Recommandations

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

Recommandations 01/2020 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

Historique des versions

Version 2.0	18 juin 2021	Adoption des recommandations après consultation publique
Version 1.0	10 novembre 2020	Adoption des recommandations après consultation publique

Résumé

Le règlement général de l'UE sur la protection des données (RGPD) a été adopté dans un double objectif: faciliter la libre circulation des données à caractère personnel au sein de l'Union européenne, tout en préservant les libertés et droits fondamentaux des personnes, en particulier leur droit à la protection des données à caractère personnel.

Dans son récent arrêt dans l'affaire C-311/18 (Schrems II), la Cour de justice de l'Union européenne (CJUE) nous rappelle que la protection accordée aux données à caractère personnel dans l'Espace économique européen (EEE) doit se déplacer avec les données, où qu'elles aillent. Le transfert de données à caractère personnel vers des pays tiers ne saurait être un moyen de compromettre ou de diluer la protection dont elles bénéficient au sein de l'EEE. La Cour l'affirme également en précisant que le niveau de protection dans les pays tiers ne doit pas être identique, mais essentiellement équivalent à celui garanti dans l'EEE. La Cour confirme également la validité des clauses contractuelles types en tant qu'instrument de transfert pouvant servir à assurer contractuellement un niveau de protection essentiellement équivalent aux données transférées vers des pays tiers.

Les clauses contractuelles types et les autres instruments de transfert visés à l'article 46 du RGPD ne fonctionnent pas en vase clos. La Cour indique que les responsables du traitement ou les sous-traitants, agissant en tant qu'exportateurs, sont chargés de vérifier, au cas par cas et, le cas échéant, en collaboration avec l'importateur dans le pays tiers, si le droit ou la pratique du pays tiers compromet l'efficacité des garanties appropriées contenues dans les instruments de transfert visés à l'article 46 du RGPD. Dans ces cas, la Cour permet toujours aux exportateurs de mettre en œuvre des mesures supplémentaires qui remédient à ces lacunes de la protection et la portent au niveau exigé par le droit de l'Union. La Cour ne précise pas ce que pourraient être ces mesures. Elle souligne toutefois que les exportateurs devront les identifier au cas par cas. Cette approche est conforme au principe de responsabilité énoncé à l'article 5, paragraphe 2, du RGPD, qui impose aux responsables du traitement de veiller au respect des principes consacrés par le RGPD en matière de protection des données à caractère personnel et d'être en mesure de le prouver.

Le comité européen de la protection des données a adopté les présentes recommandations afin d'aider les exportateurs (qu'il s'agisse de responsables du traitement ou de sous-traitants, d'entités privées ou d'organismes publics traitant des données à caractère personnel relevant du champ d'application du RGPD) à s'acquitter de la tâche complexe d'évaluer les pays tiers et de recenser les mesures complémentaires appropriées lorsqu'elles sont nécessaires. Ces recommandations présentent aux exportateurs une série d'étapes à suivre, des sources d'information potentielles et quelques exemples de mesures supplémentaires qui pourraient être mises en place.

Premièrement, le comité européen de la protection des données recommande aux exportateurs de **connaître leurs transferts**. Cartographier tous les transferts de données à caractère personnel vers des pays tiers peut se révéler ardu. Il est toutefois nécessaire de savoir où vont les données à caractère personnel pour garantir qu'elles bénéficient d'un niveau de protection essentiellement équivalent, quel que soit l'endroit où elles sont traitées. Les exportateurs doivent également vérifier que les données qu'ils transfèrent sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Deuxièmement, il y a lieu de **vérifier sur quel instrument le transfert s'appuie** parmi ceux énumérés au chapitre V du RGPD. Si la Commission européenne a déjà déclaré que le pays, le territoire ou le secteur vers lequel les données sont transférées est adéquat, par voie d'une décision d'adéquation au titre de l'article 45 du RGPD ou de la directive 95/46 antérieure, tant que la décision est en vigueur, l'exportateur sera uniquement tenu de vérifier que la décision d'adéquation est toujours valable. En l'absence de décision d'adéquation, l'exportateur doit recourir à l'un des instruments de transfert visés à l'article 46 du RGPD. Ce n'est que dans certains cas que l'exportateur peut invoquer l'une des dérogations prévues à l'article 49 du RGPD, pour autant qu'il remplisse les conditions requises. Les

dérogations ne peuvent pas devenir «la règle» dans la pratique, mais doivent être limitées à des situations particulières.

Troisièmement, il convient d'**évaluer** s'il existe dans le droit et/ou les pratiques en vigueur du pays tiers des éléments susceptibles de porter atteinte à l'efficacité des garanties appropriées qu'offrent les instruments de transfert auxquels l'exportateur a recours dans le cadre du transfert particulier. L'évaluation de l'exportateur devrait porter d'abord et surtout sur la législation du pays tiers qui est pertinente pour son transfert et l'instrument de transfert visé à l'article 46 du RGPD utilisé. L'examen des pratiques des autorités publiques du pays tiers permettra à l'exportateur de vérifier si les garanties contenues dans l'instrument de transfert peuvent garantir, dans la pratique, une protection effective des données à caractère personnel transférées. L'examen de ces pratiques sera particulièrement pertinent aux fins de l'évaluation de l'exportateur dans les cas suivants:

(i.) lorsque la législation du pays tiers qui répond formellement aux normes de l'UE n'est manifestement pas appliquée ou respectée dans la pratique;

(ii.) lorsqu'il existe des pratiques incompatibles avec les engagements de l'instrument de transfert en cas d'absence de législation pertinente dans le pays tiers;

(iii.) les données transférées de l'exportateur et/ou l'importateur relèvent ou pourraient relever du champ d'application d'une législation problématique (à savoir porter atteinte à la garantie contractuelle de l'instrument de transfert d'un niveau de protection essentiellement équivalent et ne pas respecter les normes de l'Union en matière de droits fondamentaux, de nécessité et de proportionnalité).

Dans les deux premiers cas, l'exportateur devra suspendre le transfert ou mettre en œuvre des mesures supplémentaires appropriées s'il souhaite le poursuivre.

Dans le troisième cas, compte tenu des incertitudes entourant l'application éventuelle d'une législation problématique au transfert, l'exportateur peut décider: de suspendre le transfert; de mettre en œuvre des mesures supplémentaires pour le réaliser; ou, à titre subsidiaire, de procéder au transfert sans mettre en œuvre de mesures supplémentaires s'il estime, et est en mesure de démontrer et de documenter, qu'il n'a aucune raison de croire que la législation pertinente et problématique sera interprétée et/ou appliquée dans la pratique de manière à couvrir les données transférées de l'exportateur et l'importateur.

Pour évaluer les éléments à prendre en considération lors de l'appréciation de la législation d'un pays tiers en matière d'accès des autorités publiques aux données à des fins de surveillance, le comité européen de la protection des données renvoie le lecteur à ses recommandations concernant les garanties essentielles européennes.

L'exportateur devrait également procéder à cette évaluation avec toute la diligence requise et la documenter soigneusement. Les autorités de contrôle et/ou les autorités judiciaires compétentes de l'exportateur peuvent la demander et le tenir responsable de toute décision qu'il prendrait sur cette base.

Quatrièmement, il convient d'**identifier et d'adopter les mesures supplémentaires** nécessaires pour que le niveau de protection des données transférées soit porté au niveau de la norme européenne d'équivalence essentielle. Cette étape n'est nécessaire que si l'évaluation de l'exportateur révèle que la législation et/ou les pratiques du pays tiers portent atteinte à l'efficacité de l'instrument de transfert visé à l'article 46 du RGPD, auquel l'exportateur a recours ou auquel il entend recourir dans le cadre du transfert. Les présentes recommandations contiennent également (annexe 2) une liste non exhaustive d'exemples de mesures supplémentaires, assorties de certaines des conditions nécessaires à leur efficacité. Comme pour les garanties appropriées que contiennent les instruments de transfert visés à l'article 46 du RGPD, certaines mesures supplémentaires peuvent être efficaces dans certains pays, mais pas nécessairement dans d'autres. L'exportateur sera chargé d'en évaluer l'efficacité dans le cadre du transfert et à la lumière de la législation et des pratiques du pays tiers et de l'instrument

de transfert auquel il a recours, étant donné qu'il sera tenu responsable de la décision qu'il prendra sur cette base. Cela pourrait également lui imposer de combiner plusieurs mesures supplémentaires. En dernière analyse, il se peut qu'aucune mesure supplémentaire ne puisse garantir un niveau de protection essentiellement équivalent au transfert en question. Dans les cas où aucune mesure supplémentaire ne convient, l'exportateur doit éviter, suspendre ou mettre fin au transfert afin de ne pas compromettre le niveau de protection des données à caractère personnel. Il devrait également procéder à l'évaluation de ces mesures supplémentaires avec toute la diligence requise et la documenter.

Cinquièmement, l'exportateur doit **prendre** toutes les **mesures procédurales formelles** que la mesure supplémentaire pourrait exiger, en fonction de l'instrument de transfert visé à l'article 46 du RGPD auquel il a recours. Les présentes recommandations précisent certaines de ces formalités. Il pourrait être nécessaire de consulter les autorités de contrôle compétentes à l'égard de certaines d'entre elles.

La **sixième et dernière étape** consiste à **réévaluer** à intervalles appropriés le niveau de protection dont bénéficient les données à caractère personnel que l'exportateur transfère vers des pays tiers et à vérifier s'il y a eu ou s'il y aura des développements susceptibles de l'affecter. Le principe de responsabilité exige une surveillance permanente du niveau de protection des données à caractère personnel.

Les autorités de contrôle continueront d'exercer leur mission consistant à surveiller l'application du RGPD et à le faire respecter. Elles prendront dûment en considération les mesures prises par les exportateurs pour garantir que les données qu'ils transfèrent bénéficient d'un niveau de protection essentiellement équivalent. Comme le rappelle la Cour, les autorités de contrôle compétentes suspendront ou interdiront les transferts de données lorsqu'elles constatent qu'un niveau de protection essentiellement équivalent ne peut être garanti, à la suite d'une enquête ou d'une réclamation.

