traitants et à des sous-traitants ultérieurs. Afin de répondre à ces questions, la chambre de recours mènera une analyse axée sur les situations dans lesquelles il n'y a pas de transfert de données à caractère personnel en dehors de l'EEE. En revanche, la section ci-dessous consacrée à la question 1.2 évalue les situations dans lesquelles des transferts ont lieu tout au long de la chaîne de traitement.

2.1.1 Identification des acteurs de la chaîne de traitement

21. En ce qui concerne la question de savoir si, en substance, le responsable du traitement devrait identifier tous les sous-traitants ultérieurs du sous-traitant, leurs sous-traitants ultérieurs, etc. tout au long de la chaîne de traitement, ou seulement identifier la première ligne de sous-traitants ultérieurs engagés par le sous-traitant, le comité rappelle tout d'abord que «*bien que la chaîne [du traitement] puisse être assez longue, le responsable du traitement conserve son rôle central dans la détermination de la finalité et des moyens du traitement*»[11].

22. L'EDPB interprète les termes «identifier» et «informations sur l'identité» aux fins de la réponse à la question comme faisant référence au nom, à l'adresse, à la personne de contact (nom, fonction, coordonnées) du sous-traitant et à la description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés)[12].

23. En ce qui concerne le choix des sous-traitants, les responsables du traitement devraient être en mesure de déterminer efficacement les finalités et les moyens du traitement, conformément à l'article 4, paragraphe 7, du RGPD. À cet égard, la détermination des destinataires (y compris les sous-traitants) est considérée comme un «moyen essentiel» du traitement, sur lequel le responsable du traitement décide[13].

---

[10] Cette question est distincte et indépendante de toute autre obligation incombant au responsable du traitement [ou aux sous-traitants (ultérieurs)] visant à garantir le respect du RGPD, par exemple du principe de licéité du traitement, des obligations au titre de l'article 32 ou du chapitre V du RGPD. Le responsable du traitement peut toujours être tenu responsable des traitements sous sa responsabilité qui ne sont pas conformes auxdites dispositions du RGPD, même s'il a satisfait aux obligations de vérification de ses sous-traitants (ultérieurs) conformément à l'article 28, paragraphe 1, du RGPD, telles que détaillées dans le présent avis, et le présent avis ne traite pas de la responsabilité du responsable du traitement en ce qui concerne le respect des dispositions du RGPD autres que celles énoncées à l'article 24, paragraphe 1, et à l'article 28, paragraphes 1 et 2 du RGPD.

[11] Lignes directrices 07/2020 de l'EDPB, paragraphe 152.

[12] Cela reflète les informations requises pour l'identification des sous-traitants à l'annexe IV des CCT entre responsables du traitement et sous-traitants (décision d'exécution 2021/915 de la Commission du 4 juin 2021) et à l'annexe III des CCT de la Commission pour le transfert de données vers des pays tiers (décision d'exécution 2021/914 de la Commission du 4 juin 2021).

[13] Lignes directrices 07/2020 de l'EDPB, paragraphe 40.

24. À cette fin, en ce qui concerne l'engagement de **sous-traitants supplémentaires** par le sous-traitant initial, l'autorisation écrite spécifique ou générale préalable du responsable du traitement est nécessaire en vertu de l'article 28, paragraphe 2, du RGPD. Les lignes directrices 07/2020 de l'EDPB clarifient que les obligations prévues à l'article 28, paragraphe 2 «*sont déclenchées lorsqu'un sous-traitant (ultérieur) envisage de recruter un autre acteur, ajoutant ainsi un maillon supplémentaire à la chaîne, en lui confiant des activités nécessitant le traitement de données à caractère personnel*»[14].

25. Lorsque le responsable du traitement décide d'accepter certains sous-traitants ultérieurs au moment de la signature du contrat, une liste des sous-traitants ultérieurs agréés devrait figurer dans le contrat ou dans une annexe à celui-ci. Cette liste devrait ensuite être tenue à jour, conformément à l'autorisation générale ou spécifique donnée par le responsable du traitement[15].

26. En ce qui concerne l'engagement de sous-traitants ultérieurs, le RGPD envisage la possibilité d'une autorisation générale ou spécifique. **En cas d'autorisation spécifique**, le responsable du traitement devrait préciser par écrit quel sous-traitant ultérieur est autorisé, pour quelle activité de traitement spécifique et pour quelle durée[16]. Si la demande d'autorisation spécifique du sous-traitant n'a pas reçu de réponse dans le délai imparti, elle devrait être considérée comme rejetée[17].

27. **En cas d'autorisation générale**, le sous-traitant devrait donner au responsable du traitement la possibilité d'approuver une liste de sous-traitants ultérieurs au moment de la signature de l'autorisation générale et la possibilité – y compris dans un délai suffisant – de s'opposer à tout changement concernant les sous-traitants ultérieurs[18]. Le comité rappelle qu'il devrait appartenir au **sous-traitant initial de fournir proactivement certaines informations** au responsable du traitement et que «*l'obligation du sous-traitant d'informer le responsable du traitement de tout changement de sous-traitant ultérieur implique que le sous-traitant indique ou signale **activement** ces changements à l'égard du responsable du traitement*»[19].

28. Cela signifie que les informations relatives à l'identification de tous les sous-traitants ultérieurs du sous-traitant doivent être facilement accessibles au responsable du traitement. L'identification de ces

[14] Les lignes directrices 07/2020 de l'EDPB, paragraphe 151, disposent que: *«Les activités de traitement des données sont souvent effectuées par un grand nombre d'acteurs et les chaînes de sous-traitance deviennent de plus en plus complexes. Le RGPD introduit des obligations spécifiques qui sont déclenchées lorsqu'un sous-traitant (ultérieur) envisage de recruter un autre acteur, ajoutant ainsi un maillon supplémentaire à la chaîne, en lui confiant des activités nécessitant le traitement de données à caractère personnel. La question de savoir si le prestataire de services agit comme un sous-traitant ultérieur devrait être analysée conformément à ce qui a été décrit plus haut à propos de la notion de sous-traitant»*.

[15] Lignes directrices 07/2020 de l'EDPB, paragraphe 154.

[16] Lignes directrices 07/2020 de l'EDPB, paragraphes 153 et 155. En vertu de la clause 7.7, option 1, des CCT de la CE entre responsables du traitement et sous-traitants, la liste des sous-traitants ultérieurs spécifiquement autorisés par le responsable du traitement figure à l'annexe IV, qui doit être tenue à jour.

[17] Lignes directrices 07/2020 de l'EDPB, paragraphe 155.

[18] Voir également les lignes directrices 07/2020 de l'EDPB, paragraphe 156: «*Le responsable du traitement peut également donner une autorisation générale au recours à des sous- traitants ultérieurs (contractuellement, en incluant une liste de ces sous-traitants ultérieurs dans une annexe), (...)*». L'avis 14/2019 de l'EDPB sur le projet de CCT présenté par l'AC danoise (article 28, paragraphe 8, du RGPD) est également pertinent dans ce contexte. En vertu de la clause 7.7, option 2, des CCT de la CE entre responsables du traitement et sous-traitants, le sous-traitant dispose de l'autorisation générale du responsable du traitement pour le recrutement de sous-traitants ultérieurs à partir d'une liste convenue et informe expressément le responsable du traitement, à l'avance et par écrit, de toute modification envisagée de cette liste résultant de l'ajout ou du remplacement de sous-traitants ultérieurs.

[19] Lignes directrices 07/2020 de l'EDPB, paragraphe 128 (soulignement ajouté). Voir également la note de bas de page nº 14.

acteurs est particulièrement importante pour que le responsable du traitement puisse contrôler les activités de traitement dont il est responsable et puisse être tenu pour responsable en cas de violation du RGPD.

29. Le sous-traitant doit donc fournir toutes les informations sur la manière dont l'activité de traitement sera effectuée pour le compte du responsable du traitement, y compris des informations sur le sous-traitant ultérieur utilisé[20] et une description du traitement confié au sous-traitant ultérieur[21].

30. D'autres raisons juridiques justifient la nécessité pour le responsable du traitement d'identifier tous les sous-traitants et sous-traitants ultérieurs. Les sous-traitants auxquels les données sont divulguées ou transférées sont considérés comme des «destinataires»[22].

- Afin de respecter les exigences de transparence prévues à l'article 13, paragraphe 1, point e), et à l'article 14, paragraphe 1, point e), du RGPD, les responsables du traitement devraient informer les personnes concernées des destinataires de données ou des catégories de destinataires de données, de manière aussi spécifique et concrète que possible[23]. Les informations relatives aux «catégories de destinataires» doivent également figurer dans le registre des activités de traitement [article 30, paragraphe 1, point d), du RGPD].

- L'article 15 du RGPD prévoit le droit d'accès, entre autres, aux informations sur les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées[24]. La Cour de justice a précisé que cette disposition implique l'obligation pour le responsable du traitement de fournir à la personne concernée l'identité réelle des destinataires[25]. En dehors du type de cas dans

[20] Lignes directrices 7/2020 de l'EDPB, paragraphe 143.

[21] Voir, par exemple, l'annexe IV des CCT de la CE entre responsables du traitement et sous-traitants et l'annexe II des CCT de la CE pour le transfert de données vers des pays tiers.

[22] Article 4, paragraphe 9, du RGPD; Groupe de travail «Article 29» Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, adoptées le 29 novembre 2017, version révisée et adoptée le 11 avril 2018, WP260 rev.01, approuvées par le comité européen de la protection des données (ci-après les «lignes directrices du GT «Article 29» sur la transparence»), p. 37.

[23] Lignes directrices du GT «Article 29» sur la transparence, p. 45 («Conformément au principe d'équité, les responsables du traitement doivent fournir aux personnes concernées les informations les plus significatives sur les destinataires. *En pratique, il s'agit généralement de destinataires nommément désignés afin que les personnes concernées puissent savoir exactement qui détient leurs données à caractère personnel. Si les responsables du traitement choisissent de communiquer les catégories de destinataires, les informations devraient être les plus spécifiques possible et indiquer le type de destinataire (en fonction des activités qu'il mène), l'industrie, le secteur et le sous-secteur ainsi que l'emplacement des destinataires*»); Lignes directrices 01/2022 sur les droits des personnes concernées — Droit d'accès, version 2.1, adoptées le 28 mars 2023, (ci-après «Lignes directrices 01/2022 de l'EDPB (droit d'accès)»), paragraphe 117 («*les articles 13 et 14 du RGPD indiquent déjà que les informations sur les destinataires ou les catégories de destinataires devraient être aussi concrètes que possible dans le respect des principes de transparence et d'équité*»); voir CJUE, arrêt du 12 janvier 2023, *RW c. Österreichische Post AG*, C-154/21, point 25; avis de l'avocat général portant sur CJUE C-154/21, point 36 («*Les articles 13 et 14 du RGPD [...] fixent une obligation pour le responsable du traitement de fournir à la personne concernée les informations relatives aux catégories de destinataires ou aux destinataires concrets des données à caractère personnel la concernant lorsque celles-ci sont ou ne sont pas collectées auprès de la personne concernée*»).

[24] Article 15, paragraphe 1, point c), du RGPD. Lignes directrices 01/2022 de l'EDPB (droit d'accès), paragraphes 116 à 117.

[25] Arrêt de la CJUE du 12 janvier 2023, *RW c. Österreichische Post AG*, C-154/21, point 51: «*l'article 15, paragraphe 1, sous c), du RGPD doit être interprété en ce sens que le droit d'accès de la personne concernée aux*

lesquels le responsable du traitement peut indiquer à la personne concernée uniquement les catégories de destinataires, il devrait en principe toujours être possible pour le responsable du traitement de récupérer les noms des destinataires et de fournir les informations nécessaires aux personnes concernées dans les meilleurs délais.

- L'article 19 du RGPD prévoit que le responsable du traitement communique toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement à chaque destinataire auquel les données à caractère personnel ont été communiquées, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. La CJUE a précisé que la seconde phrase de l'article 19 confère expressément à la personne concernée le droit d'être informée des destinataires concrets des données la concernant[26].

31. Bien que cela ne soit pas explicite dans ces dispositions, le comité estime qu'aux fins de l'article 28, paragraphe 1, et de l'article 28, paragraphe 2, du RGPD, les responsables du traitement devraient disposer à tout moment d'informations concernant l'identité de tous les sous-traitants, sous-traitants ultérieurs, etc.[27], afin qu'ils puissent remplir au mieux les obligations qui leur incombent en vertu des dispositions susmentionnées. Cette disponibilité est également nécessaire pour que les responsables du traitement puissent collecter et évaluer toutes les informations nécessaires pour satisfaire aux exigences du RGPD, y compris pour qu'ils puissent répondre aux demandes d'accès au titre de l'article 15 du RGPD sans retard injustifié et réagir rapidement aux violations de données survenant tout au long de la chaîne de traitement. Cela s'appliquerait quel que soit le risque associé à l'activité de traitement.

32. À cette fin, le sous-traitant devrait fournir de manière proactive[28] au responsable du traitement toutes les informations sur l'identité de tous les sous-traitants, sous-traitants ultérieurs, etc. traitant des données pour le compte du responsable du traitement, et devrait tenir à jour en permanence les informations concernant l'ensemble des sous-traitants ultérieurs engagés. Le responsable du traitement et le sous-traitant peuvent inclure dans le contrat des détails supplémentaires concernant les modalités de livraison et le format dans lequel le sous-traitant est tenu de fournir ces informations,

---

données à caractère personnel la concernant, prévu par cette disposition, implique, lorsque ces données ont été ou seront communiquées à des destinataires, l'obligation pour le responsable du traitement de fournir à cette personne l'identité même de ces destinataires, à moins qu'il ne soit impossible d'identifier ces destinataires ou que ledit responsable du traitement ne démontre que les demandes d'accès de la personne concernée sont manifestement infondées ou excessives, au sens de l'article 12, paragraphe 5, du RGPD, auxquels cas celui-ci peut indiquer à cette personne uniquement les catégories de destinataires en cause».
La Cour a reconnu que la personne concernée peut également «*choisir de se borner à demander des informations concernant les catégories de destinataires*». Arrêt de la CJUE du 12 janvier 2023, *RW c. Österreichische Post AG*, C-154/21, point 43.
Lignes directrices 01/2022 de l'EDPB (droit d'accès), paragraphe 117.