Les autorités de contrôle continueront d'élaborer des orientations à destination des exportateurs et de coordonner leurs actions au sein du comité européen de la protection des données afin de garantir la cohérence dans l'application de la législation de l'UE en matière de protection des données.

TABLE DES MATIÈRES

Le comité européen de la protection des données

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

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 Cour de justice de l'Union européenne (CJUE) conclut, dans son arrêt du 16 juillet 2020, *Data Protection Commissioner c/ Facebook Ireland LTD, Maximillian Schrems*, C-311/18, que l'article 46, paragraphe 1, et l'article 46, paragraphe 2, point d), du RGPD doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de recours effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne par ce règlement, lu à la lumière de la Charte des droits fondamentaux de l'Union européenne[2].

(2) Comme l'a souligné la Cour, un niveau de protection des personnes physiques substantiellement équivalent à celui garanti au sein de l'Union européenne par le RGPD, lu à la lumière de la Charte, doit être garanti indépendamment de la disposition du chapitre V sur le fondement de laquelle un transfert de données à caractère personnel vers un pays tiers est réalisé. Les dispositions du chapitre V visent à garantir la continuité de ce niveau de protection élevé lorsque les données à caractère personnel sont transférées vers un pays tiers[3].

(3) Le considérant 108 et l'article 46, paragraphe 1, du RGPD disposent qu'en l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Le responsable du traitement ou le sous-traitant peut fournir des garanties appropriées sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, en recourant à l'un des instruments de transfert visés à l'article 46, paragraphe 2, du RGPD, tels que les clauses types de protection des données.

(4) La Cour précise que les clauses types de protection des données adoptées par la Commission visent uniquement à fournir aux responsables du traitement et à leurs sous-traitants établis dans l'Union des

[1] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[2] Arrêt de la CJUE du 16 juillet 2020, Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems (C-311/18, ci-après l'»arrêt Schrems II»), deuxième conclusion.
[3] C-311/18 (Schrems II), points 92 et 93.

garanties contractuelles s'appliquant de manière uniforme dans tous les pays tiers. En raison de leur caractère contractuel, les clauses types de protection des données ne sauraient lier les autorités publiques des pays tiers, étant donné qu'elles ne sont pas parties au contrat. Par conséquent, les exportateurs de données peuvent être amenés à compléter les garanties contenues dans ces clauses types de protection des données par des garanties supplémentaires afin de garantir le respect du niveau de protection requis par le droit de l'Union dans un pays tiers donné. La Cour fait référence au considérant 109 du RGPD, qui mentionne cette possibilité et encourage les responsables du traitement et leurs sous-traitants à y recourir[4].

(5) La Cour a déclaré qu'il appartient avant tout à l'exportateur de données de vérifier, au cas par cas et, le cas échéant, en collaboration avec l'importateur de données, si le droit du pays tiers de destination garantit un niveau de protection essentiellement équivalent, 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[5].

(6) À défaut, pour le responsable du traitement ou son sous-traitant établi dans l'Union, de pouvoir prendre des mesures supplémentaires suffisantes pour garantir un niveau de protection essentiellement équivalent au regard du droit de l'Union, ceux-ci ou, à titre subsidiaire, l'autorité de contrôle compétente sont tenus de suspendre ou de mettre fin au transfert de données à caractère personnel vers le pays tiers concerné[6].

(7) Ni le RGPD ni la Cour ne définissent ou ne précisent les «garanties supplémentaires», les «mesures supplémentaires» ou les «mesures complémentaires» aux garanties offertes par les instruments de transfert visés à l'article 46, paragraphe 2, du RGPD que les responsables du traitement et les sous-traitants peuvent adopter pour garantir le respect du niveau de protection requis par le droit de l'Union dans un pays tiers donné.

(8) Le comité européen de la protection des données a décidé, de sa propre initiative, de se pencher sur cette question et de fournir aux responsables du traitement et aux sous-traitants, agissant en tant qu'exportateurs, des recommandations sur la procédure qu'ils pourraient suivre pour recenser et adopter des mesures complémentaires. Les présentes recommandations visent à fournir aux exportateurs une méthodologie afin de déterminer si des mesures supplémentaires devraient être mises en place pour leurs transferts et si oui, lesquelles. La responsabilité première des exportateurs consiste à veiller à ce que les données transférées bénéficient dans le pays tiers d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'EEE. Par les présentes recommandations, le comité européen de la protection des données souhaite encourager une application cohérente du RGPD et de l'arrêt de la Cour, conformément au mandat du comité[7].

A ADOPTÉ LES RECOMMANDATIONS SUIVANTES:

[4] C-311/18 (Schrems II), points 132 et 133.
[5] C-311/18 (Schrems II), point 134.
[6] C-311/18 (Schrems II), point 135.
[7] Article 70, paragraphe 1, point e), du RGPD.

1 RESPONSABILITÉ EN MATIÈRE DE TRANSFERTS DE DONNÉES

1. Le droit primaire de l'Union considère le droit à la protection des données à caractère personnel comme un droit fondamental[8]. Par conséquent, le droit à la protection des données à caractère personnel bénéficie d'un niveau de protection élevé et des limitations ne peuvent être apportées que si elles sont prévues par la loi, respectent le contenu essentiel du droit, sont proportionnées et 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[9]. Le droit à la protection des données à caractère personnel n'est pas un droit absolu, mais doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité[10].

2. Un niveau de protection essentiellement équivalent à celui garanti au sein de l'Union doit suivre les données lorsqu'elles sont transférées vers des pays tiers en dehors de l'EEE afin de s'assurer que le niveau de protection garanti par le RGPD ne soit pas compromis aussi bien pendant qu'après le transfert.

3. Le droit à la protection des données à caractère personnel est un droit actif. Il impose aux exportateurs et aux importateurs (qu'il s'agisse de responsables du traitement ou de sous-traitants) d'aller plus loin qu'une reconnaissance ou un respect passif de ce droit[11]. Les responsables du traitement et les sous-traitants doivent s'efforcer de respecter le droit à la protection de façon active et continue en mettant en œuvre des mesures d'ordre juridique, technique et organisationnel garantissant son efficacité. Ils doivent également être en mesure de démontrer ces efforts aux personnes concernées et aux autorités chargées du contrôle de la protection des données. C'est ce que l'on appelle le principe de responsabilité[12].

4. Le principe de responsabilité, qui est nécessaire pour garantir l'application effective du niveau de protection conféré par le RGPD, s'applique également aux transferts de données vers des pays tiers[13], étant donné qu'ils constituent par eux-mêmes une forme de traitement des données[14]. Comme la Cour l'a souligné dans son arrêt, un niveau de protection essentiellement équivalent à celui garanti au sein de l'Union par le RGPD, lu à la lumière de la Charte, doit être garanti, quelle que soit la disposition du chapitre V sur le fondement de laquelle est effectué un transfert de données à caractère personnel vers un pays tiers[15].

5. Dans l'arrêt Schrems II, la Cour souligne qu'il incombe aux exportateurs et aux importateurs de veiller à ce que le traitement de données à caractère personnel ait été et continue d'être réalisé dans le respect du niveau de protection déterminé par la législation de l'UE en matière de

[8] Article 8, paragraphe 1, de la Charte des droits fondamentaux et article 16, paragraphe 1, TFUE, premier considérant, article 1er, paragraphe 2, du RGPD.
[9] Article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne.
[10] Considérant 4 du RGPD et C-507/17, Google LLC, successeur en droit de Google Inc. c/ Commission nationale de l'informatique et des libertés (CNIL), point 60.
[11] C-92/09 et C-93/02, Volker und Markus Schecke GbR c/ Land Hessen, conclusions de l'avocat général Sharpston, 17 juin 2010, point 71.
[12] Article 5, paragraphe 2, et article 28, paragraphe 3, point h), du RGPD.
[13] Article 44 et considérant 101 du RGPD et article 47, paragraphe 2, point d), dudit règlement.
[14] CJUE, arrêt du 6 octobre 2015, *Maximillian Schrems c/ Data Protection Commissioner*, C-362/14 (ci-après «Schrems I»), point 45.
[15] C-311/18 (Schrems II), points 92 et 93.

protection des données et de suspendre le transfert et/ou de résilier le contrat lorsque l'importateur de données n'est pas, ou n'est plus en mesure, de respecter les clauses types de protection des données incluses dans le contrat liant l'exportateur et l'importateur[16]. Le responsable du traitement ou le sous-traitant agissant en tant qu'exportateur doit veiller à ce que l'importateur collabore avec l'exportateur, le cas échéant, dans l'exercice de ses responsabilités, en le tenant informé, par exemple, de toute évolution ayant une incidence sur le niveau de protection des données à caractère personnel reçues dans le pays de l'importateur[17]. Ces responsabilités sont une application du principe de responsabilité consacré par le RGPD aux transferts de données[18].

2 FEUILLE DE ROUTE: APPLICATION PRATIQUE DU PRINCIPE DE RESPONSABILITÉ AUX TRANSFERTS DE DONNÉES

6. L'exportateur de données trouvera ci-après une feuille de route des mesures à prendre pour savoir s'il doit mettre en place des mesures supplémentaires pour pouvoir transférer légalement des données en dehors de l'EEE. Dans le présent document, on entend par «exportateur de données»[19] le responsable du traitement ou le sous-traitant qui traite des données à caractère personnel relevant du champ d'application du RGPD, y compris le traitement par des entités privées ou des organismes publics lors du transfert de données à des organismes privés[20]. S'agissant des transferts de données à caractère personnel entre organismes publics, des orientations spécifiques sont énoncées dans les *Lignes directrices 2/2020 concernant l'article 46, paragraphe 2, point a), et l'article 46, paragraphe 3, point b), du règlement 2016/679 pour les transferts de données à caractère personnel entre autorités et organismes publics de l'EEE et de pays tiers*[21].

7. Cette évaluation et les mesures supplémentaires que l'exportateur choisit de mettre en œuvre devront être documentées et cette documentation devra être mise à la disposition de l'autorité de contrôle compétente sur demande[22].

[16] C-311/18 (Schrems II), points 134, 135, 139, 140, 141 et 142.
[17] C311/18 (Schrems II), point 134.
[18] Article 5, paragraphe 2, et article 28, paragraphe 3, point h), du RGPD.
[19] Par conséquent à titre d'exemple, l'exportateur ne sera pas considéré comme un exportateur de données s'il est une personne concernée qui fournit ses données à caractère personnel au moyen d'un questionnaire en ligne à un responsable du traitement établi dans un pays tiers.
[20] Voir Lignes directrices 3/2018 du comité européen de la protection des données relatives au champ d'application territorial du RGPD (article 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21] Lignes directrices 2/2020 du comité européen de la protection des données relatives à l'article 46, paragraphe 2, point a), et paragraphe 3, point b), du règlement (UE) 2016/679 pour les transferts de données à caractère personnel entre les autorités et organismes publics établis dans l'EEE et ceux établis hors de l'EEE; voir https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en
[22] Article 5, paragraphe 2, et article 24, paragraphe 1, du RGPD.

2.1 Étape 1: connaître les transferts

8. Pour savoir ce qui pourrait être exigé de l'exportateur de données pour pouvoir poursuivre ses transferts ou réaliser de nouveaux transferts de données à caractère personnel[23], la première chose à faire est de s'assurer qu'il a pleinement connaissance de ses transferts. L'enregistrement et la cartographie de tous les transferts peuvent être un exercice ardu pour des entités qui réalisent des transferts multiples, divers et réguliers avec des pays tiers et qui recourent à une série de sous-traitants et de sous-traitants ultérieurs. Connaître ses transferts est une première étape essentielle pour remplir les obligations qui incombent à l'exportateur de données en vertu du principe de responsabilité.

9. Pour être pleinement au fait de ses transferts, l'exportateur peut s'appuyer sur les registres des traitements qu'il peut être obligé de tenir en tant que responsable du traitement ou sous-traitant en vertu de l'article 30 du RGPD[24]. Les mesures préalables visant à remplir l'obligation d'informer les personnes concernées, en vertu de l'article 13, paragraphe 1, point f), et de l'article 14, paragraphe 1, point f), du RGPD, des transferts de leurs données à caractère personnel vers des pays tiers peuvent également aider les exportateurs[25].

10. Lors de la cartographie des transferts, il convient de ne pas oublier de tenir compte également des transferts ultérieurs, par exemple si des sous-traitants établis en dehors de l'EEE transfèrent les données à caractère personnel que l'exportateur leur a confiées à un sous-traitant ultérieur établi dans un autre pays tiers ou dans le même pays tiers[26].

11. Conformément au principe de «minimisation des données» consacré par le RGPD[27], l'exportateur doit vérifier si les données qu'il transfère sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

12. Ces activités doivent être réalisées avant tout transfert et être mises à jour avant la reprise des transferts à la suite d'une suspension des opérations de transfert de données: l'exportateur doit

[23] Il est à noter que l'accès à distance d'une entité d'un pays tiers à des données situées dans l'EEE est également considéré comme un transfert.

[24] Voir article 30 du RGPD et, en particulier, le paragraphe 1, point e), et le paragraphe 2, point c). En outre, les registres des traitements de l'exportateur devraient contenir une description de ses activités de traitement (y compris, mais sans s'y limiter, les catégories de personnes concernées, les catégories de données à caractère personnel et les finalités du traitement, ainsi que des informations spécifiques sur les transferts de données). Certains responsables du traitement et sous-traitants sont exemptés de l'obligation de tenir un registre des activités de traitement (article 30, paragraphe 5, du RGPD). Pour des orientations concernant cette exemption, voir Groupe de travail «Article 29», exposé de position sur les dérogations à l'obligation de tenir des registres des activités de traitement au titre de l'article 30, paragraphe 5, du RGPD (approuvé par le comité européen de la protection des données le 25 mai 2018).

[25] En vertu des règles de transparence du RGPD, l'exportateur doit informer les personnes concernées des transferts de données les concernant vers des pays tiers [article 13, paragraphe 1, point f), et article 14, paragraphe 1, point f) du RGPD]. En particulier, il doit les informer de l'existence ou de l'absence d'une décision d'adéquation de la Commission européenne, ou dans le cas des transferts visés aux articles 46 ou 47 du RGPD, ou à l'article 49, paragraphe 1, second alinéa, dudit règlement, il doit faire référence aux garanties appropriées ou adéquates et aux moyens d'en obtenir une copie ou à l'endroit où on peut les trouver. Les informations fournies à la personne concernée doivent être exactes et actuelles, notamment à la lumière de la jurisprudence de la Cour en matière de transferts.

[26] Lorsque le responsable du traitement a donné son autorisation écrite préalable, spécifique ou générale, conformément à l'article 28, paragraphe 2, du RGPD.

[27] Article 5, paragraphe 1, point c), du RGPD.

savoir où les données à caractère personnel qu'il a exportées peuvent être localisées ou traitées par les importateurs (carte des destinations).

13. Il y a lieu de garder à l'esprit que l'accès à distance depuis un pays tiers (par exemple, dans des situations de soutien) et/ou le stockage dans un nuage situé hors de l'EEE proposé par un prestataire de services, doit également être considéré comme un transfert[28]. Plus précisément, si l'exportateur utilise une infrastructure internationale en nuage, il doit déterminer si ses données seront transférées vers des pays tiers et la destination dudit transfert, à moins que le fournisseur de services informatiques en nuage ne soit établi dans l'EEE et n'indique clairement dans son contrat que les données ne seront pas du tout traitées dans des pays tiers.

2.2 Étape 2: recenser les instruments de transfert utilisés

14. La deuxième étape consiste à recenser les instruments de transfert auxquels l'exportateur a recours parmi ceux énumérés et envisagés au chapitre V du RGPD.

Décisions d'adéquation

15. Par ses **décisions d'adéquation** relatives à certains ou à l'ensemble des pays tiers vers lesquels l'exportateur transfère des données à caractère personnel, la Commission européenne peut reconnaître qu'ils offrent un niveau de protection adéquat à ces données[29].

16. Une telle décision d'adéquation a pour effet d'autoriser les flux de données à caractère personnel au départ de l'EEE vers le pays tiers en question, sans qu'il soit nécessaire de recourir à un instrument de transfert au titre de l'article 46 du RGPD.

17. Les décisions d'adéquation peuvent concerner un pays dans son ensemble ou être limitées à une partie de celui-ci. Elles peuvent couvrir tous les transferts de données vers un pays ou être limitées à certains types de transfert (par exemple dans un seul secteur)[30].

18. La Commission européenne publie la liste de ses décisions d'adéquation sur son site internet[31].

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**

[28] Voir FAQ nº 11: «il convient de rappeler que même le fait d'autoriser un pays tiers à accéder aux données, par exemple à des fins administratives, équivaut également à un transfert», comité européen de la protection des données, Foire aux questions sur l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire C-311/18 – Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems, 23 juillet 2020.
[29] La Commission européenne est compétente pour déterminer, sur le fondement de l'article 45 du RGPD, si un pays tiers de l'UE offre un niveau adéquat de protection des données. La Commission européenne est également compétente pour décider qu'une organisation internationale offre un niveau de protection adéquat.
[30] Article 45, paragraphe 1, du RGPD.
[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

recommandations[32]. Il doit toutefois toujours vérifier si les décisions d'adéquation concernant ses transferts ont été révoquées ou invalidées[33].

20. Toutefois, une décision d'adéquation n'empêche pas les personnes concernées d'introduire une réclamation. Pas plus qu'elle n'empêche les autorités de contrôle de saisir une juridiction nationale si elles ont des doutes quant à la validité de la décision, de sorte qu'une juridiction nationale peut procéder à un renvoi préjudiciel devant la CJUE aux fins de l'examen de cette validité[34].

Exemple:

Un citoyen de l'Union, M. Schrems, a introduit une réclamation en juin 2013 auprès de la Data Protection Commission (DPC) irlandaise et a demandé à cette autorité de contrôle d'interdire ou de suspendre le transfert de ses données à caractère personnel détenues par Facebook Ireland vers les États-Unis, car il estimait que le droit et la pratique des États-Unis ne garantissaient pas une protection adéquate des données à caractère personnel détenues sur leur territoire contre les activités de surveillance qui y étaient menées par les autorités publiques. Le DPC a rejeté la plainte au motif, notamment, que dans la décision 2000/520, la Commission européenne a considéré que, dans le cadre du régime de la «sphère de sécurité», les États-Unis assuraient un niveau de protection adéquat des données à caractère personnel transférées (la décision «sphère de sécurité»). M. Schrems a contesté la décision de la DPC et la Haute Cour d'Irlande a saisi la Cour de justice de l'Union européenne (CJUE) d'une question préjudicielle portant sur la validité de la décision 2000/520. La CJUE a ensuite décidé d'invalider la décision 2000/520 de la Commission relative à l'adéquation de la protection conférée par les principes de la sphère de sécurité[35].

Instruments de transfert visés à l'article 46 du RGPD

21. L'article 46 du RGPD énumère une série d'instruments de transfert contenant des «*garanties appropriées»* auxquels les exportateurs peuvent recourir pour transférer des données à caractère personnel vers des pays tiers en l'absence de décisions d'adéquation. Les principaux types d'instrument de transfert prévus à l'article 46 du RGPD sont les suivants:

[32] Pour autant que l'exportateur et l'importateur de données aient mis en œuvre des mesures pour se conformer aux autres obligations prévues par le RGPD; à défaut, ces mesures doivent être mises en œuvre.

[33] La Commission européenne doit réexaminer régulièrement toutes les décisions d'adéquation et contrôler si les pays tiers bénéficiant de ces décisions continuent de garantir un niveau de protection adéquat (voir article 45, paragraphes 3 et 4, du RGPD). La CJUE peut également invalider des décisions d'adéquation [voir ses arrêts dans les affaires C-362/14 (Schrems I) et C-311/18 (Schrems II)].