[26] Arrêt de la CJUE du 12 janvier 2023, *RW c. Österreichische Post AG*, C-154/21, point 41.

[27] Ces informations sont nécessaires pour que le responsable du traitement soit en mesure de remplir ses obligations également en cas de rupture de la chaîne de sous-traitance parce qu'un sous-traitant (ultérieur) est injoignable, en faillite ou non disposé à coopérer, et qu'un autre sous-traitant (ultérieur) doit être contacté.

[28] Afin de se conformer à l'article 28, paragraphe 2, du RGPD, pour permettre au responsable du traitement de décider de l'ajout de sous-traitants ultérieurs, ainsi que pour se conformer à l'article 28, paragraphe 1, du RGPD, afin de permettre au responsable du traitement de vérifier si les sous-traitants (ultérieurs) présentent des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles.

car le responsable du traitement peut souhaiter obtenir un format spécifique afin qu'il soit plus facile pour lui de récupérer ces données et de les organiser.

2.1.2 Vérification et documentation par le responsable du traitement du caractère suffisant des garanties fournies par tous les sous-traitants de la chaîne de traitement

33. Les questions 1.1.b.i, 1.1.b.iii et 1.3 visent à préciser dans quelle mesure et à quel niveau de détail le responsable du traitement devrait vérifier et documenter le caractère suffisant des garanties fournies par tous les sous-traitants de la chaîne de traitement et dans quelle mesure les obligations au titre de l'article 28, paragraphe 1, et de l'article 28, paragraphe 2, du RGPD, lues conjointement avec l'article 5, paragraphe 2, et l'article 24 du RGPD, varient en fonction du risque associé à l'activité de traitement. En ce qui concerne ces questions, le comité souligne les éléments suivants.

34. L'article 5, paragraphe 2, du RGPD consacre le principe de responsabilité, en rendant le responsable du traitement responsable du respect des principes de protection des données énoncés à l'article 5, paragraphe 1, du RGPD et de la capacité à démontrer ce respect. L'article 5, paragraphe 2, du RGPD s'applique à tous les principes généraux énumérés à l'article 5, paragraphe 1, du RGPD.

35. L'article 24, paragraphe 1, du RGPD inclut l'obligation du responsable du traitement de démontrer que le traitement est effectué conformément au RGPD, mais développe davantage l'une des obligations auxquelles s'applique le principe de responsabilité, à savoir présenter des «garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées»[29]. L'article 24, paragraphe 1, du RGPD fait référence à la notion de «risque»[30] comme étant pertinente pour son application, comme l'un des critères que le responsable du traitement doit prendre en compte pour évaluer le caractère approprié de ces mesures[31]. L'article 24, paragraphe 1, du RGPD ajoute également que ces mesures doivent être réexaminées et actualisées si nécessaire.

---

[29] Arrêt du 25 janvier 2024, *BL contre MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, paragraphe 36: «*L'article 24 du RGPD prévoit une obligation générale, pesant sur le responsable du traitement de données à caractère personnel, de mettre en œuvre des mesures techniques et organisationnelles appropriées afin d'assurer que ledit traitement est effectué en conformité avec ce règlement et de pouvoir le démontrer*».

[30] Le considérant 75 du RGPD énumère quelques exemples de risques: «*le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important*»; le considérant 76 du RGPD indique: «*Il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé».* Comme l'a résumé la CJUE «*selon le considérant 76 de ce règlement, la probabilité et la gravité du risque dépendent des spécificités du traitement en cause et ce risque devrait faire l'objet d'une évaluation objective.*» (CJUE, arrêt du 14 décembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, point 36).

[31] Comme l'a indiqué la CJUE, «*À cette fin, cet article 24 énumère, à son paragraphe 1, un certain nombre de critères à prendre en compte pour évaluer le caractère approprié de telles mesures, à savoir la nature, la portée, le contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques*», arrêt du 14 décembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, point 25. Dans ce même arrêt, la CJUE a précisé que «*Le caractère approprié de telles mesures doit être évalué de manière concrète, en examinant si ces mesures ont été mises en œuvre par ce responsable en tenant compte des différents critères visés (...) et des besoins de protection des données spécifiquement inhérents au traitement concerné ainsi qu'aux risques induits par ce dernier*», point 30; également rappelé dans l'arrêt du 25 janvier 2024, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, point 38: «*Il ressort ainsi des libellés des articles 24 et 32 du RGPD que le caractère approprié*

36. Comme l'a indiqué la CJUE, «*l'article 5, paragraphe 2, et l'article 24 du RGPD imposent des obligations générales de responsabilité et de conformité aux responsables du traitement de données à caractère personnel. En particulier, ces dispositions exigent des responsables du traitement qu'ils adoptent les mesures appropriées visant à prévenir les violations éventuelles des règles prévues par le RGPD pour assurer le droit à la protection des données»*[32].

37. Le principe de responsabilité s'adresse au responsable du traitement, y compris lorsque le responsable du traitement a confié à des sous-traitants ou à des sous-traitants ultérieurs le traitement de données à caractère personnel pour son compte.

38. Conformément à l'article 28, paragraphe 1, du RGPD, lorsqu'un responsable du traitement engage un sous-traitant pour effectuer un traitement de données à caractère personnel pour son compte, le responsable du traitement ne doit faire appel qu'à un sous-traitant qui peut fournir «*des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences*» du RGPD «*et garantisse la protection des droits de la personne concernée*»[33]. Comme indiqué dans les lignes directrices 07/2020 de l'EDPB, le principe de responsabilité est également reflété à l'article 28 du RGPD[34].

39. À cet égard, l'EDPB souligne qu'aux fins de l'évaluation de la conformité avec l'article 24, paragraphe 1, et l'article 28, paragraphe 1, du RGPD, les autorités de contrôle devraient considérer que **le recrutement de sous-traitants ne devrait pas abaisser le niveau de protection des droits des personnes concernées** par rapport à une situation où le traitement est effectué directement par le responsable du traitement. Il s'agit du recrutement du sous-traitant initial, mais aussi de du recrutement de sous-traitants supplémentaires tout au long de la chaîne de traitement, par exemple les sous-traitants ultérieurs et leurs sous-traitants respectifs. L'article 24, paragraphe 1, et l'article 28, paragraphe 1, du RGPD doivent être interprétés comme imposant au responsable du traitement de veiller à ce que la chaîne de traitement ne soit constituée que de sous-traitants, de sous-traitants ultérieurs et de leurs sous-traitants respectifs (etc.) qui présentent «des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées». En outre, le responsable du traitement doit être en mesure de prouver qu'il a pris sérieusement en considération tous les éléments prévus dans le RGPD[35]. Ces considérations sont valables même si la chaîne de traitement peut être longue et complexe avec différents sous-traitants, sous-traitants ultérieurs, etc. impliqués à différents stades des activités de traitement. Le responsable du traitement devrait faire preuve de toute la diligence requise dans la sélection et la surveillance de ses sous-traitants.

40. En ce qui concerne le choix du **sous-traitant initial**, le responsable du traitement devrait vérifier le caractère suffisant des garanties fournies au cas par cas en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques, sur la base du type de traitement confié au sous-traitant[36]. Conformément à l'article 28,

---

des mesures mises en œuvre par le responsable du traitement doit être évalué de manière concrète, compte tenu des différents critères visés à ces articles et des besoins de protection des données spécifiquement inhérents au traitement concerné ainsi qu'aux risques induits par ce dernier, et cela d'autant plus que ledit responsable doit être en mesure de démontrer la conformité avec ce règlement desdites mesures, possibilité dont il serait privé si une présomption irréfragable était admise». Il convient de noter que l'analyse de la CJUE se rapporte également à l'article 32 du RGPD.

[32] Arrêt du 27 octobre 2022, *Proximus NV contre Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, paragraphe 81. Voir également les lignes directrices 07/2020 de l'EDPB, paragraphe 9.

[33] Lignes directrices 07/2020 de l'EDPB, paragraphe 94.

[34] Lignes directrices 07/2020 de l'EDPB, paragraphe 8.

[35] Lignes directrices 07/2020 de l'EDPB, paragraphe 94.

[36] Lignes directrices 07/2020 de l'EDPB, paragraphe 96.

paragraphe 5, du RGPD, l'adhésion d'un sous-traitant à un code de conduite approuvé en vertu de l'article 40 du RGPD ou à un mécanisme de certification approuvé en vertu de l'article 42 du RGPD peut être utilisée comme un élément permettant de démontrer l'existence de garanties suffisantes.

41. Comme l'a indiqué précédemment le comité européen de la protection des données, le responsable du traitement devrait tenir compte de plusieurs éléments lors de la vérification des garanties fournies par les sous-traitants[37], et un échange de documents pertinents sera souvent nécessaire[38]. En tout état de cause, «*les garanties 'fournies' par le sous-traitant sont celles qu'il est en mesure de démontrer à la satisfaction du responsable du traitement, puisque ce sont les seules à pouvoir être effectivement prises en compte par le responsable du traitement lors de l'évaluation du respect de ses obligations*»[39]. Ni l'article 28, paragraphe 1, du RGPD lui-même ni les documents déjà publiés de l'EDPB ne fournissent une liste exhaustive des documents ou des actions que le sous-traitant doit montrer ou démontrer, car cela dépend largement des circonstances spécifiques du traitement[40]. Par exemple, le responsable du traitement peut établir un questionnaire afin de recueillir des informations auprès de son sous-traitant afin de vérifier les garanties pertinentes, demander la présentation de documents pertinents, s'appuyer sur des informations publiques et/ou des certifications ou des rapports d'audit de tiers dignes de confiance et/ou effectuer des audits sur place.

42. Le comité européen de la protection des données a déjà précisé que l'obligation de n'utiliser que des sous-traitants «fournissant des garanties suffisantes» figurant à l'article 28, paragraphe 1, du RGPD est une obligation permanente et que le responsable du traitement devrait, à intervalles appropriés, vérifier les garanties du sous-traitant[41].

43. À la lumière de la question 1.3 soulevée par l'AC danoise dans sa demande concernant le risque associé au traitement, l'EDPB souligne que la notion de risque joue un rôle important dans un certain nombre de dispositions du RGPD, en particulier celles relatives au chapitre IV du RGPD[42].

44. Il importe de souligner que la référence au «risque» figurant à l'article 24, paragraphe 1, et au considérant 74 du RGPD ne devrait pas être interprétée en ce sens que le responsable du traitement peut négliger ou s'écarter des obligations qui lui incombent en vertu du RGPD en raison du simple fait qu'il considère que le risque pour les droits et libertés des personnes concernées est «faible». L'obligation de présenter des «garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées» pour assurer le respect du RGPD conformément à l'article 24,

[37] Lignes directrices 07/2020 de l'EDPB, paragraphes 97 à 98 (se référant aux connaissances spécialisées, à la fiabilité et aux ressources du sous-traitant, ainsi qu'à la réputation du sous-traitant sur le marché et à l'adhésion à un code de conduite ou à un mécanisme de certification approuvé).

[38] Lignes directrices 07/2020 de l'EDPB, paragraphe 95 (certains exemples sont cité: la politique en matière de respect de la vie privée, les conditions de service, l'enregistrement des activités de traitement, la politique en matière de gestion des documents, la politique de sécurité de l'information, les rapports des audits externes en matière de protection des données, les certifications internationales reconnues, comme la série ISO 27000).

[39] Lignes directrices 07/2020 de l'EDPB, paragraphe 95.

[40] Lignes directrices 07/2020 de l'EDPB, paragraphe 96 («*L'appréciation par le responsable du traitement du caractère suffisant des garanties est une forme d'évaluation des risques, qui dépendra grandement du type de traitement qui est confié au sous-traitant, et doit être effectuée au cas par cas, en tenant compte de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes physiques. En conséquence, le comité européen de la protection des données ne peut fournir une liste exhaustive des documents que le sous-traitant doit présenter ou des actions qu'il doit démontrer dans une situation donnée, car cela dépend dans une large mesure des circonstances particulières du traitement*»).

[41] Lignes directrices 07/2020 de l'EDPB, paragraphe 99: «*y compris au moyen d'audits et d'inspections, le cas échéant*».

[42] Le terme «risque» est mentionné aux articles 24, 25, 27, 30, 32, 33, 34, 35, 36 et 39 du RGPD.

paragraphe 1, du RGPD s'applique systématiquement, mais les mesures nécessaires pour atteindre ce résultat peuvent varier en fonction du risque[43].

45. Bien que l'article 28, paragraphe 1, du RGPD ne fasse pas spécifiquement référence au «risque», il implique la nécessité d'examiner le niveau de risque pour les droits et libertés des personnes concernées. L'obligation prévue à l'article 28, paragraphe 1, de n'avoir recours qu'à des sous-traitants offrant des «garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées» devrait être interprétée comme impliquant la nécessité d'envisager la fourniture par les sous-traitants de garanties suffisantes pour mettre en œuvre ces mesures à la lumière des risques liés au traitement, étant donné que, par exemple, le niveau des mesures de sécurité à mettre en œuvre dépend également des risques.

46. Le risque associé à l'activité de traitement joue un rôle important dans la détermination de l'adéquation des mesures techniques et organisationnelles, au même titre que les autres critères cités à l'article 24, paragraphe 1, du RGPD[44]. En fonction du niveau de risque associé à l'activité de traitement (par exemple, si des catégories particulières de données à caractère personnel sont traitées), le responsable du traitement peut définir des mesures techniques et organisationnelles plus strictes ou plus étendues. Tout sous-traitant devrait donc fournir des garanties suffisantes pour mettre effectivement en œuvre les mesures «appropriées» définies par le responsable du traitement.

47. Le comité estime que ***l'obligation*** **du responsable du traitement de vérifier si les sous-traitants (ultérieurs) présentent des garanties suffisantes pour mettre en œuvre les mesures définies par le responsable du traitement devrait s'appliquer quel que soit le risque pour les droits et libertés des personnes concernées.**

48. **Toutefois, *l'étendue* de cette vérification variera, dans la pratique, en fonction de la nature de ces mesures organisationnelles et techniques déterminées par le responsable du traitement sur la base, entre autres critères, du risque associé au traitement.** Par exemple, lorsque les activités de traitement présentent un risque moindre pour les droits et libertés des personnes concernées, les «mesures appropriées» correspondantes seront moins strictes. Par conséquent, l'étendue de la vérification du responsable du traitement peut être moins importante dans la pratique. À l'inverse, en cas de risques plus élevés découlant du traitement en question, le niveau de vérification du responsable du traitement peut être plus important en ce qui concerne la vérification des garanties suffisantes présentées par l'ensemble de la chaîne de traitement, étant donné que les «mesures appropriées» à mettre en œuvre sont plus importantes et plus robustes pour faire face aux risques pesant sur les personnes concernées.