[34] C-311/18 (Schrems II), points 118-120. Les autorités de contrôle ne peuvent pas ignorer la décision d'adéquation et suspendre ou interdire des transferts de données à caractère personnel vers ces pays en invoquant uniquement un niveau de protection inadéquat. Elles ne peuvent exercer leur pouvoir de suspendre ou interdire des transferts de données à caractère personnel que pour d'autres motifs (insuffisance des mesures de sécurité en violation de l'article 32 du RGPD, absence de base juridique pour le traitement proprement dit en violation de l'article 6 du RGPD, par exemple). Les autorités de contrôle peuvent examiner, en toute indépendance, si le transfert de ces données respecte les exigences posées par le RGPD et, le cas échéant, introduire un recours devant les juridictions nationales afin que ces dernières procèdent, si elles ont des doutes quant à la validité de la décision d'adéquation de la Commission, à un renvoi préjudiciel devant la Cour de justice de l'Union européenne aux fins de l'examen de cette validité.

[35] Affaire C-362/14 (Schrems I).

- les clauses types de protection des données (CCT);
- les règles d'entreprise contraignantes;
- les codes de conduite;
- les mécanismes de certification et
- les clauses contractuelles ad hoc.

22. Quel que soit l'instrument de transfert visé à l'article 46 du RGPD que choisit l'exportateur, il doit s'assurer que, dans l'ensemble, les données à caractère personnel transférées bénéficieront d'un niveau de protection essentiellement équivalent.

23. Les instruments de transfert visés à l'article 46 du RGPD contiennent principalement des garanties appropriées à caractère contractuel qui peuvent s'appliquer aux transferts vers tous les pays tiers. La situation prévalant dans le pays tiers vers lequel l'exportateur transfère des données peut toujours nécessiter qu'il complète ces instruments et les garanties qu'ils contiennent par des mesures additionnelles (les «mesures supplémentaires») afin d'assurer un niveau de protection essentiellement équivalent[36].

Dérogations

24. Outre les décisions d'adéquation et les instruments de transfert visés à l'article 46 du RGPD, le RGPD prévoit une troisième voie permettant le transfert de données à caractère personnel dans certaines situations. Sous réserve du respect de conditions particulières, l'exportateur pourra toujours être en mesure de transférer des données à caractère personnel sur la base d'une des dérogations prévues à l'article 49 du RGPD.

25. L'article 49 du RGPD a un caractère exceptionnel. Les dérogations qu'il contient doivent être interprétées de manière à ne pas contredire la nature même des dérogations, à savoir des exceptions à la règle selon laquelle les données à caractère personnel ne peuvent être transférées vers un pays tiers que si ce pays prévoit un niveau adéquat de protection des données ou, à défaut, si des garanties appropriées sont mises en place. Les dérogations ne peuvent pas devenir «la règle» dans la pratique, mais doivent être limitées à des situations particulières. Le comité européen de la protection des données a publié ses lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679. [37]

26. Avant d'invoquer une dérogation au titre de l'article 49 du RGPD, l'exportateur doit d'abord vérifier que son transfert respecte les conditions strictes énoncées par cette disposition pour chacune des dérogations prévues.

***

27. Si le transfert ne peut être légalement fondé ni sur une décision d'adéquation ni sur une dérogation au titre de l'article 49, il convient de passer à l'étape 3.

[36] C-311/18 (Schrems II), points 130 et 133. Voir également le point 2.3 ci-dessous.
[37] Pour de plus amples informations à ce sujet, voir: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

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

28. L'instrument de transfert visé à l'article 46 du RGPD que l'exportateur a choisi doit assurer que le niveau de protection garanti par le RGPD n'est pas compromis par le transfert dans la pratique[38].

29. En particulier, la protection accordée aux données à caractère personnel transférées vers le pays tiers doit être essentiellement équivalente à celle garantie dans l'EEE par le RGPD, lu à la lumière de la Charte des droits fondamentaux de l'UE[39]. Tel n'est pas le cas si l'importateur de données n'est pas en mesure de se conformer aux obligations qui lui incombent en vertu de l'instrument de transfert visé à l'article 46 du RGPD qu'il a choisi en raison du droit du pays tiers et des pratiques applicables au transfert, y compris pendant le transit des données du pays de l'exportateur à celui de l'importateur[40].

30. Tout d'abord, l'exportateur doit évaluer, le cas échéant en collaboration avec l'importateur, s'il existe dans le droit et/ou les pratiques en vigueur[41] du pays tiers des éléments susceptibles de porter atteinte à l'efficacité des garanties appropriées qu'offre l'instrument de transfert visé à l'article 46 du RGPD auquel l'exportateur a recours dans le cadre du transfert particulier. Cela implique de déterminer si le transfert relève du champ d'application du droit et/ou de pratiques susceptibles de porter atteinte à l'efficacité de l'instrument de transfert visé à l'article 46 du RGPD. L'évaluation requise doit d'abord et avant tout se fonder sur la législation accessible au public.

31. Cette évaluation doit contenir des éléments concernant l'accès aux données par les autorités publiques du pays tiers de l'importateur, tels que:

    - des éléments permettant de déterminer si les autorités publiques du pays tiers de l'importateur peuvent chercher à accéder aux données, à l'insu ou non de l'importateur des données, compte tenu de la législation, de la pratique et des précédents signalés;
    - des éléments permettant de déterminer si les autorités publiques du pays tiers de l'importateur peuvent avoir accès aux données par l'intermédiaire de l'importateur, des fournisseurs de services de télécommunication ou de canaux d'information, compte tenu de la législation, des compétences légales, des ressources techniques, financières et humaines dont elles disposent et des précédents signalés.

Identification des législations et des pratiques pertinentes compte tenu de l'ensemble des circonstances du transfert

32. L'exportateur devra analyser les caractéristiques de chaque transfert et déterminer si l'ordre juridique interne et/ou les pratiques en vigueur du pays vers lequel les données sont transférées (ou sont transférées ultérieurement) ont une incidence sur ses transferts. La portée de l'évaluation se limite donc à la législation et aux pratiques pertinentes pour la protection des données spécifiques que l'exportateur transfère, à la différence des évaluations d'adéquation

[38] Article 44 du RGPD et points 126, 137 et 148 de l'arrêt dans l'affaire C-311/18 (Schrems II).
[39] C-311/18 (Schrems II), point 105 et deuxième conclusion.
[40] Voir C-311/18 (Schrems II), point 183 lu en combinaison avec le point 184.
[41] Voir point 126 de l'arrêt C-311/18 (Schrems II), où la Cour fait explicitement référence au «droit et [aux] pratiques en vigueur dans le pays tiers concerné» et impose «d'assurer, en pratique, la protection effective des données à caractère personnel transférées dans le pays tiers concerné» (soulignement ajouté) et point 158.

générales et à large portée que réalise la Commission européenne en application de l'article 45 du RGPD.

33. Le cadre juridique applicable et/ou les pratiques en vigueur dépendront des circonstances spécifiques du transfert et notamment:

- les finalités pour lesquelles les données sont transférées et traitées (commercialisation, ressources humaines, stockage, support informatique, essais cliniques, par exemple);
- les types d'entités intervenant dans le traitement (publiques ou privées; responsable du traitement ou sous-traitant);
- le secteur dans lequel le transfert a lieu (technologies publicitaires, télécommunications, finances, etc.);
- les catégories de données à caractère personnel transférées (des données à caractère personnel concernant des enfants peuvent relever du champ d'application d'une législation spécifique du pays tiers, par exemple)[42];
- le fait que les données seront stockées dans le pays tiers ou qu'il existe un accès à distance aux données stockées dans l'UE/EEE;
- le format des données à transférer (c'est-à-dire en texte clair/pseudonymisées ou chiffrées[43]);
- la possibilité que les données puissent faire l'objet de transferts ultérieurs depuis le pays tiers vers un autre pays tiers[44].

34. L'évaluation de l'exportateur devrait prendre en considération tous les acteurs intervenant dans le transfert (à savoir les responsables du traitement, les sous-traitants et les sous-traitants ultérieurs qui traitent les données dans le pays tiers), qui ont été identifiés dans le cadre de l'exercice de cartographie des transferts. Plus le nombre de responsables du traitement, de sous-traitants ou d'importateurs intervenant dans le transfert est élevé, plus l'évaluation de l'exportateur sera complexe. Il devra également intégrer dans cette évaluation les transferts ultérieurs qui sont envisagés.

35. En tout état de cause, il devrait accorder une attention particulière à toute législation pertinente, en particulier aux lois imposant des conditions à la divulgation de données à caractère personnel aux autorités publiques ou accordant à ces autorités des pouvoirs d'accès à des données à caractère personnel (par exemple, à des fins d'application du droit pénal, de contrôle réglementaire ou de sécurité nationale). Si ces exigences ou pouvoirs restreignent les droits fondamentaux des personnes concernées tout en respectant leur substance et en étant des

[42] Un transfert de données à caractère personnel est une opération de traitement (article 4, paragraphe 2, du RGPD). Si l'exportateur souhaite transférer des données sensibles relevant des articles 9 et 10 du RGPD, il ne peut effectuer le transfert que s'il est couvert par l'une des dérogations et conditions énoncées aux articles 9 et 10 du RGPD et dans la législation des États membres de l'Union. Conformément à l'article 32 du RGPD, l'importateur agissant en qualité de responsable du traitement ou de sous-traitant, l'exportateur devra également mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques que représente pour les droits et libertés des personnes concernées une violation potentielle des données à caractère personnel transférées (article 4, paragraphe 12, du RGPD). Les catégories de données transférées et leur sensibilité sont pertinents aux fins de l'évaluation du risque et du caractère approprié des mesures.

[43] Certains pays tiers n'autorisent pas l'importation de données chiffrées.

[44] Lorsque le responsable du traitement a donné son autorisation écrite préalable, spécifique ou générale, conformément à l'article 28, paragraphe 2, du RGPD.

mesures nécessaires et proportionnées dans une société démocratique pour préserver des objectifs importants, également reconnus dans le droit de l'Union ou de ses États membres[45], ils ne peuvent porter atteinte aux engagements contenus dans l'instrument de transfert visé à l'article 46 du RGPD auquel l'exportateur a recours.

36. L'exportateur devra évaluer les règles et pratiques pertinentes à caractère général dans la mesure où elles ont une incidence sur l'application effective des garanties contenues dans l'instrument de transfert visé à l'article 46 du RGPD.

37. Lors de cette évaluation, différents aspects du système juridique du pays tiers concerné, comme les éléments énumérés à l'article 45, paragraphe 2, du RGPD, sont également pertinents. À titre d'exemple, la situation de l'état de droit dans un pays tiers peut être pertinente pour apprécier l'efficacité des mécanismes mis à la disposition des personnes physiques pour introduire un recours (juridictionnel) contre l'accès illicite du gouvernement à des données à caractère personnel. L'existence d'une législation complète en matière de protection des données ou d'une autorité indépendante chargée de la protection des données, ainsi que l'adhésion à des instruments internationaux prévoyant des garanties en la matière peuvent contribuer à assurer la proportionnalité de l'ingérence du gouvernement.

38. Les obligations ou les pouvoirs découlant de ces législations et pratiques seront considérés comme portant atteinte ou étant incompatibles avec les engagements de l'instrument de transfert visé à l'article 46 du RGPD dans les cas suivants[46]:

- s'ils ne respectent pas la substance des droits et libertés fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne; ou

- s'ils vont au-delà de ce qui est nécessaire et proportionné dans une société démocratique pour préserver l'un des objectifs importants également reconnus par le droit de l'Union ou des États membres, tels que ceux énumérés à l'article 23, paragraphe 1, du RGPD.

39. L'exportateur doit vérifier si les engagements de l'importateur des données permettant aux personnes concernées d'exercer les droits tels qu'ils sont prévus dans l'instrument de transfert visé à l'article 46 du RGPD [tels que les demandes d'accès, de rectification et d'effacement de données transférées, et un droit de recours (juridictionnel)] peuvent être effectivement appliqués en pratique et ne sont pas entravés par le droit et/ou les pratiques du pays tiers de destination.

40. Les normes de l'Union, comme les articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, doivent servir de référence, notamment pour déterminer si l'accès des autorités publiques est limité à ce qui est nécessaire et proportionné dans une société démocratique et si les personnes concernées disposent d'un droit de recours effectif.

[45] Voir articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, article 23, paragraphe 1, du RGPD et recommandations 2/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[46] Voir articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, article 23, paragraphe 1, du RGPD, C-311/18 (Schrems II), points 174 et 187, et recommandations 2/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020.

41. Les recommandations du comité européen de la protection des données sur les garanties essentielles européennes[47] contiennent des éclaircissements sur les éléments qui doivent être évalués afin de déterminer si le cadre juridique régissant l'accès des autorités publiques à des données à caractère personnel dans un pays tiers, qu'il s'agisse d'agences chargées de la sécurité nationale ou d'autorités répressives, peut être ou non considéré comme une ingérence justifiable[48]. Celles-ci devraient être soigneusement prises en considération lorsque la législation régissant l'accès des autorités publiques aux données est ambiguë ou n'est pas accessible au public. La première exigence des garanties essentielles européennes est qu'il existe un cadre juridique prévoyant un tel accès, lorsqu'il est envisagé, qui soit accessible au public et suffisamment clair.

42. Appliquées aux transferts de données fondés sur des instruments de transfert visés à l'article 46, les recommandations du comité européen de la protection des données sur les garanties essentielles peuvent aider l'exportateur de données à évaluer si ces pouvoirs interfèrent de manière injustifiée avec les obligations faites à l'exportateur et à l'importateur de données de garantir un niveau de protection essentiellement équivalent conformément au RGPD ou avec les engagements contenus dans l'instrument de transfert. L'absence d'un niveau de protection essentiellement équivalent sera particulièrement manifeste lorsque le droit et/ou les pratiques du pays tiers concerné par le transfert ne répondent pas aux exigences des garanties essentielles européennes. Le comité européen de la protection des données rappelle que les garanties essentielles européennes constituent une norme de référence aux fins de l'évaluation de l'ingérence résultant des mesures de surveillance d'un pays tiers dans le cadre des transferts internationaux de données. Ces normes découlent du droit de l'Union et de la jurisprudence de la CJUE et de la CouEDH, qui est contraignante pour les États membres de l'Union.

43. L'évaluation de l'exportateur doit d'abord et avant tout se fonder sur la législation accessible au public. L'examen des pratiques des autorités publiques du pays tiers permettra également à l'exportateur de vérifier si les garanties contenues dans l'instrument de transfert visé à l'article 46 du RGPD peuvent constituer un moyen suffisant d'assurer, en pratique, la protection effective des données à caractère personnel transférées[49]. L'examen des pratiques en vigueur dans le pays tiers sera particulièrement important aux fins de l'évaluation des cas décrits ci-dessous.

43.1 **La législation pertinente du pays tiers peut satisfaire formellement les normes de l'UE en matière de droits et libertés fondamentaux ainsi que de nécessité et de proportionnalité des restrictions à ces droits et libertés.** Toutefois, les pratiques des autorités publiques (par exemple, l'accès à des données à caractère personnel détenues par le secteur privé ou dans le cadre de l'application – ou non – de la législation en tant qu'organes de contrôle ou judiciaires) peuvent clairement indiquer qu'elles ne s'appliquent ou ne respectent normalement pas la législation qui régit, en principe, leurs activités. Dans ce cas, l'exportateur doit tenir compte de ces pratiques dans son évaluation et considérer que l'instrument prévu à l'article 46 du RGPD ne sera pas en mesure de garantir effectivement, en soi (c'est-à-dire sans mesures supplémentaires), un niveau de protection essentiellement équivalent. En pareil cas, si

[47] Recommandations 02/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020.

[48] Et, par conséquent, comme ne portant pas atteinte aux engagements prévus dans l'instrument de transfert au titre de l'article 46 du RGPD.

[49] C-311/18 (Schrems II), point 126.

l'exportateur souhaite procéder au transfert, il devra mettre en œuvre des mesures supplémentaires adéquates.

43.2 **La législation pertinente du pays tiers (par exemple sur l'accès aux données à caractère personnel détenues par le secteur privé) peut faire défaut.** Dans ce cas, l'exportateur ne peut pas automatiquement déduire de cette absence de législation pertinente que l'instrument de transfert visé à l'article 46 du RGPD peut être effectivement appliqué. Il devra vérifier s'il existe des indices de pratiques en vigueur dans le pays qui sont incompatibles avec le droit de l'Union et les engagements contenus dans l'instrument de transfert visé à l'article 46 du RGPD. S'il existe des pratiques incompatibles, l'instrument de transfert visé à l'article 46 du RGPD ne sera pas en mesure de garantir effectivement, en soi (c'est-à-dire sans mesures supplémentaires adéquates), un niveau de protection essentiellement équivalent. En pareil cas, si l'exportateur souhaite procéder au transfert, il devra mettre en œuvre des mesures supplémentaires adéquates.

43.3 **L'évaluation peut révéler que la législation pertinente du pays tiers peut être problématique[50] et que les données transférées et/ou l'importateur en cause relèvent ou pourraient relever du champ d'application de cette législation problématique[51].**

Compte tenu des incertitudes entourant l'application potentielle d'une législation problématique au transfert, l'exportateur peut décider:

- de suspendre le transfert;
- de mettre en œuvre des mesures supplémentaires[52] afin d'éviter le risque d'application potentielle à l'importateur et/ou aux données transférées de législations et/ou de pratiques du pays tiers de l'importateur de données, qui sont susceptibles de porter atteinte aux garanties contractuelles contenues dans l'instrument de transfert d'assurer un niveau de protection essentiellement équivalent à celui garanti dans l'EEE; ou
- à titre subsidiaire, l'exportateur peut décider de procéder au transfert sans être tenu de mettre en œuvre des mesures supplémentaires s'il considère qu'il n'y a pas lieu de croire qu'une législation pertinente et problématique sera appliquée, en pratique, aux données transférées et/ou à l'importateur. L'exportateur devra démontrer et documenter son évaluation, le cas échéant en collaboration avec l'importateur, selon laquelle l'interprétation et/ou l'application de la législation pratique ne couvre pas les données transférées et l'importateur, compte tenu également de l'expérience d'autres acteurs

[50] On entend par «législation problématique» une législation qui: 1) impose des obligations au destinataire de données à caractère personnel provenant de l'Union européenne et/ou affecte les données transférées d'une manière susceptible de porter atteinte à la garantie contractuelle d'un niveau de protection essentiellement équivalent contenue dans les instruments de transfert; et 2) ne respecte pas la substance des droits et libertés fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne ou va au-delà de ce qui est nécessaire et proportionné dans une société démocratique pour préserver l'un des objectifs importants également reconnus dans le droit de l'Union ou de ses États membres, tels que ceux énumérés à l'article 23, paragraphe 1, du RGPD.

[51] Il peut être difficile de déterminer si l'importateur et/ou les données transférées relèvent de la portée des termes généraux souvent utilisés dans la législation relative à la sécurité nationale pour limiter leur champ d'application, tels que, par exemple, «fournisseur de services de communications électroniques» et «informations de renseignement étranger».

[52] Voir considérant 109 du RGPD et C-311/18 (Schrems II), point 132.

opérant dans le même secteur et/ou dans des secteurs liés à des données personnelles transférées similaires et d'autres sources d'information décrites ci-dessous[53].

L'exportateur devra donc avoir démontré et documenté dans un rapport détaillé[54] que la législation problématique ne sera pas appliquée en pratique aux données transférées et/ou à l'importateur et, partant, qu'elle n'empêchera pas l'importateur de remplir les obligations qui lui incombent en vertu de l'instrument de transfert visé à l'article 46 du RGPD[55].

Sources d'information possibles

44. L'importateur de données devrait fournir à l'exportateur les sources et informations pertinentes concernant le pays tiers dans lequel il est établi, ainsi que la législation et les pratiques en vigueur qui sont applicables au transfert.

45. L'exportateur et son importateur peuvent compléter l'évaluation par des informations obtenues auprès de sources telles que celles énumérées à titre d'exemples à l'annexe 3.