49. À cet égard, en fonction du niveau de risque associé à l'activité de traitement, le responsable du traitement peut augmenter le niveau de sa vérification en vérifiant lui-même les contrats de sous-traitance et/ou en imposant également au sous-traitant initial une obligation de vérification et une documentation étendues.

---

[43] CJUE, arrêt du 14 décembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, point 35: «*le considérant 74 du RGPD met en exergue qu'il importe que le responsable du traitement soit tenu de mettre en œuvre des mesures appropriées et effectives et soit à même de démontrer la conformité des activités de traitement avec ce règlement, y compris l'efficacité des mesures, lesquelles devraient tenir compte des critères, liés aux caractéristiques du traitement concerné et au risque présenté par celui-ci, qui sont aussi énoncés à ses articles 24 et 32*».

[44] L'article 24, paragraphe 1, fait référence à «*la nature, de la portée, du contexte et [l]es finalités du traitement ainsi que [l]es risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques*».

50. Conformément au principe de responsabilité, toute mesure jugée nécessaire pour se conformer au RGPD, y compris sur la base du risque encouru par le traitement, devrait être dûment documentée par le responsable du traitement[45]. Cette obligation est facilitée, d'une part, par les **obligations d'assistance et d'audit** imposées aux sous-traitants et, d'autre part, par les **informations fournies par le sous-traitant initial** au responsable du traitement avant l'engagement de sous-traitants supplémentaires.

51. Tout d'abord, le comité note que les sous-traitants ont l'obligation d'aider le responsable du traitement à se conformer à certaines exigences du RGPD [en vertu de son article 28, paragraphe 3, points e) et f)][46]. Plus généralement, le sous-traitant a l'obligation de mettre à la disposition du responsable du traitement toutes les informations nécessaires pour attester du respect de l'article 28 [article 28, paragraphe 3, point h), du RGPD][47]. Le responsable du traitement devrait être pleinement informé des détails du traitement qui sont pertinents pour démontrer le respect des obligations prévues à l'article 28 du RGPD, et le sous-traitant devrait fournir toutes les informations sur la manière dont l'activité de traitement est exécutée pour le compte du responsable du traitement[48]. Le contrat devrait préciser la fréquence et la manière dont ces échanges d'informations doivent avoir lieu[49].

52. Par conséquent, le responsable du traitement peut s'appuyer sur les informations fournies par le sous-traitant, conformément à l'article 28, paragraphe 3, point h), du RGPD, pour s'acquitter de son obligation de documentation des mesures adoptées, à condition que les informations soumises par le sous-traitant démontrent effectivement le respect de cette obligation. Étant donné que le sous-traitant est bien placé pour connaître les détails du traitement qu'il effectue et du traitement effectué par les sous-traitants ultérieurs, il devrait mettre proactivement à la disposition du responsable du traitement toutes les informations pertinentes[50].

---

[45] En ce qui concerne la charge de la preuve du responsable du traitement, voir CJUE, arrêt du 14 décembre 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, point 52: «*Il ressort sans ambiguïté des libellés de l'article 5, paragraphe 2, de l'article 24, paragraphe 1, et de l'article 32, paragraphe 1, du RGPD que la charge de prouver que les données à caractère personnel sont traitées de façon à garantir une sécurité appropriée de ces dernières, au sens de l'article 5, paragraphe 1, sous f), et de l'article 32 de ce règlement, incombe au responsable du traitement concerné*»; voir également l'arrêt de la CJUE du 25 janvier 2024, BL c. MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, point 42 «*À cet égard, il importe de souligner qu'il résulte d'une lecture combinée des articles 5, 24 et 32 du RGPD, lus à la lumière du considérant 74 de celui-ci, que, dans le cadre d'une action en réparation fondée sur l'article 82 de ce règlement, la charge de prouver que les données à caractère personnel sont traitées de façon à garantir une sécurité appropriée de ces dernières, au sens de l'article 5, paragraphe 1, sous f), et de l'article 32 dudit règlement, incombe au responsable du traitement concerné. Une telle répartition de la charge de la preuve est de nature non seulement à inciter les responsables du traitement de ces données à adopter des mesures de sécurité requises par le RGPD, mais aussi à sauvegarder l'effet utile du droit à réparation prévu à l'article 82 de ce règlement et à respecter les intentions du législateur de l'Union mentionnées au considérant 11 de celui-ci*».

[46] Voir les lignes directrices 07/2020 de l'EDPB, paragraphes 130 à 138.

[47] Voir les lignes directrices 07/2020 de l'EDPB, paragraphes 143 à 145.

[48] Lignes directrices 07/2020 de l'EDPB, paragraphe 143.

[49] Lignes directrices 07/2020 de l'EDPB, paragraphe 143.

[50] Lignes directrices 07/2020 de l'EDPB, paragraphe 143, faisant référence à l'article 28, paragraphe 3, point h): «*Par exemple, les parties pertinentes des registres des activités de traitement du sous-traitant peuvent être communiquées au responsable du traitement. Le sous-traitant devrait fournir toutes les informations sur la manière dont l'activité de traitement sera effectuée pour le compte du responsable du traitement. Ces informations devraient comprendre des données sur le fonctionnement des systèmes utilisés, les mesures de sécurité, la manière dont les exigences en matière de conservation des données sont respectées, la localisation des données, les transferts de données, les personnes qui ont accès aux données et les destinataires des données, les sous-traitants ultérieurs utilisés, etc.*». La possibilité pour le responsable du traitement d'effectuer un audit

53. Ce qui précède s'applique également aux sous-traitants ultérieurs. En effet, les sous-traitants sont tenus de répercuter les obligations d'assistance en aval de la chaîne de traitement (article 28, paragraphe 4, du RGPD).

54. Deuxièmement, le **recrutement de sous-traitants ultérieurs**, comme rappelé ci-dessus, n'est possible qu'avec l'autorisation écrite préalable du responsable du traitement, laquelle peut être spécifique ou générale. Si le responsable du traitement choisit de donner une autorisation générale, celle-ci «*devrait être complétée par des critères permettant d'orienter le choix du sous-traitant (par exemple, des garanties en matière de mesures techniques et organisationnelles, des connaissances spécialisées, la fiabilité et les ressources)*»[51].

55. Comme l'a expliqué le comité: «*Pour évaluer et décider d'autoriser ou non la sous-traitance, une liste des sous-traitants ultérieurs envisagés (comprenant pour chacun d'entre eux: la localisation, ce qu'ils feront et la preuve des garanties qui ont été mises en œuvre) devra être fournie au responsable du traitement par le sous-traitant*»[52]. Ces informations sont nécessaires pour que le responsable du traitement puisse se conformer au principe de responsabilité établi à l'article 5, paragraphe 2 et à l'article 24 et aux dispositions de l'article 28, paragraphe 1, de l'article 32 et du chapitre V du RGPD[53]. En ce qui concerne les transferts de données à caractère personnel en dehors de l'EEE, le comité renvoie à la réponse fournie ci-dessous à la question 1.2 posée par l'AC danoise.

56. Comme l'a rappelé le comité européen de la protection des données, le sous-traitant initial devrait veiller à proposer des sous-traitants ultérieurs fournissant des garanties suffisantes[54]. La nécessité pour le sous-traitant initial de fournir les informations susmentionnées montre que **le sous-traitant a un rôle à jouer dans le choix des sous-traitants ultérieurs et dans la vérification des garanties qu'ils fournissent, et qu'il est tenu de fournir des informations suffisantes au responsable du traitement**. Cela est également cohérent avec le fait que, indépendamment des critères suggérés par le responsable du traitement pour sélectionner les sous-traitants supplémentaires, le sous-traitant initial demeure pleinement responsable, devant le responsable du traitement, de l'exécution des obligations des sous-traitants ultérieurs (article 28, paragraphe 4, du RGPD).

57. À cet égard, même si, conformément à l'article 28, paragraphe 4, du RGPD, il incombe directement au sous-traitant qui fait appel à un sous-traitant ultérieur de veiller à ce que les mêmes obligations en matière de protection des données que celles énoncées dans le contrat initial entre le responsable du traitement et le sous-traitant soient imposées au sous-traitant ultérieur, cela ne supprime pas la responsabilité du responsable du traitement de veiller au respect des exigences de l'article 28, paragraphe 1, et de l'article 24, paragraphe 1, du RGPD et d'être en mesure de démontrer le respect de ces exigences.

58. **La décision finale de recruter ou non un sous-traitant ultérieur (et/ou son sous-traitant respectif) et la responsabilité qui en découle, y compris en ce qui concerne la vérification du caractère suffisant des garanties fournies par le sous-traitant (ultérieur), incombent au responsable du traitement.** Comme déjà énoncé, en cas d'autorisation générale ou spécifique, il appartient systématiquement au

est également précisée au paragraphe 144: «*L'objet de ces audits est de garantir que le responsable du traitement dispose de toutes les informations relatives à l'activité de traitement effectuée pour son compte et aux garanties fournies par le sous-traitant.*»

[51] Lignes directrices 07/2020 de l'EDPB, paragraphe 156.

[52] Lignes directrices 07/2020 de l'EDPB, paragraphe 152.

[53] Lignes directrices 07/2020 de l'EDPB, note de bas de page 69.

[54] Lignes directrices 07/2020 de l'EDPB, paragraphe 159.

responsable du traitement de décider s'il approuve le recrutement d'un sous-traitant ultérieur ou s'il s'y oppose.

59. Lorsqu'elles évaluent le respect de l'article 24, paragraphe 1, et de l'article 28, paragraphe 1, du RGPD, les autorités de contrôle devraient évaluer si le responsable du traitement est en mesure de démontrer que la vérification du caractère suffisant des garanties fournies par ses sous-traitants ultérieurs a eu lieu à la satisfaction du responsable du traitement. Cela signifie que le responsable du traitement peut choisir de s'appuyer sur les informations reçues de son sous-traitant et, si nécessaire, de les développer. Par exemple, lorsque les informations reçues par le responsable du traitement semblent incomplètes, inexactes ou soulèvent des questions, ou, le cas échéant, sur la base des circonstances de l'espèce, y compris le risque associé au traitement, le responsable du traitement devrait demander des informations complémentaires et/ou vérifier les informations et les compléter/corriger si nécessaire.

60. Plus précisément, pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées, le responsable du traitement devrait accroître son niveau de vérification en ce qui concerne le contrôle des informations fournies concernant les garanties présentées par les différents sous-traitants dans la chaîne de traitement.

2.1.3 Vérification du contrat entre le sous-traitant initial et les sous-traitants supplémentairesError! Bookmark not defined.

61. L'AC danoise demande en substance si et dans quelle mesure le responsable du traitement a l'obligation de vérifier et de documenter le fait que les contrats de sous-traitance imposent les mêmes obligations aux sous-traitants supplémentaires.

62. L'article 28, paragraphe 4, du RGPD[55] impose une obligation directe aux sous-traitants à cet égard. En outre, l'article 28, paragraphe 3, point d), du RGPD, exige que le contrat entre le responsable du traitement et le sous-traitant «prévoie» l'obligation pour le sous-traitant de respecter les conditions visées à l'article 28, paragraphe 4, faisant ainsi de cette exigence une obligation contractuelle imposée au sous-traitant. En d'autres termes, **le sous-traitant initial est légalement et contractuellement tenu de transférer les mêmes obligations en matière de protection des données dans les contrats de sous-traitance qu'il conclut avec les sous-traitants supplémentaires.**

[55] Article 28, paragraphe 4, du RGPD. «*Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement.*»

63. De même, les sous-traitants supplémentaires seront contractuellement tenus (par le sous-traitant initial) d'imposer les mêmes obligations en matière de protection des données à leurs propres sous-traitants, et ainsi de suite tout au long de la chaîne de traitement[56]. Il n'est pas nécessaire que le contrat de sous-traitance ultérieure soit identique dans son libellé au contrat de traitement des données conclu avec le sous-traitant initial[57].

64. Le comité rappelle que si un sous-traitant ultérieur ne remplit pas ses obligations, la responsabilité finale de l'exécution des obligations dudit sous-traitant ultérieur incombe au responsable du traitement. Toutefois, le sous-traitant initial reste responsable vis-à-vis du responsable du traitement, de sorte que ce dernier a la possibilité d'introduire une réclamation contractuelle à l'encontre de son sous-traitant initial si ce dernier ne transmet pas les mêmes obligations en matière de protection des données dans les contrats de sous-traitance ultérieure.

65. Les sous-traitants ont l'obligation de mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de l'article 28, paragraphe 3, point h), du RGPD. Par conséquent, à la demande du responsable du traitement, le sous-traitant initial devra fournir les contrats de sous-traitance entre le sous-traitant initial et les sous-traitants supplémentaires.

66. À cet égard, les clauses contractuelles types (CCT)[58] de la CE entre responsables du traitement et sous-traitants et les CCT de la CE pour le transfert de données vers des pays tiers[59] donnent au responsable

[56] Dans l'avis conjoint 2/2021 de l'EDPB et du CEPD concernant la décision d'exécution de la Commission européenne relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, l'EDPB et le CEPD ont souligné que l'exigence visée à l'article 28, paragraphe 4, du RGPD devait être prise en considération par les parties dans le cadre d'un transfert de sous-traitant à sous-traitant (paragraphe 66).

[57] Lignes directrices 07/2020 de l'EDPB, paragraphe 160: «*L'imposition des 'mêmes' obligations devrait être interprétée de manière fonctionnelle plutôt que formelle; en effet, il n'est pas nécessaire que le contrat comporte exactement les mêmes termes que ceux utilisés dans le contrat conclu entre le responsable du traitement et le sous-traitant, mais il devrait assurer que les obligations sont identiques en substance*». L'EDPB note également que lorsque deux sous-traitants s'appuient sur le module trois (transfert de sous-traitant à sous-traitant) des CCT de la CE pour le transfert de données vers des pays tiers, une garantie supplémentaire est fournie par le sous-traitant initial. En vertu de la clause 8.1, point d), des CCT de la CE pour le transfert de données vers des pays tiers, l'exportateur de données (le sous-traitant initial) garantit qu'il a imposé à l'importateur de données (le sous-traitant ultérieur) les mêmes obligations en matière de protection des données que celles énoncées dans le contrat ou tout autre acte juridique au titre du droit de l'Union ou du droit d'un État membre entre le responsable du traitement et l'exportateur de données.

[58] À la section 7 sur le recours à des sous-traitants ultérieurs, l'article 7, paragraphe 7, point c), des CCT de la CE entre responsables du traitement et sous-traitants dispose ce qui suit: «*À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie*». Décision d'exécution 2021/915 de la Commission du 4 juin 2021 sur les clauses contractuelles types entre responsables du traitement et sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 (ci-après «les CCT de la CE entre responsables du traitement et sous-traitants»).

[59] Le module 2 (transfert de responsable du traitement à sous-traitant), clause 9, paragraphe c), des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers dispose ce qui suit: «*L'importateur de données fournit à l'exportateur de données, à la demande de celui-ci, une copie du contrat avec le sous-traitant ultérieur et de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie*». En outre, le module trois (transfert de sous-traitant à sous-traitant) prévoit que «*L'importateur de données fournit sur demande, à l'exportateur de données ou au responsable du traitement, une copie du contrat avec le sous-traitant ultérieur et*

du traitement la possibilité de demander une copie du contrat de sous-traitance conclu entre le sous-traitant initial et les sous-traitants supplémentaires. Cette possibilité est également prévue par trois CCT entre responsables du traitement et sous-traitants adoptées par les autorités de contrôle[60]. Cette possibilité est l'expression du droit d'audit du responsable du traitement au titre de l'article 28, paragraphe 3, point h), du RGPD. À la demande du responsable du traitement, le sous-traitant est tenu fournir une telle copie du contrat de sous-traitance.

67. Néanmoins, l'EDPB note que les CCT ne précisent pas si un responsable du traitement *doit* demander une telle copie afin de se conformer à l'article 28, paragraphe 1, du RGPD.

68. Dans le même ordre d'idées, le fait que le responsable du traitement choisisse ou non de demander une telle copie ne saurait déterminer la responsabilité du responsable du traitement. Le sous-traitant assume également, en tout état de cause, des obligations juridiques et contractuelles en vertu desquelles il est tenu d'imposer les mêmes obligations en matière de protection des données que dans le contrat initial.

69. Cela étant, le **responsable du traitement n'a pas l'obligation de demander systématiquement les contrats de sous-traitance afin de vérifier si les obligations en matière de protection des données prévues dans le contrat initial ont été transmises en aval de la chaîne de traitement**. Le responsable du traitement devrait évaluer, au cas par cas, s'il est nécessaire de demander une copie des contrats précités ou de les réexaminer lorsque cela est nécessaire pour être en mesure de démontrer la conformité à la lumière du principe de responsabilité. Dans le cadre de l'exercice de son droit d'audit au titre de l'article 28, paragraphe 3, point h), du RGPD, le responsable du traitement devrait avoir mis en place une procédure pour mener des campagnes d'audit afin de vérifier, par des vérifications par échantillonnage, que les contrats avec ses sous-traitants ultérieurs contiennent les obligations nécessaires en matière de protection des données.

70. La nécessité de demander une copie du contrat de sous-traitance dépend donc des circonstances de l'espèce. Par exemple, en cas de doute quant au respect par le sous-traitant ou le sous-traitant ultérieur des exigences de l'article 28, paragraphes 1 et 4, ou à la demande de l'AC, le responsable du traitement devrait demander la présentation du contrat pour l'examiner (par exemple, si le sous-traitant supplémentaire est victime d'une violation de données, ou au regard d'autres informations publiques ou portées à la connaissance du responsable du traitement); par exemple, certains modèles de contrat de traitement de données utilisés par le sous-traitant ultérieur peuvent ne pas répondre aux exigences de l'article 28, paragraphe 3, du RGPD.

71. Afin de garantir le respect de l'article 28, paragraphe 1, à la lumière du principe de responsabilité, une copie des contrats de sous-traitance ultérieure peut aider le responsable du traitement à démontrer que ses sous-traitants et sous-traitants ultérieurs présentent des garanties suffisantes, notamment que le sous-traitant respecte l'article 28, paragraphe 4, du RGPD. L'EDPB observe qu'un responsable du traitement peut ne pas être en mesure d'évaluer si les garanties fournies à l'égard d'un sous-traitant

de ses éventuelles modifications ultérieures. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, notamment les données à caractère personnel, l'importateur de données peut occulter une partie du texte du contrat avant d'en communiquer une copie». Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil (ci-après les «CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers»).

[60] Clauses contractuelles types de l'AC danoise aux fins du respect de l'article 28 du RGPD, en particulier la clause 7.5; clauses contractuelles types de l'AC lituanienne aux fins du respect de l'article 28 du RGPD, en particulier la clause 18; clauses contractuelles types de l'AC slovène aux fins du respect de l'article 28 du RGPD, en particulier la clause 6.5.

ultérieur sont suffisantes, notamment s'il n'a pas pu accéder au contenu du contrat de sous-traitance et évaluer celui-ci. Même si des garanties sont prévues par écrit dans le contrat, ces clauses contractuelles ne suffisent pas - à elles seules - à démontrer que les garanties suffisantes sont effectivement mises en œuvre par les parties au contrat.

2.2 Sur l'interprétation de l'article 28, paragraphe 1, du RGPD, lu conjointement avec l'article 44 du RGPD (transferts dans la chaîne de traitement – questions 1.2 et 1.3)

72. La question 1.2 de la demande vise à clarifier, dans les cas de transferts ou de transferts ultérieurs d'un sous-traitant (ultérieur) à un autre sous-traitant (ultérieur), dans quelle mesure le responsable du traitement doit, dans le cadre de son obligation au titre de l'article 28, paragraphe 1, du RGPD, lu conjointement avec l'article 44 du RGPD, évaluer la documentation des sous-traitants (ultérieurs) attestant que le niveau de protection des données à caractère personnel n'est pas affaibli par les transferts initiaux ou ultérieurs.

73. La question 1.3 vise à clarifier si l'étendue des obligations au titre de l'article 28, paragraphe 1, du RGPD, lu conjointement avec l'article 5, paragraphe 2, et l'article 24 du RGPD, telle que traitée à la question 1.2, varie en fonction du risque associé à l'activité de traitement. Dans l'affirmative, l'AC danoise a demandé à savoir quelle est l'étendue de ces obligations pour les activités de traitement «à faible risque» et «à haut risque».

Clarifications préalables

74. Par souci de clarté, certaines clarifications préalables relatives à ces questions sont fournies dans le cadre du présent avis.

75. Premièrement, l'EDPB comprend le terme «transfert» au sens défini dans les lignes directrices 05/2021 de l'EDPB relatives à l'interaction entre l'article 3 et le chapitre V du RGPD[61] [ci-après les «lignes directrices 05/2021 de l'EDPB (interaction)»], qui font également référence aux lignes directrices 3/2018 de l'EDPB relatives au champ d'application territorial du RGPD[62]. Comme l'a souligné précédemment le comité européen de la protection des données, l'accès à distance depuis un pays tiers constitue un transfert s'il remplit les critères énoncés dans les lignes directrices 05/2021 du comité européen de la protection des données (interaction)[63]. En tout état de cause, l'existence d'un transfert déclenche l'application du chapitre V du RGPD.

76. Deuxièmement, étant donné que la question 1.2 fait référence à une situation dans laquelle un sous-traitant (ultérieur) effectue un transfert initial ou ultérieur à un autre sous-traitant (ultérieur), le responsable du traitement n'est pas l'exportateur de données; l'exportateur de données est plutôt un sous-traitant, qui transfère les données à caractère personnel à un autre sous-traitant en aval de la chaîne pour le compte du responsable du traitement, et non à un responsable du traitement distinct. Elle exclut donc les données à caractère personnel transférées à des responsables du traitement distincts, y compris des tribunaux, des juridictions ou des autorités administratives de pays tiers. Par conséquent, l'interprétation de l'article 48 du RGPD n'entre pas dans le cadre de ces questions.

77. Troisièmement, l'EDPB note que la question 1.2 fait référence à des transferts qui ont lieu tout au long de la chaîne de traitement conformément aux instructions documentées du responsable du traitement au titre de l'article 28, paragraphe 3, point a), du RGPD. Il convient de souligner qu'il appartient au responsable du traitement de décider si un transfert de données à caractère personnel en dehors de l'EEE est possible dans le cadre des activités de traitement confiées aux sous-traitants (ultérieurs). Le sous-traitant devrait s'abstenir d'effectuer tout transfert initial ou ultérieur en dehors des instructions du responsable du traitement[64]. Les instructions documentées du responsable du traitement concernant les transferts initiaux ou ultérieurs de données à caractère personnel doivent être transmises en aval de l'ensemble de la chaîne de traitement[65].

78. Quatrièmement, l'EDPB précise que la notion de risque visée à la question 1.3 doit être comprise comme le risque pour les droits et libertés des personnes concernées dont les données à caractère personnel sont traitées, au sens des considérants 75 et 76 du RGPD (comme indiqué au paragraphe 35 ci-dessus).

---

[61] Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD, version 2.0, adoptées le 14 février 2023; le paragraphe 9 des lignes directrices 05/2021 définit les trois critères cumulatifs permettant de qualifier une opération de traitement comme un transfert et, plus généralement, la section 2 détaille ces critères.

[62] Lignes directrices 05/2021 de l'EDPB (interaction), paragraphe 12 renvoyant aux lignes directrices 3/2018 de l'EDPB relatives au champ d'application territorial du RGPD, version 2.1, adoptées le 12 novembre 2019 (avec rectificatif daté du 7 janvier 2020), page 5 et sections 1–3. Voir en particulier le point «d) Sous-traitant non établi dans l'Union» à la section 2.

[63] Lignes directrices 05/2021 de l'EDPB (interaction), paragraphe 16.

[64] Article 24, du RGPD. Comme l'a rappelé l'EDPB, «*[l]e contrat devrait préciser les exigences applicables aux transferts vers des pays tiers ou à des organisations internationales, en tenant compte des dispositions du chapitre V du RGPD*» (lignes directrices 07/2020 de l'EDPB, paragraphe 119). Par exemple, le responsable du traitement peut choisir d'interdire les transferts ou de ne les autoriser que vers certains pays.

[65] Article 60, paragraphe 4, du RGPD.

La responsabilité du responsable du traitement est engagée même si le transfert initial ou ultérieur est réalisé par le sous-traitant (ultérieur)

79. En ce qui concerne la teneur de la demande, l'EDPB a déjà précisé que «*(...) une situation de transfert se présente lorsqu'un sous-traitant (que ce soit en vertu de l'article 3, paragraphe 1, ou — pour un traitement donné — en vertu de l'article 3, paragraphe 2, (...)) envoie des données à un autre sous-traitant ou même à un responsable du traitement dans un pays tiers, conformément aux instructions de son responsable du traitement Dans ces cas, le sous-traitant agit en tant qu'exportateur de données pour le compte du responsable du traitement et doit garantir que les dispositions du chapitre V sont respectées pour le transfert en cause conformément aux instructions du responsable du traitement, et notamment qu'un instrument de transfert approprié est utilisé. Étant donné que le transfert est une activité de traitement effectuée pour le compte du responsable du traitement,* ***celui-ci est également responsable et pourrait être tenu responsable au titre du chapitre V; le responsable du traitement doit aussi veiller à ce que le sous-traitant prévoie des garanties suffisantes conformément à l'article 28.****»*[66]

80. En d'autres termes, en cas de transfert, même s'il n'est pas effectué directement par le responsable du traitement, mais plutôt par un sous-traitant pour le compte du responsable du traitement, le responsable du traitement reste soumis aux obligations découlant à la fois de l'article 44 du RGPD et de l'article 28, paragraphe 1, du RGPD[67] [68].

La responsabilité découlant de l'article 44 du RGPD

81. Les obligations prévues à l'article 44 du RGPD[69] s'adressent à la fois aux sous-traitants (dans le contexte de l'avis, agissant en tant qu'exportateurs de données) et aux responsables du traitement[70]. Les sous-traitants et les responsables du traitement devraient donc tous deux veiller à ce que le niveau de protection des données à caractère personnel ne soit pas compromis par le transfert initial ou ultérieur, quel que soit le motif pour lequel le transfert a lieu[71]. Par exemple, le responsable du traitement et le sous-traitant restent, en principe, responsables, en vertu du chapitre V du RGPD, de tout transfert initial ou ultérieur illicite[72] et pourraient donc être tous deux individuellement tenus responsables en cas d'infraction.

[66] Lignes directrices 05/2021 de l'EDPB (interaction), paragraphe 19, caractères gras ajoutés.

[67] Il convient également d'indiquer que l'article 28, paragraphe 1, du RGPD fait référence au respect des exigences du RGPD et doit donc être interprété comme incluant les dispositions du chapitre V relatives aux transferts initiaux ou ultérieurs de données à caractère personnel vers des pays tiers. Cela couvre à la fois les transferts initiaux et les transferts ultérieurs, cf. article 44 du RGPD.

[68] Aux fins de la présente section de l'avis, les obligations découlant de l'article 44 et de l'article 28, paragraphe 1, du RGPD sont abordées, étant précisé que le responsable du traitement reste toujours soumis à l'ensemble des obligations applicables aux responsables du traitement en vertu du RGPD.

[69] L'article 44 du RGPD fait référence aux dispositions du chapitre V du RGPD.

[70] L'article 44 du RGPD s'adresse à la fois au «responsable du traitement et au sous-traitant» en ce qui concerne la conformité avec le chapitre V; voir également le considérant 101. C'est la raison pour laquelle les recommandations 01/2020 de l'EDPB sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, version 2.0, adoptées le 18 juin 2021 (ci-après les «recommandations 01/2020 de l'EDPB») s'appliquent aux «exportateurs de données» [qu'il s'agisse de responsables du traitement ou de sous-traitants (ultérieurs) traitant des données à caractère personnel].

[71] Arrêt de la CJUE du 16 juillet 2020, *Data Protection Commissionner/Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559, point 92 (ci-après «arrêt de la CJUE dans l'affaire Schrems II»)

[72] Le responsable du traitement peut réclamer à son sous-traitant une indemnisation correspondant à sa part de responsabilité, pour autant que les conditions énoncées à l'article 82, paragraphe 5, du RGPD soient remplies.