46. Outre le cadre juridique du pays tiers applicable au transfert, les sources et les informations devraient être pertinentes, objectives, fiables, vérifiables et accessibles au public ou être accessibles d'une autre manière, afin de déterminer si l'instrument de transfert visé à l'article 46 peut être effectivement appliqué[56] et l'exportateur devra évaluer et documenter qu'elles le sont.

[53] Voir paragraphes 44 à 46.

[54] Les rapports établis par l'exportateur devront inclure des informations complètes sur l'évaluation juridique de la législation et des pratiques ainsi que de leur application aux transferts spécifiques, la procédure interne menant à l'évaluation (y compris des informations sur les acteurs intervenant dans l'évaluation, par exemple des cabinets juridiques, des consultants ou des services internes) et les dates des contrôles. Les rapports devraient être approuvés par le représentant légal de l'exportateur.

[55] Démontrer qu'une législation problématique ne s'applique pas en pratique aux données transférées et à l'importateur, en tenant compte également de l'expérience d'autres acteurs opérant dans le même secteur et/ou dans des secteurs liés à des données personnelles transférées similaires, n'exempte pas l'exportateur de prévoir les mesures supplémentaires nécessaires pour protéger les données à caractère personnel pendant leur transmission et leur traitement dans le pays tiers de destination (par exemple, chiffrement de bout en bout des données – voir les exemples de mesures techniques supplémentaires à l'annexe 2), si son analyse de la législation applicable du pays tiers de destination indique que l'accès aux données est possible, même en l'absence d'une intervention de l'importateur, à ce moment du transfert. L'exportateur doit également prévoir ces mesures avec l'importateur agissant en qualité de responsable du traitement ou de sous-traitant, conformément à l'article 32 du RGPD.

[56] Voir l'annexe 3 pour une liste non exhaustive des sources d'information que l'exportateur et l'importateur peuvent utiliser.

Informations pertinentes: les informations doivent être pertinentes pour le transfert spécifique et/ou l'importateur et pour leur conformité avec les exigences énoncées dans le droit de l'Union et avec l'instrument de transfert visé à l'article 46 du RGPD, et ne pas être trop générales ou abstraites.

Informations objectives: les informations doivent être étayées par des données empiriques fondées sur les connaissances acquises et non sur des hypothèses concernant des événements et des risques potentiels.

Informations fiables: l'exportateur et l'importateur doivent évaluer objectivement la fiabilité de la source d'information et les informations proprement dites et les évaluer séparément.

Informations vérifiables: les informations et les conclusions devraient être vérifiables ou comparables à d'autres types ou sources d'information, dans le cadre d'une évaluation globale, afin de permettre également à l'autorité de contrôle ou à l'autorité judiciaire compétente de vérifier l'objectivité et la fiabilité de ces informations, si nécessaire.

Informations accessibles au public ou accessibles d'une autre manière: les informations devraient, de préférence, être publiques ou à tout le moins accessibles afin de faciliter la vérification des critères susvisés et de permettre leur éventuel partage avec les autorités de contrôle, les autorités judiciaires et, enfin, les personnes concernées.

47. L'exportateur peut également prendre en considération l'expérience pratique documentée de l'importateur en ce qui concerne les demandes précédentes pertinentes d'accès provenant des autorités publiques du pays tiers. L'exportateur ne sera en mesure d'utiliser l'expérience de l'importateur comme source supplémentaire d'informations que si le cadre juridique du pays tiers n'interdit pas à l'importateur de fournir des informations sur les demandes de divulgation émanant des autorités publiques ou sur l'absence de telles demandes (et l'exportateur devrait également documenter cette évaluation). Il convient toutefois de noter que l'absence de demandes antérieures adressées à l'importateur ne peut jamais être considérée, à elle seule, comme un facteur déterminant de l'efficacité de l'instrument de transfert visé à l'article 46 du RGPD permettant de procéder au transfert sans mesures supplémentaires. L'exportateur pourra prendre ces informations en considération, ainsi que d'autres types d'informations provenant d'autres sources, dans le cadre de son évaluation globale de la législation et des pratiques du pays tiers par rapport à son transfert. L'expérience pertinente et démontrée de l'importateur devrait être corroborée et non contredite par des informations pertinentes, objectives, fiables, vérifiables et accessibles au public ou accessibles d'une autre manière sur l'application pratique de la législation pertinente (par exemple, l'existence ou l'absence de demandes d'accès reçues par d'autres acteurs opérant dans le même secteur et/ou liées à des données personnelles transférées similaires[57] et/ou l'application pratique de la législation, telle que la jurisprudence et les rapports d'organes de contrôle indépendants).

[57] L'expérience pourrait être celle d'autres entités que l'exportateur connaît personnellement du fait de transferts antérieurs du même type que celui qu'il met en place, ou celle mentionnée dans la jurisprudence pertinente, dans des rapports d'ONG, etc. (voir annexe 3).

Résultats de l'évaluation de l'exportateur

48. L'exportateur devrait procéder à cette évaluation globale de la législation et des pratiques du pays tiers de l'importateur qui s'appliquent au transfert avec toute la diligence requise et la documenter soigneusement. Les autorités de contrôle et/ou les autorités judiciaires compétentes de l'exportateur peuvent la demander et le tenir responsable de toutes les décisions qu'il prendrait sur cette base[58].

49. Enfin, l'évaluation de l'exportateur peut révéler que l'instrument de transfert prévu à l'article 46 du RGPD auquel il a recours:

    - garantit effectivement que les données à caractère personnel transférées bénéficient dans le pays tiers d'un niveau de protection essentiellement équivalent à celui qui est garanti dans l'EEE. Le droit et les pratiques du pays tiers applicables au transfert permettent à l'importateur de données de se conformer aux obligations qui lui incombent en vertu de l'instrument de transfert choisi. L'exportateur devrait réévaluer la situation à intervalles appropriés ou lorsque des changements significatifs interviennent (voir étape 6); ou

    - ne garantit pas effectivement un niveau de protection essentiellement équivalent. L'importateur de données ne peut pas se conformer à ses obligations étant donné que la législation et/ou les pratiques du pays tiers applicables au transfert ne répondent pas aux normes de l'UE en matière de droits et libertés fondamentaux et de nécessité et de proportionnalité des restrictions à ceux-ci pour préserver des objectifs légitimes d'intérêt public. La CJUE a souligné que, lorsque les instruments de transfert prévus à l'article 46 du RGPD sont insuffisants, il incombe à l'exportateur de données de mettre en place des mesures supplémentaires efficaces ou de ne pas transférer de données à caractère personnel[59].

Exemple:

Contexte:
La CJUE a estimé que l'article 702 de la loi américaine sur la surveillance et le renseignement étranger (FISA) ne respecte pas les garanties minimales découlant du principe de proportionnalité en vertu du droit de l'Union et ne saurait être considéré comme étant limité à ce qui est strictement nécessaire. En d'autres termes, le niveau de protection des programmes autorisés par l'article 702 de la FISA n'est pas substantiellement équivalent aux garanties exigées par le droit de l'Union.

Évaluation:
Si l'évaluation de la législation américaine pertinente conduit l'exportateur à considérer que son transfert pourrait relever du champ d'application de l'article 702 de la FISA, mais qu'il n'est pas certain qu'il relève de son champ d'application pratique, il peut décider soit:

1. d'arrêter le transfert;
2. d'adopter des mesures supplémentaires appropriées qui garantissent effectivement un niveau de protection des données transférées essentiellement équivalent à celui garanti dans l'EEE; soit
3. d'examiner d'autres informations objectives, fiables, pertinentes, vérifiables et de préférence accessibles au public (lesquelles peuvent inclure des informations fournies à l'exportateur par

[58] Article 5, paragraphe 2, du RGPD.
[59] CJUE, C-311/18 (Schrems II), points 134 et 135.

l'importateur de données) afin de préciser le champ d'application pratique de l'article 702 de la FISA pour le transfert concerné. Ces informations devraient apporter des réponses à certaines questions pertinentes, telles que:

- les informations accessibles au public indiquent-elles qu'il existe une interdiction légale de fournir des informations sur une demande spécifique d'accès aux données reçues et des restrictions larges à la fourniture d'informations générales sur les demandes d'accès aux données reçues ou sur l'absence de demandes reçues?

- l'importateur de données a-t-il confirmé avoir reçu des demandes d'accès à des données émanant des autorités publiques américaines dans le passé? Ou l'importateur de données a-t-il confirmé qu'il n'a pas reçu de demandes d'accès à des données émanant des autorités publiques américaines dans le passé et qu'il n'est pas interdit de fournir des informations sur ces demandes ou sur leur absence?

- les informations accessibles au public que l'exportateur a obtenues sur la jurisprudence américaine et les rapports d'organes de contrôle, d'organisations de la société civile et d'établissements universitaires[60] révèlent-elles que des importateurs de données du même secteur que l'importateur ont reçu des demandes d'accès à des données transférées similaires dans le passé?

Les réponses à ces questions obtenues grâce à l'évaluation globale de l'exportateur le conduisent à conclure ce qui suit:

- l'article 702 de la FISA s'applique en pratique au transfert en cause et porte donc atteinte à l'efficacité de l'instrument de transfert prévu à l'article 46 du RGPD. Par conséquent, si l'exportateur souhaite procéder au transfert, il doit déterminer, le cas échéant en collaboration avec l'importateur, s'il peut adopter des mesures supplémentaires qui garantissent effectivement un niveau de protection des données transférées essentiellement équivalent à celui garanti dans l'EEE. Si l'exportateur ne trouve pas de mesures supplémentaires efficaces, il ne doit pas transférer les données à caractère personnel;

ou

- l'article 702 de la FISA ne s'applique pas en pratique au transfert en cause et ne porte donc pas atteinte à l'efficacité de l'instrument de transfert prévu à l'article 46 du RGPD. L'exportateur peut alors procéder au transfert sans mesures supplémentaires.