La responsabilité découlant de l'article 28, paragraphe 1, du RGPD

82. En vertu du principe de responsabilité, les responsables du traitement sont tenus de prendre des «mesures appropriées» pour prévenir toute violation des règles énoncées dans le RGPD afin de garantir le droit à la protection des données[73], ce qui inclut la prévention des violations au titre du chapitre V du RGPD. Cette responsabilité s'applique avant le début du transfert, et aussi longtemps que les données à caractère personnel transférées sont traitées dans le pays tiers.

83. Comme expliqué aux paragraphes 47 et 48 ci-dessus, l'*obligation du responsable du traitement* de vérifier si les sous-traitants (ultérieurs) présentent des garanties suffisantes pour mettre en œuvre les mesures déterminées par le responsable du traitement au titre de l'article 28, paragraphe 1, du RGPD[74] devrait s'appliquer indépendamment du risque pour les droits et libertés des personnes concernées. Toutefois, l'*étendue* de cette vérification variera, dans la pratique, en fonction de la nature des mesures organisationnelles et techniques déterminées par le responsable du traitement sur la base, entre autres critères, du risque associé au traitement[75]. À cet égard, l'existence d'un transfert initial ou ultérieur vers des pays tiers tout au long de la chaîne de traitement peut accroître les risques liés au traitement et, partant, avoir une incidence sur les mesures «appropriées» déterminées par le responsable du traitement[76].

84. Sur demande, le responsable du traitement — assisté par le sous-traitant et les sous-traitants ultérieurs — devrait être en mesure de démontrer à l'autorité de contrôle compétente qu'il respecte les exigences de l'article 28, paragraphe 1, du RGPD. La documentation appropriée pourrait être basée - entre autres - sur les informations reçues des sous-traitants dans le cadre du recrutement des sous-traitants (ultérieurs)[77] (voir paragraphes 54-56), mais aussi avec l'assistance de ses sous-traitants, conformément à l'article 28, paragraphe 3, point h), du RGPD (voir paragraphes 51-52).

---

[73] Voir la section ci-dessus sur l'article 5, paragraphe 2, et l'article 24, paragraphe 1, lus conjointement avec l'article 28, paragraphe 1, du RGPD.

[74] Pour éviter toute ambiguïté, il convient de préciser que les «garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées» visées à l'article 24, paragraphe 1 et 28, paragraphe 1, du RGPD ne doivent pas être confondues avec les «mesures supplémentaires», mentionnées dans les recommandations 01/2020 de l'EDPB (paragraphe 50: «*Par définition, les «mesures supplémentaires» complètent les garanties déjà prévues par l'instrument de transfert visé à l'article 46 du RGPD et toutes les autres exigences de sécurité applicables (par exemple, les mesures techniques de sécurité) énoncées dans le RGPD*», se référant au considérant 109 du RGPD et à l'arrêt de la CJUE dans l'affaire Schrems II, point 133).

[75] Voir la définition du risque, telle qu'elle est expliquée aux paragraphes 35 et 78.

[76] Le considérant 116 du RGPD dispose ce qui suit: «*Lorsque des données à caractère personnel franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations.*»

[77] Voir également la clause 9, point a) du module 3 (transfert de sous-traitant à sous-traitant) des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers et son annexe III; voir également la clause 9, point a) du module deux (transfert de responsable du traitement à sous-traitant); et la clause 7.7, point a) des CCT de la CE entre responsables du traitement et sous-traitants et son annexe IV «Liste des sous-traitants ultérieurs». Tant l'annexe II des CCT de la CE pour le transfert de données vers des pays tiers que l'annexe IV des CCT de la CE entre responsables du traitement et sous-traitants doivent être complétées par les informations suivantes concernant les sous-traitants ultérieurs en cas d'autorisation spécifique du responsable du traitement: nom; adresse; nom, fonction et coordonnées de la personne de contact; description du traitement. En outre, à l'annexe I des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers, la section B «Description du transfert» inclut la mention «Pour les transferts à des sous-traitants (ultérieurs), veuillez également préciser l'objet, la nature et la durée du traitement». De même, l'annexe II des CCT entre responsables du traitement et sous-traitants inclut la mention: «Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement».

85. Le responsable du traitement a également besoin de toutes les informations pertinentes pour donner les instructions nécessaires au transfert des données à caractère personnel vers les pays tiers concernés et pour pouvoir se conformer au principe de responsabilité énoncé à l'article 5, paragraphe 2, et à l'article 24 du RGPD, ainsi qu'aux dispositions de l'article 28, paragraphe 1, de l'article 32 et du chapitre V du RGPD[78]. Le responsable du traitement peut s'opposer au recrutement d'un sous-traitant supplémentaire ou ne pas l'autoriser lorsque cela entraînerait un transfert de données à caractère personnel du sous-traitant initial (en tant qu'exportateur) vers le sous-traitant supplémentaire envisagé (en tant qu'importateur) sur la base des informations reçues.

86. Conformément au paragraphe 58 ci-dessus, le responsable du traitement est garant en dernier ressort de toute violation de l'article 28, paragraphe 1, du RGPD lorsqu'il a recours à des sous-traitants (ultérieurs), et pourrait en être tenu pour responsable. L'EDPB souligne que les difficultés pratiques invoquées par les responsables du traitement, concernant le contrôle, par leur sous-traitant, du recrutement de sous-traitants ultérieurs - qui peuvent rendre difficile la vérification des «garanties suffisantes», notamment en ce qui concerne les transferts vers des pays tiers - n'exonèrent pas le responsable du traitement de ses responsabilités dans le cadre du traitement[79].

87. Des exemples non exhaustifs de la documentation que le responsable du traitement devrait évaluer et être en mesure de présenter à l'autorité de contrôle compétente – la cartographie des transferts, le motif de transfert utilisé et, le cas échéant, «l'évaluation de l'impact du transfert» et les mesures supplémentaires – sont décrits ci-dessous.

La cartographie des transferts:

88. Dans un premier temps, lorsque des données à caractère personnel seront transférées vers des pays tiers dans le cadre de l'utilisation de sous-traitants (ultérieurs), le responsable du traitement devrait évaluer et être en mesure de présenter la documentation relative à la cartographie des transferts[80]. Le responsable du traitement devrait veiller à ce qu'une cartographie des transferts soit effectuée par l'exportateur (qui traite des données à caractère personnel pour son compte), indiquant quelles données à caractère personnel sont transférées (y compris l'accès à distance), où et à quelles fins[81]. Le responsable du traitement peut s'appuyer sur cette cartographie et, si nécessaire, la développer. Par exemple, lorsque la cartographie reçue par le responsable du traitement semble incomplète[82], inexacte ou soulève des questions, le responsable du traitement devrait demander des informations supplémentaires, vérifier les informations et les compléter/corriger si nécessaire.

89. Le responsable du traitement devrait recevoir ces informations[83] avant qu'un sous-traitant supplémentaire ne soit recruté. Il convient également de rappeler que le responsable du traitement est soumis à des exigences de transparence spécifiques en ce qui concerne les transferts vers des pays tiers en vertu de l'article 13, paragraphe 1, point f), de l'article 14, paragraphe 1, point f), de l'article 15, paragraphe 1, point c), et de l'article 15, paragraphe 2, du RGPD, ainsi qu'à l'obligation de

[78] Lignes directrices 07/2020 de l'EDPB, paragraphe 152, note de bas de page 69.

[79] Rapport CEF sur les services en nuage, p. 16.

[80] La «cartographie» fait référence à la première étape (appelée «Connaître les transferts») des recommandations 01/2020 de l'EDPB, section 2.1 «Étape 1: connaître les transferts». Cette première étape s'applique quel que soit le motif du transfert.

[81] Il convient de préciser que les finalités sont déterminées par le responsable du traitement, de même que les «moyens essentiels» du traitement (voir les lignes directrices 07/2020 de l'EDPB, paragraphe 40).

[82] Par exemple, si la cartographie ne précise pas le lieu où se trouvent les sous-traitants ultérieurs, ou si les transferts sous la forme d'un accès à distance ne sont pas mentionnés dans la cartographie pendant qu'ils ont lieu.

[83] Comme expliqué aux paragraphes 54 à 56 ci-dessus.

tenir des registres des activités de traitement en vertu de l'article 30, paragraphe 1, points d) et e), du RGPD. Afin de satisfaire à ces exigences, le responsable du traitement devrait savoir où se trouvent les sous-traitants ultérieurs et où ont lieu les transferts – y compris l'accès à distance[84].

Le motif de transfert utilisé et, le cas échéant, «l'évaluation de l'impact du transfert» et les mesures supplémentaires:

90. Le responsable du traitement devrait évaluer et être en mesure de présenter les documents relatifs au motif du transfert[85] sur lequel l'exportateur se fonde, conformément aux instructions du responsable du traitement[86]. Cela signifie que le responsable du traitement devrait recevoir ces informations de la part des sous-traitants (ultérieurs)/exportateurs avant que les transferts n'aient lieu. L'EDPB a rappelé dans ce contexte que le responsable du traitement est soumis à des exigences de transparence spécifiques en ce qui concerne «l'existence ou l'absence d'une décision d'adéquation» en vertu de l'article 45 du RGPD ou les «garanties appropriées» fournies conformément à l'article 46 du RGPD (article 13, paragraphe 1, point f), article 14, paragraphe 1, point f), et article 15, paragraphe 2, du RGPD[87]).

91. En ce qui concerne l'étendue de l'obligation du responsable du traitement d'évaluer cette documentation, elle dépend du type de motif utilisé pour le transfert initial ou ultérieur par les sous-traitants (ultérieurs) (en tant qu'exportateurs de données)[88]:

92. Les transferts peuvent être effectués sur la base d'une **décision d'adéquation** si, conformément à l'article 45 du RGPD, la Commission a décidé qu'un pays tiers, un territoire ou un ou plusieurs secteurs spécifiques dans ce pays tiers, ou qu'une organisation internationale garantisse un niveau de protection adéquat. Afin d'évaluer si le niveau de protection est adéquat, la Commission tient compte, entre autres critères, des règles régissant le transfert ultérieur de données à caractère personnel vers un autre pays tiers ou une organisation internationale qui sont respectées dans ce pays ou cette organisation internationale, de la jurisprudence, ainsi que des droits effectifs et opposables des personnes concernées et des voies de recours administratives et judiciaires efficaces pour les personnes concernées dont les données à caractère personnel sont transférées[89].

93. Dans ce contexte, lorsqu'un transfert est effectué par un sous-traitant (ultérieur) (pour le compte du responsable du traitement) sur la base d'une décision d'adéquation en vertu de l'article 45 du RGPD,

---

[84] Une telle cartographie est également nécessaire lorsque les parties complètent les annexes pertinentes des CCT de la CE pour le transfert de données vers des pays tiers et des CCT de la CE entre responsables du traitement et sous-traitants (voir note de bas de page 80 ci-dessus).

[85] Recommandations 01/2020 de l'EDPB, section 2.2. «Étape 2: recenser les instruments de transfert utilisés».

[86] Article 28, paragraphe 3, point a), du RGPD.

[87] Lignes directrices 01/2022 de l'EDPB (droit d'accès), paragraphe 122.

[88] Conformément aux instructions documentées du responsable du traitement en ce qui concerne les transferts de données à caractère personnel tout au long de la chaîne de traitement.

[89] Voir l'article 45 du RGPD et Critères de référence pour l'adéquation du GT «Article 29» adoptés le 28 novembre 2017, WP 254, approuvé par l'EDPB le 25 mai 2018, page 7: «*Les transferts ultérieurs des données à caractère personnel par le destinataire initial du transfert original de données ne devraient être autorisés que si le nouveau destinataire (c'est-à-dire le destinataire du transfert ultérieur) est également soumis à des règles (y compris des règles contractuelles) assurant un niveau de protection adéquat et suivant les instructions pertinentes lors du traitement des données pour le compte du responsable du traitement. Le niveau de protection des personnes physiques dont les données sont transférées ne doit pas être compromis par le transfert ultérieur. Le destinataire initial des données transférées depuis l'UE doit s'assurer que les garanties appropriées sont prévues pour les transferts ultérieurs de données en l'absence d'une décision d'adéquation. Ces transferts ultérieurs de données ne devraient avoir lieu qu'à des fins limitées et précises et tant que ce traitement a un fondement juridique*».

le degré de vérification exigé du responsable du traitement en vertu de l'article 28, paragraphe 1, du RGPD, selon lequel son sous-traitant (ultérieur) présente des garanties suffisantes en ce qui concerne le respect du chapitre V du RGPD, devrait couvrir les éléments suivants:

- la question de savoir si la décision d'adéquation est en vigueur[90];

- et la question de savoir si les transferts effectués pour le compte du responsable du traitement relèvent du champ d'application de cette décision (par exemple, les catégories de données à caractère personnel ou les secteurs entrant dans le champ d'application)[91].

94. Lorsque des données à caractère personnel transférées par un sous-traitant (ultérieur) (pour le compte du responsable du traitement) sur la base d'une décision d'adéquation font l'objet d'un **transfert ultérieur** à partir de ce pays tiers, le niveau de protection des personnes physiques garanti par le RGPD pour ce transfert ultérieur ne doit pas non plus être compromis[92]. À cet égard, conformément à l'article 45, paragraphe 2, point a), du RGPD, toute décision d'adéquation émise par la Commission européenne couvre, entre autres, les règles des pays tiers régissant les transferts ultérieurs. Par conséquent, en vertu de l'article 44 du RGPD, le responsable du traitement n'est pas tenu de vérifier lui-même ces exigences.

95. En ce qui concerne l'obligation du responsable du traitement au titre de l'article 28, paragraphe 1, du RGPD, cela signifie que le responsable du traitement devrait veiller à ce que le sous-traitant (ultérieur) fournisse des «garanties suffisantes» également en ce qui concerne les transferts ultérieurs effectués par un sous-traitant (ultérieur) à partir d'un pays couvert par une décision d'adéquation.