2.4 Étape 4: adoption de mesures supplémentaires

50. Lorsqu'il ressort de l'évaluation réalisée par l'exportateur à l'étape 3 que l'instrument de transfert visé à l'article 46 du RGPD n'est pas efficace, l'exportateur devra déterminer, le cas échéant en collaboration avec l'importateur, s'il existe des mesures supplémentaires qui, ajoutées aux garanties contenues dans les instruments de transfert, pourraient garantir que les données transférées bénéficient dans le pays tiers d'un niveau de protection substantiellement équivalent

[60] Par exemple, dispositions de l'article 702 de la FISA; règlement de procédure de la Cour de surveillance du renseignement étranger (FISC), avis et décisions déclassifiés de la FISC, jurisprudence des juridictions américaines; rapports et transcriptions des auditions du comité de surveillance de la vie privée et des libertés civiles (PCLOB); rapports du Bureau de l'inspecteur général — ministère américain de la Justice; rapports du directeur du bureau des libertés civiles et de la vie privée de la NSA; rapports préparés par le service de recherche du Congrès; rapports de la Fondation américaine pour les libertés civiles (ACLU).

à celui qui est garanti au sein de l'Union[61]. 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[62].

51. L'exportateur doit déterminer au cas par cas quelles mesures supplémentaires pourraient être efficaces pour un ensemble de transferts vers un pays tiers donné lorsqu'il recourt à un instrument de transfert spécifique visé à l'article 46 du RGPD. L'exportateur ne doit pas recommencer l'évaluation chaque fois qu'il effectue le même transfert d'un type particulier de données vers le même pays tiers. Certaines données dont le transfert est prévu peuvent nécessiter des mesures supplémentaires et d'autres non (compte tenu de l'application formelle et/ou pratique de la législation du pays tiers). L'exportateur sera en mesure de s'appuyer sur ses évaluations et conclusions précédentes dans le cadre des étapes 1, 2 et 3 ci-dessus et de vérifier, sur la base de leurs conclusions, l'efficacité potentielle des mesures supplémentaires pour garantir le niveau de protection requis.

52. En principe, des mesures supplémentaires peuvent avoir un caractère contractuel, technique ou organisationnel. Combiner diverses mesures de telle sorte qu'elles se soutiennent et se renforcent mutuellement peut accroître le niveau de protection et, partant, contribuer à atteindre les normes de l'UE.

53. Des mesures contractuelles et organisationnelles ne permettront pas généralement, à elles seules, de surmonter l'accès des autorités publiques du pays tiers à des données à caractère personnel sur la base d'une législation et/ou de pratiques problématiques[63]. En effet, dans certaines situations, seules des mesures techniques dûment mises en œuvre pourraient empêcher ou rendre inopérant l'accès des autorités publiques de pays tiers à des données à caractère personnel, notamment à des fins de surveillance[64]. En pareil cas, des mesures contractuelles ou organisationnelles peuvent compléter des mesures techniques et renforcer le niveau global de protection des données (par exemple, en introduisant des contrôles et en éliminant des automatismes pour contrer les tentatives des autorités publiques d'accéder aux données en violation des normes de l'Union).

54. En collaboration, le cas échéant, avec l'importateur de données, l'exportateur peut examiner la liste (non exhaustive) suivante de facteurs permettant de déterminer quelles mesures

[61] C-311/18 (Schrems II), point 96.
[62] Considérant 109 du RGPD et C-311/18 (Schrems II), point 133.
[63] On entend par «législation problématique» une législation qui: 1) impose des obligations au destinataire de données à caractère personnel provenant de l'Union européenne et/ou affecte les données transférées d'une manière susceptible de porter atteinte à la garantie contractuelle d'un niveau de protection essentiellement équivalent contenue dans les instruments de transfert; et 2) ne respecte pas la substance des droits et libertés fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne ou va au-delà de ce qui est nécessaire et proportionné dans une société démocratique pour préserver l'un des objectifs importants également reconnus dans le droit de l'Union ou de ses États membres, tels que ceux énumérés à l'article 23, paragraphe 1, du RGPD.
[64] Lorsque cet accès va au-delà de ce qui est nécessaire et proportionné dans une société démocratique; voir articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, article 23, paragraphe 1, du RGPD et recommandations 2/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

supplémentaires seraient les plus efficaces pour protéger les données transférées contre les demandes des autorités publiques d'accéder à ces données sur la base d'une législation problématique appliquée dans la pratique:

- le format des données à transférer (c'est-à-dire en texte clair/pseudonymisées ou chiffrées);
- la nature des données (par exemple, un niveau de protection plus élevé est prévu dans l'EEE pour les catégories de données couvertes par les articles 9 et 10 du RGPD)[65];
- la longueur et la complexité du flux de traitement de données, le nombre d'acteurs intervenant dans le traitement et la relation entre eux [par exemple, les transferts impliquent-ils de multiples responsables du traitement ou des responsables du traitement et des sous-traitants, ou l'intervention de sous-traitants qui transféreront les données de l'exportateur à l'importateur (compte tenu des dispositions pertinentes qui leur sont applicables en vertu de la législation du pays tiers de destination)][66];
- la technique ou les paramètres de l'application pratique de la législation du pays tiers issus de l'étape 3;
- la possibilité que les données puissent faire l'objet de transferts ultérieurs, dans le même pays tiers, voire vers d'autres pays tiers (par exemple, l'intervention de sous-traitants ultérieurs de l'importateur de données)[67].

Exemples de mesures supplémentaires

55. Les listes non exhaustives figurant à l'annexe 2 présentent quelques exemples de mesures techniques, contractuelles et organisationnelles qui pourraient être envisagées et n'étaient pas déjà incluses dans l'instrument de transfert visé à l'article 46 du RGPD.

***

56. Si l'exportateur a mis en place des mesures supplémentaires efficaces, qui, combinées à l'instrument de transfert visé à l'article 46 du RGPD qu'il a choisi, atteignent un niveau de protection essentiellement équivalent à celui garanti au sein de l'EEE, il peut poursuivre ses transferts.

[65] Voir note de bas de page 42.
[66] Le RGPD impose des obligations distinctes aux responsables du traitement et aux sous-traitants. Les transferts peuvent se faire de responsable du traitement à responsable du traitement, entre responsables conjoints du traitement, de responsable du traitement à sous-traitant et, sous réserve de l'autorisation du responsable du traitement, de sous-traitant à responsable du traitement ou de sous-traitant à sous-traitant.
[67] Voir note de bas de page 26.

57. Lorsqu'il n'est pas en mesure de trouver ou de mettre en œuvre des mesures supplémentaires efficaces garantissant que les données à caractère personnel transférées bénéficient d'un niveau de protection essentiellement équivalent[68], l'exportateur ne doit pas commencer à transférer des données à caractère personnel vers le pays tiers concerné en recourant à l'instrument de transfert visé à l'article 46 du RGPD qu'il a choisi. S'il effectue déjà des transferts, il doit suspendre ou mettre fin au transfert de données à caractère personnel[69]. Conformément aux garanties contenues dans l'instrument de transfert visé à l'article 46 du RGPD auquel l'exportateur a recours, les données qu'il a déjà transférées vers ce pays tiers et les copies de ces données devraient lui être renvoyées ou être intégralement détruites par l'importateur[70].

Exemple:

La législation du pays tiers interdit les mesures supplémentaires que l'exportateur a recensées (par exemple, elle interdit le recours au chiffrement) ou entrave leur efficacité d'une autre manière. L'exportateur ne doit pas commencer à transférer des données à caractère personnel ou doit mettre fin aux transferts en cours vers ce pays.

58. L'autorité de contrôle compétente peut imposer toute autre mesure correctrice (par exemple, une amende) si, malgré le fait que l'exportateur n'est pas en mesure de démontrer l'existence d'un niveau de protection essentiellement équivalent dans le pays tiers, il commence un transfert ou le poursuit.

2.5 Étape 5: étapes de la procédure à suivre lorsque l'exportateur a identifié des mesures supplémentaires efficaces

59. Les étapes procédurales que l'exportateur devra peut-être prendre s'il identifie des mesures supplémentaires efficaces à mettre en place peuvent varier en fonction de l'instrument de transfert visé à l'article 46 du RGPD auquel il a recours ou envisage d'avoir recours.

2.5.1 Clauses types de protection des données («CCT») [article 46, paragraphe 2, points c) et d), du RGPD]

60. Lorsque l'exportateur a l'intention de mettre en place des mesures supplémentaires qui s'ajoutent aux CCT, il n'est pas nécessaire de demander une autorisation à l'autorité de contrôle compétente pour adopter ce type de clauses ou de garanties additionnelles, pour autant que les mesures supplémentaires identifiées ne contredisent pas, directement ou indirectement, les CCT et soient suffisantes pour assurer que le niveau de protection garanti par le RGPD n'est pas

[68] Lorsque cet accès va au-delà de ce qui est nécessaire et proportionné dans une société démocratique; voir articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, article 23, paragraphe 1, du RGPD et recommandations 2/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[69] C-311/18 (Schrems II), point 135.

[70] Voir, par exemple, clause 12 de l'annexe de la décision 87/2010 relative aux CCT; voir clause (facultative) de résiliation supplémentaire à l'annexe B de la décision 2004/915/CE relative aux CCT.

compromis[71]. L'exportateur et l'importateur de données doivent veiller à ce que les clauses supplémentaires ne puissent en aucun cas être interprétées comme restreignant les droits et obligations contenus dans les CCT ou comme réduisant autrement le niveau de protection des données. L'exportateur devrait être en mesure de le démontrer, y compris l'absence d'ambiguïté de toutes les clauses, conformément au principe de responsabilité et à son obligation d'offrir un niveau suffisant de protection des données. Les autorités de contrôle compétentes ont le pouvoir de réexaminer ces clauses supplémentaires si nécessaire (par exemple, en cas de réclamation ou dans le cadre d'une enquête d'initiative).

61. Lorsque l'exportateur a l'intention de modifier les clauses types de protection des données proprement dites ou lorsque les mesures supplémentaires ajoutées «contredisent», directement ou indirectement, les CCT, l'exportateur n'est plus réputé se prévaloir de clauses contractuelles types[72] et doit demander l'autorisation de l'autorité de contrôle compétente, conformément à l'article 46, paragraphe 3, point a), du RGPD.