96. En l'absence de décision d'adéquation, les transferts peuvent être effectués sous réserve de la mise en place de «**garanties appropriées**» conformément à **l'article 46 du RGPD**. Dans ce cas, le responsable du traitement devrait évaluer les garanties appropriées mises en place et être attentif à toute législation problématique qui pourrait empêcher le sous-traitant ultérieur de se conformer aux obligations établies dans son contrat avec le sous-traitant initial[93]. Plus précisément, le responsable du traitement devrait veiller à ce qu'une telle «évaluation de l'impact du transfert»[94] soit effectuée, conformément à la jurisprudence[95], et comme expliqué dans les recommandations 01/2020 de l'EDPB. La documentation relative aux garanties appropriées mises en place, «l'évaluation de l'impact du transfert» et les éventuelles mesures complémentaires devraient être produites par le sous-

[90] Recommandations 01/2020 de l'EDPB, paragraphe 19: «*Si l'exportateur transfère des données à caractère personnel vers des pays tiers, des régions ou des secteurs couverts par une décision d'adéquation de la Commission (dans la mesure applicable), il ne doit prendre aucune des autres mesures décrites dans les présentes recommandations. Il doit toutefois toujours vérifier si les décisions d'adéquation concernant ses transferts ont été révoquées ou invalidées*.»

[91] Recommandations 01/2020 de l'EDPB, paragraphe 19.

[92] Voir article 44 du RGPD: «*les conditions définies dans le présent chapitre sont respectées [...], y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale*».

[93] À cet égard, voir arrêt de la CJUE dans l'affaire Schrems II, points 132 et 133, dans lequel la CJUE insiste sur la nature contractuelle des CCT de la CE pour le transfert de données vers des pays tiers.

[94] Cette évaluation est expliquée plus en détail dans les recommandations 01/2020 de l'EDPB, «Étape 3: évaluer si l'instrument de transfert prévu à l'article 46 du RGPD auquel l'exportateur a recours est efficace compte tenu de toutes les circonstances du transfert».

[95] Arrêt de la CJUE dans l'affaire Schrems II, point 134.

traitant/l'exportateur[96] (le cas échéant en collaboration avec le sous-traitant/l'importateur[97]). Le responsable du traitement peut s'appuyer sur l'évaluation préparée par le sous-traitant (ultérieur) et, si nécessaire, la développer. Par exemple, lorsque l'évaluation reçue par le responsable du traitement semble incomplète, inexacte ou soulève des questions, le responsable du traitement devrait demander des informations supplémentaires, vérifier les informations et les compléter/les corriger si nécessaire, en gardant à l'esprit que l'évaluation devrait être conforme aux recommandations 01/2020 de l'EDPB et aux étapes qui y sont énoncées[98]. Il s'agit notamment d'identifier les lois et pratiques pertinentes à la lumière de toutes les circonstances du transfert[99] et d'identifier les mesures complémentaires appropriées si nécessaire[100]. À cet égard, le responsable du traitement devrait accorder une attention particulière à la question de savoir si l'exportateur de données, c'est-à-dire le sous-traitant ou le sous-traitant ultérieur, a évalué s'il existe dans le droit et/ou les pratiques du pays tiers des éléments susceptibles de porter atteinte à l'efficacité des garanties appropriées du motif de transfert invoqué par l'exportateur[101], notamment en raison de la législation et des pratiques régissant l'accès des autorités publiques du pays tiers aux données à caractère personnel transférées[102].

97. En outre, et à l'instar des transferts fondés sur une décision d'adéquation (article 45 du RGPD, voir ci-dessus les paragraphes 94 et 95), lorsque des données à caractère personnel sont transférées par un sous-traitant (ultérieur) sur la base de garanties appropriées en vertu de l'article 46 du RGPD, l'obligation du responsable du traitement en vertu de l'article 28, paragraphe 1, du RGPD couvre également l'obligation de s'assurer que le sous-traitant (ultérieur) présente des garanties suffisantes en ce qui concerne **les transferts ultérieurs**. Les garanties appropriées au titre de l'article 46 du RGPD comprennent généralement des dispositions établissant les règles qui régiront tout transfert ultérieur[103]. Cela signifie que les responsables du traitement ne sont pas tenus de vérifier si ces règles en tant que telles sont conformes aux exigences du chapitre V du RGPD. Toutefois, les responsables

[96] Recommandations 1/2022 de l'EDPB concernant la demande d'approbation et les éléments et principes des règles d'entreprise contraignantes pour les responsables du traitement (article 47 du RGPD), adoptées le 20 juin 2023, version 2.1, paragraphe 10: «[...] *En outre, il incombe, par exemple, à chaque exportateur de données d'évaluer, pour chaque transfert, au cas par cas, s'il est nécessaire de mettre en œuvre des mesures supplémentaires afin d'assurer un niveau de protection essentiellement équivalent à celui prévu par le RGPD.*»

[97] Dans l'arrêt de la CJUE dans l'affaire Schrems II, point 134, la CJUE a fait observer qu'un tel exercice de vérification peut être effectué en collaboration avec l'importateur, le cas échéant. Voir également les recommandations 01/2020 de l'EDPB, section 4.

[98] Voir en particulier «Étape 3: évaluer si l'instrument de transfert prévu à l'article 46 du RGPD auquel l'exportateur a recours est efficace compte tenu de toutes les circonstances du transfert», «Étape 4: adoption de mesures supplémentaires» et «Étape 6: réévaluation à intervalles appropriés», comme expliqué dans les recommandations 01/2020 de l'EDPB.

[99] Arrêt de la CJUE dans l'affaire Schrems II, point 126. Voir également les recommandations 01/2020 de l'EDPB, section 2,3. Étape 3: évaluer si l'instrument de transfert prévu à l'article 46 du RGPD auquel l'exportateur a recours est efficace compte tenu de toutes les circonstances du transfert Dans l'arrêt de la CJUE dans l'affaire Schrems II, point 134, la CJUE a noté qu'un tel exercice de vérification peut être effectué en collaboration avec l'importateur, le cas échéant (voir également les recommandations 01/2020 de l'EDPB, paragraphe 30).

[100] Sur la base de la jurisprudence, il appartient, dès lors, avant tout, à ce responsable du traitement ou à son sous-traitant de vérifier, au cas par cas et, le cas échéant, en collaboration avec le destinataire du transfert, si le droit du pays tiers de destination assure une protection appropriée, au regard du droit de l'Union, des données à caractère personnel transférées sur le fondement de clauses types de protection des données, en fournissant, au besoin, des garanties supplémentaires à celles offertes par ces clauses (arrêt de la CJUE dans l'affaire Schrems II, point 134). Voir également les recommandations 01/2020 de l'EDPB, section 2.4, «Étape 4: adoption de mesures supplémentaires».

[101] Voir les recommandations 01/2020 de l'EDPB, section 2.3 («Étape 3»).

[102] Voir les recommandations 01/2020 de l'EDPB, paragraphes 41 et suivants.

[103] Voir par exemple la clause 8.7 (module 1), respectivement 8.8 (modules 2 et 3) des CCT de la CE pour le transfert de données vers des pays tiers (décision d'exécution 2021/914 de la Commission) du 4 juin 2021.

du traitement devraient être en mesure de présenter des documents relatifs à ces transferts ultérieurs. Cela signifie que le responsable du traitement devrait recevoir ces informations de la part des sous-traitants (ultérieurs)/exportateurs, démontrant que les importateurs respectent effectivement les exigences relatives aux transferts ultérieurs telles qu'énoncées dans l'instrument de garanties approprié.

2.3 Sur l'interprétation de l'article 28, paragraphe 3, point a) du RGPD (question 2)

98. Afin de garantir une répartition transparente des responsabilités et des obligations, tant en interne (entre responsables du traitement et sous-traitants) qu'en externe vis-à-vis des personnes concernées et des régulateurs, en vertu de l'article 28, paragraphe 3, du RGPD, tout traitement de données à caractère personnel par un sous-traitant doit être régi par un contrat ou un autre acte juridique en vertu du droit de l'UE ou de l'État membre[104] entre le responsable du traitement et le sous-traitant. Conformément à l'article 28, paragraphe 3, point a), du RGDP, ce contrat prévoit, notamment, que le sous-traitant «*ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*». Cette disposition prévoit également que «*dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public*».

99. La demande fait référence à l'existence de contrats qui comportent un engagement de ne traiter les données à caractère personnel que sur instruction du responsable du traitement «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» (en omettant la référence au droit de l'Union ou de l'État membre). À cet égard, l'EDPB a été saisi de plusieurs questions, qui ont été abordées conjointement dans la section ci-dessous:

> 2 Un contrat ou un autre acte juridique en vertu du droit de l'Union ou de l'État membre conformément à l'article 28, paragraphe 3, du RGPD doit-il contenir l'exception prévue à l'article 28, paragraphe 3, point a), «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» (que ce soit textuellement ou dans des termes très similaires) afin d'être conforme au RGPD?
>
> 2a Si la réponse à la question 2 est négative, lorsqu'un contrat ou un autre acte juridique en vertu du droit de l'Union ou de l'État membre élargit l'exception prévue à l'article 28, paragraphe 3, point a), du RGPD pour couvrir également le droit d'un pays tiers (par exemple, «à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental»), cela constitue-t-il en soi une violation de l'article 28, paragraphe 3, point a), du RGPD?

100. Les lignes directrices 07/2020 de l'EDPB rappellent «*l'importance de négocier et de rédiger avec soin les accords de traitement des données*» en ce qui concerne toute obligation juridique de l'Union ou d'un État membre à laquelle le sous-traitant est soumis[105]. En ce qui concerne leur contenu, les lignes directrices 07/2020 de l'EDPB indiquent qu'un contrat «*entre le responsable du traitement et le sous-traitant doit respecter les exigences de l'article 28 du RGPD afin d'assurer que le sous-traitant traite*

[104] Ci-après, le terme «**contrat**» sera utilisé pour désigner «un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre».
[105] Lignes directrices 07/2020 de l'EDPB, paragraphe 121.

des données à caractère personnel conformément aux dispositions du RGPD. *Un tel accord devrait tenir compte des responsabilités spécifiques des responsables du traitement et des sous-traitants. Bien que l'article 28 dresse une liste des éléments qui doivent être abordés dans tout contrat régissant la relation entre les responsables du traitement et les sous-traitants, il laisse aux parties une certaine latitude pour négocier ces contrats*»[106]. La marge de négociation est limitée par les exigences énoncées à l'article 28, paragraphe 3, du RGPD.

[106] Lignes directrices 07/2020 de l'EDPB, paragraphe 109.

101. Tout d'abord, l'engagement du sous-traitant à ne traiter les données à caractère personnel que sur instructions documentées du responsable du traitement constitue un élément central du contrat.

102. Toutefois, comme le reconnaît l'article 28, paragraphe 3, point a), du RGPD, les sous-traitants peuvent légalement traiter des données à caractère personnel - autrement que sur instructions documentées du responsable du traitement - afin de se conformer à des obligations juridiques en vertu de la législation de l'UE ou des États membres (ci-après «**obligation juridique de l'UE/des États membres**»). La même disposition exige également que le sous-traitant s'engage à informer le responsable du traitement - à l'avance - lorsqu'une obligation juridique de l'UE/des États membres de traiter/transférer des données à caractère personnel vers un pays tiers ou une organisation internationale s'applique, à moins que cette loi n'interdise une telle information pour des raisons importantes d'intérêt public. Cet engagement est explicitement inclus, avec un libellé très similaire à celui de l'article 28, paragraphe 3, point a), du RGPD, dans les CCT la CE entre responsables du traitement et sous-traitants [107] et dans plusieurs clauses contractuelles types, en particulier les CCT adoptées par les AC danoise[108], slovène[109] et lituanienne[110] aux fins du respect de l'article 28 du RGPD.

103. Outre l'engagement de ne traiter que sur instruction documentée du responsable du traitement, l'article 28, paragraphe 3, point a), du RGPD contient donc trois éléments principaux: a) une règle régissant les situations dans lesquelles une obligation juridique contraint le sous-traitant à effectuer un traitement de données à caractère personnel qui n'est pas fondé sur les instructions du responsable

[107] Voir en particulier les clauses 7.1, point a) et 7.8, point a):
- Clause 7.1, point a): «*Le sous-traitant ne traite 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 de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées*.» (soulignement ajouté). Dans leur avis conjoint sur les projets de CCT de la CE, l'EDPB et le CEPD ont recommandé l'inclusion du libellé complet de l'article 28, paragraphe 3, point a) (en ajoutant donc une référence à l'obligation du sous-traitant d'informer le responsable du traitement de l'obligation juridique) afin de renforcer la cohérence. Avis conjoint 1/2021 de l'EDPB et du CEPD concernant la décision d'exécution de la Commission européenne relative aux clauses contractuelles types entre responsables du traitement et sous-traitants pour les questions visées à l'article 28, paragraphe 7, du règlement (UE) 2016/679 et à l'article 29, paragraphe 7, du règlement (UE) 2018/1725, paragraphe 38. La formulation «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» était déjà présente dans le projet de CCT.
- Clause 7.8, point a): «*Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725.»* En ce qui concerne la clause 7.8, point a), l'EDPB et le CEPD ont recommandé l'inclusion d'une référence à la possibilité pour le sous-traitant d'effectuer des transferts sur la base d'une exigence spécifique prévue par la législation de l'Union ou de l'État membre à laquelle le sous-traitant est soumis, ce qui n'était pas spécifié initialement dans le projet de CCT. Annexe 2 de l'avis conjoint 1/2021 de l'EDPB et du CEPD, observations relatives à la clause 7.7, point a).

[108] Clauses contractuelles types de l'AC danoise aux fins du respect de l'article 28 du RGPD, en particulier les clauses 4.1 et 8.2. Dans son avis 14/2019 sur le projet de clauses contractuelles types présenté par l'AC danoise (article 28, paragraphe 8, du RGPD), l'EDPB a recommandé l'inclusion du libellé de l'article 28, paragraphe 3, point a), afin de garantir la sécurité juridique.

[109] Clauses contractuelles types de l'AC slovène aux fins du respect de l'article 28 du RGPD, en particulier les clauses 3.1 et 7.2.

[110] Clauses contractuelles types de l'AC lituanienne aux fins du respect de l'article 28 du RGPD, en particulier les clauses 4.1, 22 et 23.

du traitement, et qui n'est donc pas effectué pour le compte du responsable du traitement, b) la nécessité pour le sous-traitant d'informer le responsable du traitement[111], et c) la référence à cette obligation juridique telle qu'elle découle du droit de l'Union ou du droit d'un État membre.

104. Dans ce contexte, l'EDPB rappelle qu'en tant que principe général, les contrats ne sauraient prévaloir sur la loi. En substance, que le contrat stipule ou non la clause prévue à l'article 28, paragraphe 3, point a), du RGPD («*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*»), une telle clause ne saurait empêcher une obligation juridique de venir s'appliquer en plus des exigences contractuelles ou, dans certains cas, de venir s'y opposer. En outre, conformément au principe général selon lequel un contrat ne crée pas d'obligations à l'égard des tiers, un contrat ne saurait lier, par exemple, les autorités publiques d'un État membre ou d'un pays tiers[112].

105. Tous les contrats conclus entre un responsable du traitement et un sous-traitant doivent traiter des situations dans lesquelles le sous-traitant peut être tenu, en vertu d'une obligation juridique, de traiter des données à caractère personnel autrement que sur le fondement des instructions du responsable du traitement. En outre, l'obligation du sous-traitant d'informer le responsable du traitement avant d'effectuer un traitement qui n'est pas fondé sur ses instructions constitue également un élément central du contrat, qui doit également y être inclus[113].

106. Pour les données à caractère personnel traitées en dehors de l'EEE, la référence au droit de l'UE ou des États membres peut s'avérer peu pertinente, étant donné qu'un sous-traitant situé en dehors de l'EEE ne sera qu'exceptionnellement soumis aux obligations juridiques de l'UE ou des États membres. À cet égard, l'EDPB note que les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers, qui sont destinés à satisfaire, outre les exigences de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, point d), du RGPD, les exigences de l'article 28, paragraphes 3 et 4, du RGPD[114], ne contiennent pas de formulation similaire à la clause «à moins qu'il ne soit tenu d'y procéder (...)» prévue l'article 28, paragraphe 3, point a), du RGPD. Toutefois, l'obligation de ne traiter les données à caractère personnel que sur instructions documentées du responsable du traitement, à moins que la législation de l'UE ou d'un État membre ne l'exige, est déjà abordée indirectement par la

[111] L'article 28, paragraphe 3, point a), du RGPD prévoit que lorsque le droit de l'Union ou de l'État membre impose au sous-traitant de traiter des données à caractère personnel, alors «*le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public*».

[112] C'est la raison pour laquelle les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers comprennent plusieurs garanties exigeant que l'exportateur et l'importateur évaluent les obligations juridiques issues de la législation des pays tiers avant de transférer les données afin de s'assurer qu'elles ne vont pas au-delà de ce qui est nécessaire dans une société démocratique [clause 14, points a) à d)], exigeant que l'importateur notifie l'exportateur en cas de changement et que ce dernier agisse en conséquence [clause 14 points e) et f)], et imposant à l'importateur des obligations en cas d'accès par les autorités publiques (clause 15). Voir l'arrêt de la CJUE dans l'affaire Schrems II, points 125 et 141.

[113]Dans son avis 18/2021 sur le projet de clauses contractuelles types soumis par l'AC lituanienne (article 28, paragraphe 8, du RGPD), l'EDPB a recommandé l'inclusion du dernier élément de l'article 28, paragraphe 3, point a), dans les CCT (c'est-à-dire l'obligation pour le sous-traitant d'informer le responsable du traitement de toute obligation juridique applicable), avis 18/2021 de l'EDPB, paragraphe 19.

[114] Voir le considérant 9 des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers: «*Si le traitement suppose des transferts de données de responsables du traitement soumis au règlement (UE) 2016/679 vers des sous-traitants ne relevant pas du champ d'application territorial dudit règlement ou de sous-traitants soumis au règlement (UE) 2016/679 vers des sous-traitants ultérieurs ne relevant pas du champ d'application territorial dudit règlement, les clauses contractuelles types figurant à l'annexe de la présente décision devraient également permettre de satisfaire aux exigences de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679.*»

clause 8.1 des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers.[115] En outre, cela ne signifie pas que l'obligation d'information prévue à l'article 28, paragraphe 3, point a), du RGPD n'est pas prise en compte, étant donné que les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers prévoient explicitement l'obligation pour l'importateur de données d'informer l'exportateur de données s'il n'est pas en mesure de suivre les instructions du responsable du traitement[116]. Par conséquent, l'engagement du sous-traitant d'informer le responsable du traitement lorsqu'une obligation juridique de traitement s'applique (qu'elle découle du droit de l'Union, du droit d'un État membre ou du droit d'un pays tiers) découle des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers sans le besoin d'utiliser le libellé exact «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» de l'article 28, paragraphe 3, point a), du RGPD [élément c) susmentionné].

107. Cela est conforme à l'objectif de l'article 28, paragraphe 3, point a), du RGPD, qui consiste à garantir que le responsable du traitement est informé lorsque le sous-traitant est tenu par la loi de traiter des données à caractère personnel autrement que sur le fondement des instructions du responsable du traitement.

108. À la lumière de l'analyse ci-dessus, l'EDPB estime que l'inclusion, dans un contrat entre le responsable du traitement et le sous-traitant[117], de l'exception prévue à l'article 28, paragraphe 3, point a), du

[115] À la clause 8, portant sur les garanties en matière de protection des données (module 2: transfert de responsable du traitement à sous-traitant), section 8.1 - instructions:
«*a) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées de l'exportateur de données. L'exportateur de données peut donner ces instructions pendant toute la durée du contrat.*
b) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données.»
De même, au module 3: transfert de sous-traitant à sous-traitant, clause 8: garanties en matière de protection des données indique, section 8.1 – instructions:
«*a) L'exportateur de données a informé l'importateur de données qu'il agit en qualité de sous-traitant sur instructions de son ou ses responsables du traitement, instructions qu'il met à la disposition de l'importateur de données avant le traitement.*
b) L'importateur de données ne traite les données à caractère personnel que sur instructions documentées du responsable du traitement, telles qu'elles lui ont été communiquées par l'exportateur de données, ainsi que sur instructions documentées supplémentaires de l'exportateur de données. Ces instructions supplémentaires ne sont pas en contradiction avec les instructions du responsable du traitement. Le responsable du traitement ou l'exportateur de données peut donner d'autres instructions documentées concernant le traitement des données pendant toute la durée du contrat.
c) S'il n'est pas en mesure de suivre ces instructions, l'importateur de données en informe immédiatement l'exportateur de données. Lorsque l'importateur de données n'est pas en mesure de suivre les instructions du responsable du traitement, l'exportateur de données en informe immédiatement ce dernier.»

[116] En plus de la clause 8.1 (voir la note de bas de page précédente), la clause 14, point e) stipule que: «*L'importateur de données accepte d'informer sans délai l'exportateur de données si, après avoir souscrit aux présentes clauses et pendant la durée du contrat, il a des raisons de croire qu'il est ou est devenu soumis à une législation ou à des pratiques qui ne sont pas conformes aux exigences du paragraphe a), notamment à la suite d'une modification de la législation du pays tiers ou d'une mesure (telle qu'une demande de divulgation) indiquant une application pratique de cette législation qui n'est pas conforme aux exigences du paragraphe a). [Pour le module 3: l'exportateur de données transmet la notification au responsable du traitement.]*»

[117] En particulier, lorsque le responsable du traitement et le sous-traitant s'appuient sur leur propre contrat de traitement plutôt que sur les CCT de la CE entre responsables du traitement et sous-traitants, sur les CCT adoptées par les AC aux fins du respect de l'article 28 du RGPD ou sur les CCT de la CE pour le transfert de données vers des pays tiers. Voir également le considérant 109 et l'article 28, paragraphe 6, du règlement (UE) 2016/679.

RGPD «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*» (soit textuellement, soit dans des termes très similaires) est fortement recommandée, mais pas strictement nécessaire pour garantir le respect de l'article 28, paragraphe 3, point a), du RGPD. Cette position est sans préjudice de la nécessité d'une obligation contractuelle d'informer le responsable du traitement lorsque le sous-traitant est juridiquement obligé de traiter des données à caractère personnel autrement que sur le fondement des instructions du responsable du traitement, comme le prévoit l'article 28, paragraphe 3, point a), du RGPD. Lorsqu'il est clair que les obligations juridiques de l'UE ou des États membres sont pertinentes pour le traitement, l'utilisation du libellé de l'article 28, paragraphe 3, point a), du RGPD contribuerait à démontrer la conformité.

109. L'EDPB se penche maintenant sur la question de savoir si un contrat comportant une exception plus large couvrant également le droit d'un pays tiers, comme par exemple une exception à l'engagement de ne traiter les données à caractère personnel que sur instructions documentées du responsable du traitement «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*», constitue en soi une violation de l'article 28, paragraphe 3, point a), du RGPD.

110. Ce libellé, s'il n'est pas accompagné de précisions supplémentaires, peut englober deux situations distinctes qui devraient être analysées séparément à la lumière du contexte juridique:

- l'obligation juridique ou l'ordonnance contraignante envisagée découle du droit de l'Union ou du droit d'un État membre (de l'EEE).
- l'obligation juridique ou l'ordonnance contraignante envisagée découle de lois autres que le droit de l'Union ou le droit d'État membre (de l'EEE).

111. La première situation relève des dispositions expresses de l'article 28, paragraphe 3, point a), du RGPD, qui prévoit un engagement contractuel pour le sous-traitant de ne traiter que sur instructions documentées du responsable du traitement «*à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis*». Ceci s'applique indépendamment du fait que le traitement des données à caractère personnel soit effectué à l'intérieur ou à l'extérieur de l'EEE.

112. Le droit de l'Union, y compris le RGPD et les obligations juridiques des États membres, s'inscrivent dans la même tradition constitutionnelle que le RGPD, qui consacre en tant que droit fondamental la protection des personnes physiques au regard du traitement de leurs données à caractère personnel, en vertu de l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (ci-après le «**TFUE**») et de l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne(ci-après la «**Charte**»)[118].

113. Lorsque les parties peuvent démontrer, sur la base d'autres éléments indiqués dans leur(s) contrat(s), que seule cette première situation est couverte par les mots «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental»,* cette formulation n'a pas d'incidence sur les garanties prévues par l'article 28, paragraphe 3, point a), du RGPD.

114. Dans certains cas, la portée du (des) contrat(s) entre les parties s'étendra au-delà de cette première situation, ce qui signifie qu'une référence à «*la loi ou à une ordonnance contraignante d'un organisme gouvernemental*» englobera les obligations juridiques/ordonnances contraignantes découlant de lois autres que le droit de l'Union ou le droit d'un État membre (de l'EEE) (deuxième situation).

115. L'EDPB note que les exigences relatives au traitement des données fondées sur des lois autres que celles de l'Union ou des États membres (de l'EEE) ne s'inscrivent pas nécessairement dans la même tradition constitutionnelle et ne sauraient être automatiquement considérées de la même manière que celles relevant de l'ordre juridique de l'UE (à la lumière de l'article 44 du RGPD). Sur ce point, l'EDPB rappelle qu'en vertu de l'article 6 du RGPD, les termes «obligation légale», «intérêt public» et «autorité publique» se réfèrent au droit de l'Union ou de l'État membre[119]. De même, l'EDPB note que l'article 29 du RGPD sur le traitement sous l'autorité du responsable du traitement ou du sous-traitant prévoit que: «*[l]e sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces*

[118] Le considérant 1 du RGPD fait référence à l'article 16, paragraphe 1 du traité sur le fonctionnement de l'Union européenne (le «TFUE») et à l'article 8, paragraphe 1 de la charte des droits fondamentaux de l'Union européenne (la «Charte»). L'article 52, paragraphe 1, de la Charte dispose que «*[t]oute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés*. *Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.*»

[119] L'article 6, paragraphe 3, du RGPD prévoit que lorsque la base juridique du traitement est une «obligation légale» [article 6, paragraphe 1, point c], du RGPD) ou «une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement» [article 6, paragraphe 1, point e), du RGPD], il s'agit des dispositions prévues par le droit de l'Union ou le droit de l'État membre auxquelles le responsable du traitement est soumis. En référence à l'article 6 du RGPD, le considérant 40 du RGPD explique que lorsque la base juridique du traitement est prévue par la loi, cela signifie «*soit dans le présent règlement soit dans une autre disposition du droit national ou du droit de l'Union, ainsi que le prévoit le présent règlement*». L'article 49, paragraphe 4, du RGPD dispose que seuls les intérêts publics reconnus dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis peuvent conduire à l'application de cette dérogation.

données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre». (soulignement ajouté).

116. Dans le contexte des transferts, il est prévisible que des exigences légales peuvent également découler de législations autres que celle de l'UE ou des États membres. Lorsque des transferts sont effectués, l'EDPB rappelle que le chapitre V du RGPD s'applique en plus de l'article 28 du RGPD. L'EDPB estime que, en ce qui concerne les données à caractère personnel traitées en dehors de l'EEE, l'article 28, paragraphe 3, point a), du RGPD n'empêche pas – en principe – l'inclusion, dans le contrat, de dispositions qui répondent aux exigences du droit d'un pays tiers en matière de traitement des données à caractère personnel transférées. De telles dispositions peuvent être incluses notamment pour garantir le respect du chapitre V du RGPD, mais il est peu vraisemblable que le simple fait d'inclure le libellé «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» soit suffisant.

117. Dans ce contexte, l'EDPB observe que les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers traitent spécifiquement des «législations et pratiques locales ayant une incidence sur le respect des clauses» à la clause 14 et des «obligations de l'importateur de données en cas d'accès des autorités publiques» à la clause 15. Avant de signer les CCT, les parties doivent évaluer s'il existe des législations et des pratiques locales ayant une incidence sur le respect des clauses (clause 14 des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers). La clause 14 impose aux parties de garantir qu'elles n'ont pas connaissance de législations ou de pratiques en vigueur dans le pays tiers où l'importateur est établi qui l'empêcheraient de remplir les obligations qui lui incombent en vertu des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers, à la suite d'une évaluation de ces législations et pratiques par l'importateur, et impose à l'importateur d'informer rapidement l'exportateur de tout changement, auquel cas il incombe à l'exportateur d'identifier des mesures appropriées pour remédier à la situation, ou, en vertu de la clause 14, de suspendre le transfert, voire de résilier le contrat. La clause 15 impose certaines obligations à l'importateur de données en cas d'accès par les autorités publiques d'un pays tiers. Elle définit un certain nombre de mesures que l'importateur de données doit prendre lorsqu'il est confronté à l'accès d'un gouvernement d'un pays tiers (soit sur demande, soit directement), afin de s'assurer que le responsable du traitement est (en fin de compte) informé. Outre l'obligation de notifier l'exportateur de données, l'importateur a notamment l'obligation d'examiner la légalité de la demande d'accès et de documenter cette évaluation juridique, ainsi que l'obligation de contester la demande dans certains cas. L'exportateur de données - en consultation avec le responsable du traitement lorsque l'exportateur de données n'est pas le responsable du traitement - sera alors en mesure de prendre les mesures nécessaires, y compris la suspension éventuelle du transfert ou la résiliation des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers. La question de savoir si les transferts (ultérieurs) vers les autorités du pays tiers sont conformes au RGPD dépendra d'une analyse au cas par cas (entre autres en ce qui concerne la base juridique, la responsabilité du traitement et le respect du chapitre V du RGPD). En vertu du module 3 des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers (transfert de sous-traitant à sous-traitant), l'importateur/sous-traitant a l'obligation de mettre l'évaluation juridique à la disposition de l'exportateur. À cet égard, l'EDPB se réfère également aux paragraphes 88, 89 et 106 ci-dessus.

118. En outre, en vertu des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers , tant l'exportateur que l'importateur sont tenus de s'assurer que la législation du pays tiers de destination permet à l'importateur de se conformer aux CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers avant de transférer des données à caractère personnel vers ce

pays tiers[120]. Lorsque le sous-traitant exporte des données à caractère personnel pour le compte du responsable du traitement, cette obligation incombe également au responsable du traitement (voir également les paragraphes 79 et suivants ci-dessus).

119. De même, les recommandations relatives aux règles d'entreprise contraignantes pour les responsables du traitement (BCR-C) et les référentiels relatifs aux règles d'entreprise contraignantes applicables aux-sous-traitants définissent également un ensemble d'obligations dans le cas où un membre du BCR est soumis à un conflit entre ses lois locales et les BCR[121], et/ou reçoit une demande de divulgation de la part d'une autorité chargée de l'application de la loi ou d'un organisme de sécurité de l'État[122]. Plus précisément, les recommandations 1/2022 de l'EDPB[123] indiquent que les règles d'entreprise contraignantes pour les responsables du traitement (BCR-C) devraient contenir des clauses traitant des législations et pratiques locales ayant une incidence sur le respect des BCR-C (section 5.4.1) ainsi que des obligations de l'importateur de données en cas de demandes d'accès émanant du gouvernement (section 5.4.2). Les BCR-C peuvent servir de mécanisme de transfert pour les transferts vers des sous-traitants au sein du groupe.

120. Dans les cas où les transferts sont couverts par des décisions d'adéquation, la législation concernant «*l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation*» est l'un des éléments dont la Commission européenne doit tenir compte lorsqu'elle évalue le caractère adéquat du niveau de protection, conformément à l'article 45, paragraphe 2, point a), du RGPD[124].

[120] Arrêt de la CJUE dans l'affaire *Schrems II*, point 141. Voir également les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers, clause 14, points a) à d).

[121] Section 5.4.1 «Législations et pratiques locales ayant une incidence sur le respect des BCR-C», recommandations 1/2022 de l'EDPB concernant la demande d'approbation et les éléments et principes des règles d'entreprise contraignantes pour les responsables du traitement (article 47 du RGPD). Section 6.3 «Le besoin de transparence dans les cas où la législation nationale empêche le groupe d'observer les BCR» du GT «Article 29», Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants, WP 257 rev.01, approuvé par l'EDPB le 25 mai 2018.

[122] Section 5.4.2 «Obligations de l'importateur de données en cas de demandes d'accès émanant du gouvernement», recommandations 1/2022 de l'EDPB concernant la demande d'approbation et les éléments et principes des règles d'entreprise contraignantes pour les responsables du traitement (article 47 du RGPD); voir également section 6.3 «Le besoin de transparence dans les cas où la législation nationale empêche le groupe d'observer les BCR» du GT «Article 29», Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants, WP 257 rev.01.

[123] Recommandations 1/2022 de l'EDPB concernant la demande d'approbation et les éléments et principes des règles d'entreprise contraignantes pour les responsables du traitement (article 47 du RGPD).

[124] La CJUE a abordé cet élément dans ses arrêts Schrems I et Schrems II. Arrêt de la CJUE du 6 octobre 2015, *Maximillian Schrems/Data Protection Commissionner*, (ci-après l'«arrêt de la CJUE dans l'affaire Schrems I»), C-362/14, ECLI:EU:C:2015:650, points 91 et suivants. Arrêt de la CJUE dans l'affaire Schrems II, points 141, 174-177, 187-189.

121. Les décisions d'adéquation [125], les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers[126] et les recommandations et référentiels relatifs aux BCR[127] s'accordent sur l'interprétation selon laquelle le niveau de protection garanti par le RGPD[128] ne sera pas affaibli par des législations et pratiques d'un pays tiers qui sont respectueuses de l'essence des libertés et des droits fondamentaux consacrés par le TFUE, la Charte et le RGPD et qui ne vont pas au-delà des mesures nécessaires et proportionnés dans une société démocratique prises aux fins de sauvegarder l'un des objectifs énumérés à l'article 23, paragraphe 1, du RGPD. C'est la raison pour laquelle les CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers[129] et les recommandations et référentiels relatifs aux BCR[130] comprennent des dispositions qui prévoient des conséquences différentes pour les législations et les pratiques selon qu'elles portent atteinte ou non au niveau de protection garanti par le RGPD. Les contrats ad hoc fondés sur l'article 46, paragraphe 3, point a), du RGPD devraient également contenir des dispositions similaires[131].

122. Il ressort clairement de ce qui précède que, lorsque la législation du pays tiers impose au sous-traitant de traiter des données à caractère personnel autrement que sur le fondement des instructions du responsable du traitement, le niveau de protection consacré par le RGPD ne sera respecté que si ladite législation satisfait aux conditions susmentionnées. En tout état de cause, le sous-traitant devrait mettre en œuvre des mesures supplémentaires si ces conditions ne sont pas satisfaites et le contrat devrait veiller à ce que lesdites conditions soient remplies.

123. Lorsque le sous-traitant traite des données à caractère personnel au sein de l'EEE, il peut toujours être confronté au droit d'un pays tiers, dans certaines circonstances. L'EDPB souligne que l'ajout dans le contrat d'une référence au droit d'un pays tiers ne libère pas le sous-traitant de ses obligations au titre du RGPD.

---

[125] Cf. article 45, paragraphe 2, point a), du RGPD: «*l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées;*». Voir également les Critères de référence pour l'adéquation du GT «Article 29» WP 254 rev.01, adoptés le 6 février 2018 et approuvés par l'EDPB le 25 mai 2018. La notion de «niveau de protection adéquat» a été développée par la CJUE dans ses arrêts Schrems I (point 73 et 74) et Schrems II (point 94).

[126] Clause 14, point a), des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers.

[127] Cela est explicite dans les recommandations 1/2022 de l'EDPB (ci-après les «recommandations BCR-C»), version 2.1, points 5.4.1 et 5.4.2. La même interprétation sous-tend implicitement la section 6.3 «Le besoin de transparence dans les cas où la législation nationale empêche le groupe d'observer les BCR» du GT «Article 29», Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants, WP 257 rev.01, approuvé par l'EDPB le 25 mai 2018.

[128] Recommandations 01/2020 de l'EDPB sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE et les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, paragraphes 22 et 24.

[129] Clause 14 des CCT de la CE pour le transfert de données à caractère personnel vers des pays tiers.

[130] Voir note de bas de page 127.

[131] Recommandations 01/2020 de l'EDPB sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE , v. 2.0, paragraphe 66.

124. À la lumière de l'analyse qui précède, l'EDPB estime que l'inclusion d'un libellé similaire à «*à moins qu'il ne soit tenu de le faire par la loi ou par une ordonnance contraignante d'un organisme gouvernemental*» est une prérogative relevant de la liberté contractuelle des parties et ne constitue pas en soi une violation de l'article 28, paragraphe 3, point a), du RGPD. Une telle prérogative reste sans préjudice de l'obligation de se conformer au RGPD chaque fois que des données à caractère personnel sont traitées. En outre, une telle clause n'exonère pas le responsable du traitement et le sous-traitant du respect des obligations qui leur incombent en vertu du RGPD, notamment en ce qui concerne les informations à fournir au responsable du traitement et, le cas échéant, les conditions des transferts vers des pays tiers de données à caractère personnel traités pour le compte du responsable du traitement.[132]

125. Enfin, la demande présente une question subsidiaire:

> Si la réponse à la question 2a est négative, cette exception élargie doit-elle être interprétée comme une instruction documentée émise par le responsable du traitement au sens de l'article 28, paragraphe 3, point a), du RGPD?

126. À la lumière de la réponse donnée ci-dessus, l'EDPB considère que la question subsidiaire est de savoir si les parties peuvent prétendre que la formulation «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» (que ce soit textuellement ou dans des termes très similaires) dans leur contrat doit être interprétée comme une instruction documentée du responsable du traitement au sens de l'article 28, paragraphe 3, point a), du RGPD.

127. L'EDPB examine tout d'abord si cet argument est défendable lorsque l'obligation juridique ou l'ordonnance contraignante découle du droit de l'Union ou du droit d'un État membre (de l'EEE).

128. L'EDPB relève que la notion d'«instruction» telle qu'elle est utilisée à l'article 28, paragraphe 3, point a), du RGPD concerne spécifiquement le responsable du traitement, qui définit le traitement des données que le sous-traitant est censé effectuer pour son compte et la manière dont il doit le faire[133]. Toute disposition que le responsable du traitement inclut dans le contrat avec son prestataire de services / sous-traitant et qui ne consiste pas en une demande de traitement de données à caractère personnel pour le compte du responsable du traitement n'est pas considérée comme une instruction au sens de l'article 28, paragraphe 3, point a), du RGPD. En outre, les instructions du responsable du traitement devraient être suffisamment précises pour couvrir un traitement spécifique de données à caractère personnel, ce qui n'est pas le cas du libellé en question. En outre, le responsable du traitement serait (devrait être) toujours en mesure de retirer une telle instruction — et aurait même l'obligation juridique de le faire si l'instruction de traiter des données à caractère personnel pour le compte du responsable du traitement enfreint le RGPD. Le sous-traitant devrait alors se conformer au retrait de l'instruction du responsable du traitement et mettre fin au traitement.

129. En donnant des instructions au sous-traitant, le responsable du traitement met en pratique sa détermination des finalités et des moyens du traitement des données, notamment en exerçant une influence sur les éléments clés du traitement[134]. En principe, l'influence du responsable du traitement sur le traitement des données à caractère personnel cesse lorsque la législation de l'Union ou des États membres impose au sous-traitant d'effectuer un traitement de données à caractère personnel que le

[132]En particulier, l'obligation du responsable du traitement de veiller à ce que, en ce qui concerne le traitement en dehors de l'EEE, seule la législation d'un pays tiers garantissant un niveau de protection essentiellement équivalent puisse exiger le traitement par le sous-traitant. Voir également les paragraphes 116 à 122 ci-dessus.
[133] Lignes directrices 07/2020 de l'EDPB, paragraphe 116.
[134] Lignes directrices 07/2020 de l'EDPB, paragraphe 20.

responsable du traitement n'est pas en mesure de contrôler ou d'empêcher[135]. Bien que le responsable du traitement puisse rappeler au sous-traitant de se conformer au droit de l'Union ou au droit d'un État membre, cela ne saurait être interprété comme une instruction au sens de l'article 28, paragraphe 3, point a), du RGPD[136]. Le RGPD lui-même reconnaît cet état de fait, précisément en soulignant que le sous-traitant ne doit traiter que sur le fondement d'une 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 de l'État membre auquel le sous-traitant est soumis (article 28, paragraphe 3, point a), du RGPD), et doit immédiatement informer le responsable du traitement si une instruction enfreint le RGPD (article 28, paragraphe 3, du RGPD, dernier alinéa).

130. L'EDPB considère que le raisonnement ci-dessus s'applique également lorsque l'obligation juridique ou l'ordonnance contraignante découle du droit d'un pays tiers. Dans cette situation, la loi en question limite l'influence que le responsable du traitement peut exercer sur le traitement des données.

131. Outre ce qui précède, une clause par laquelle un sous-traitant s'engage à ne traiter des données à caractère personnel que sur le fondement d'une instruction documentée du responsable du traitement «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» indique en soi que le traitement sur instruction du responsable du traitement est la règle, alors que l'exception existe précisément pour le traitement non fondé sur une instruction du responsable du traitement (comme le montre les mots «à moins que»). En outre, il appartient toujours au sous-traitant de décider s'il se conforme à la demande juridique ou à l'injonction contraignante à laquelle il est soumis ou s'il est confronté aux conséquences juridiques de ne pas s'y conformer.

132. Sur cette base, l'EDPB conclut que «*à moins qu'il ne soit tenu d'y procéder en vertu de la loi ou d'une ordonnance contraignante d'un organisme gouvernemental*» (que ce soit textuellement ou dans des termes très similaires) ne peut être interprété comme une instruction documentée du responsable du traitement. Le responsable du traitement reste responsable lorsqu'il n'a pas veillé à ce que le sous-traitant (ultérieur) traite les données à caractère personnel uniquement sur le fondement de ses instructions documentées. Toutefois, cela ne s'applique pas lorsque le traitement est requis par la législation de l'UE ou d'un État membre, ou pour le traitement en dehors de l'EEE, requis par la législation d'un pays tiers à laquelle le sous-traitant (ultérieur) est soumis et que cette législation assure un niveau de protection essentiellement équivalent.

Pour le comité européen de la protection des données

La présidente

(Anu Talus)

[135] À cet égard, la situation pourrait alors être celle prévue par l'article 4, paragraphe 7, du RGPD, qui dispose que lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. Voir arrêt de la CJUE du 11 janvier 2024, *État belge (Données traitées par un journal officiel),* C-231/22, ECLI:EU:C:2024:7, point 28-30, 35 et 39; lignes directrices 07/2020 de l'EDPB, paragraphes 22-24.

[136] Un tel rappel sera plutôt considéré comme la mise en place par le responsable du traitement de garanties contractuelles visant à assurer que le traitement effectué pour le compte du responsable du traitement sera conforme à toutes les exigences du RGPD et assurera la protection des droits de la personne concernée.