2.5.2 Règles d'entreprise contraignantes [article 46, paragraphe 2, point b), du RGPD]

62. Le raisonnement exposé dans l'arrêt Schrems II s'applique également à d'autres instruments de transfert visés à l'article 46, paragraphe 2, du RGPD, étant donné que tous ces instruments ont essentiellement un caractère contractuel, de sorte que les garanties prévues et les engagements pris par les parties dans ces instruments ne sauraient lier les autorités publiques de pays tiers[73].

63. L'arrêt Schrems II est pertinent pour les transferts de données à caractère personnel fondés sur les règles d'entreprise contraignantes, étant donné que le droit des pays tiers peut porter atteinte à la protection qu'offrent ces instruments.

64. Tous les engagements qui doivent être inclus seront mentionnés dans les références WP256/257 mises à jour[74], sur lesquelles tous les groupes qui ont recours aux règles d'entreprise contraignantes comme instruments de transfert devront aligner leurs règles d'entreprise contraignantes actuelles et futures.

---

[71] Le considérant 109 du RGPD dispose ce qui suit: «La possibilité qu'ont les responsables du traitement et les sous-traitants de recourir à des clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle ne devrait pas les empêcher d'inclure ces clauses dans un contrat plus large, tel qu'un contrat entre le sous-traitant et un autre sous-traitant, ni d'y ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses contractuelles types adoptées par la Commission ou par une autorité de contrôle et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées». Des dispositions similaires sont prévues dans les ensembles de CCT adoptés par la Commission européenne au titre de la directive 95/45/CE.

[72] Voir, par analogie, avis 17/2020 du comité européen de la protection des données sur le projet de clauses contractuelles types présenté par l'autorité de contrôle de la Slovénie (article 28, paragraphe 8, du RGPD), déjà adopté, qui contient une disposition similaire («En outre, le comité rappelle que la possibilité d'utiliser des clauses contractuelles types adoptées par une autorité de contrôle n'empêche pas les parties d'ajouter d'autres clauses ou garanties supplémentaires, pour autant qu'elles ne contredisent pas, directement ou indirectement, les clauses contractuelles types adoptées ou ne portent pas atteinte aux droits ou libertés fondamentaux des personnes concernées. Par ailleurs, en cas de modification des clauses types de protection des données, les parties ne seront plus réputées avoir mis en œuvre les clauses contractuelles types adoptées»), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_fr.pdf.

[73] CJUE, C-311/18 (Schrems II), point 132.

[74] Groupe de travail «Article 29», document de travail établissant un tableau reprenant les éléments et principes qui figurent dans les règles d'entreprise contraignantes, tel que révisé et adopté en dernier lieu le 6 février 2018,

65. La Cour a souligné qu'il incombe à l'exportateur et à l'importateur de données d'apprécier si le niveau de protection requis par le droit de l'Union est respecté dans le pays tiers concerné afin de déterminer si les garanties établies par les clauses contractuelles types ou par les règles d'entreprise contraignantes peuvent être respectées dans la pratique. Si tel n'est pas le cas, l'exportateur devrait vérifier s'il peut prévoir des mesures supplémentaires permettant d'assurer un niveau de protection substantiellement équivalent à celui établi dans l'EEE et si le droit ou la pratique du pays tiers n'affectera pas ces mesures supplémentaires au point d'en compromettre l'efficacité.

2.5.3 Clauses contractuelles ad hoc. [article 46, paragraphe 3, point a), du RGPD]

66. Le raisonnement exposé dans l'arrêt Schrems II s'applique également à d'autres instruments de transfert au titre de l'article 46, paragraphe 2, du RGPD, étant donné que tous ces instruments ont essentiellement un caractère contractuel, de sorte que les garanties prévues et les engagements pris par les parties dans ces instruments ne sauraient lier les autorités publiques de pays tiers[75]. L'arrêt Schrems II est donc pertinent pour les transferts de données à caractère personnel fondés sur les clauses contractuelles ad hoc, étant donné que le droit des pays tiers peut porter atteinte à la protection qu'offrent ces instruments.

2.6 Étape 6: Réévaluation à intervalles appropriés

67. L'exportateur doit contrôler, en permanence, et le cas échéant en collaboration avec les importateurs de données, l'évolution de la situation dans le pays tiers vers lequel il a transféré des données à caractère personnel qui pourrait avoir une incidence sur son évaluation initiale du niveau de protection et sur les décisions qu'il peut, par conséquent, avoir prises en ce qui concerne ses transferts. La responsabilité est une obligation permanente (article 5, paragraphe 2, du RGPD).

68. L'exportateur devrait mettre en place des mécanismes suffisamment solides pour s'assurer qu'il peut suspendre ou cesser immédiatement ses transferts lorsque:

- l'importateur a enfreint ou n'est pas en mesure d'honorer les engagements liés à l'instrument de transfert visé à l'article 46 du RGPD; ou
- les mesures supplémentaires ne sont plus efficaces dans ce pays tiers.

3 CONCLUSION

69. Le RGPD établit des règles relatives au traitement des données à caractère personnel au sein de l'EEE et permet, de ce fait, la libre circulation des données à caractère personnel à l'intérieur de cet Espace. Le chapitre V du RGPD régit les transferts de données à caractère personnel vers des pays tiers et place la barre haut: le transfert ne doit pas porter atteinte au niveau de protection des personnes physiques garanti par le RGPD (article 44 du RGPD). L'arrêt de la CJUE dans l'affaire C-311/18 (Schrems II) souligne la nécessité d'assurer la continuité du niveau de protection accordé par le RGPD aux données à caractère personnel transférées vers un pays tiers[76].

WP256 rev.01; groupe de travail «Article 29», document de travail établissant un tableau reprenant les éléments et principes qui figurent dans les règles d'entreprise contraignantes, tel que révisé et adopté en dernier lieu le 6 février 2018, WP257 rev.01.

[75] CJUE, C-311/18 (Schrems II), point 132.

[76] C-311/18 (Schrems II), point 93.

70. Pour garantir un niveau de protection essentiellement équivalent de ses données, l'exportateur doit d'abord et avant tout connaître parfaitement ses transferts. Les exportateurs doivent également vérifier que les données qu'ils transfèrent sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

71. Ils doivent également identifier l'instrument de transfert auquel ils ont recours pour leurs transferts. Si l'instrument de transfert n'est pas une décision d'adéquation, l'exportateur doit vérifier au cas par cas si le droit ou la pratique du pays tiers de destination porte ou non atteinte aux garanties contenues dans l'instrument de transfert visé à l'article 46 du RGPD dans le cadre de ses transferts. Lorsque l'instrument de transfert visé à l'article 46 du RGPD ne permet pas d'atteindre, à lui seul, un niveau de protection essentiellement équivalent pour les données à caractère personnel que l'exportateur transfère, des mesures supplémentaires peuvent combler cette lacune.

72. Lorsqu'il n'est pas en mesure de trouver ou de mettre en œuvre des mesures supplémentaires efficaces garantissant que les données à caractère personnel transférées bénéficient d'un niveau de protection essentiellement équivalent, l'exportateur ne doit pas commencer à transférer des données à caractère personnel vers le pays tiers concerné en recourant à l'instrument de transfert qu'il a choisi. S'il effectue déjà des transferts, il est tenu de suspendre ou de mettre fin immédiatement au transfert de données à caractère personnel.

73. L'autorité de contrôle compétente a le pouvoir de suspendre ou de faire cesser des transferts de données à caractère personnel vers le pays tiers lorsque la protection des données transférées exigée par le droit de l'Union, en particulier par les articles 45 et 46 du RGPD et la Charte des droits fondamentaux, n'est pas garantie.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

ANNEXE 1: DÉFINITIONS

- On entend par «pays tiers» tout pays qui n'est pas un État membre de l'EEE.
- L' «EEE» désigne l'Espace économique européen et comprend les États membres de l'Union européenne ainsi que l'Islande, la Norvège et le Liechtenstein. Le RGPD s'applique à ces derniers en vertu de l'accord EEE, notamment son annexe XI et son protocole 37.
- Le «RGPD» désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- La «Charte» désigne la Charte des droits fondamentaux de l'Union européenne, JO C 326 du 26.10.2012, p. 391.
- La ««CJUE» ou «la Cour»» désignent la Cour de justice de l'Union européenne. Elle est l'autorité judiciaire de l'Union européenne et assure, en coopération avec les juridictions des États membres, l'application et l'interprétation uniformes du droit de l'Union.
- On entend par «exportateur de données» le responsable du traitement ou le sous-traitant établi dans l'EEE qui transfère des données à caractère personnel vers un responsable du traitement ou un sous-traitant établi dans un pays tiers.
- On entend par «importateur de données» le responsable du traitement ou le sous-traitant établi dans un pays tiers qui reçoit ou a accès aux données à caractère personnel transférées depuis l'EEE.
- On entend par «instrument de transfert visé à l'article 46 du RGPD» les garanties appropriées au sens de l'article 46 du RGPD que les exportateurs de données mettent en place lorsqu'ils transfèrent des données à caractère personnel vers un pays tiers en l'absence de décision d'adéquation au titre de l'article 45, paragraphe 3, du RGPD. L'article 46, paragraphes 2 et 3, du RGPD contient la liste des instruments de transfert visés à l'article 46 du RGPD auxquels les responsables du traitement et les sous-traitants peuvent recourir.
- Les «CCT» désignent les clauses types de protection des données (ou «clauses contractuelles types») adoptées par la Commission européenne pour les transferts de données à caractère personnel entre des responsables du traitement ou des sous-traitants établis dans l'EEE et des responsables du traitement ou des sous-traitants établis en dehors de l'EEE. Les clauses contractuelles types adoptées par la Commission européenne sont un instrument de transfert en vertu du RGPD, conformément à l'article 46, paragraphe 2, point c), et à l'article 46, paragraphe 5, du RGPD.

ANNEXE 2: EXEMPLES DE MESURES SUPPLÉMENTAIRES

74. Les mesures présentées ci-dessous sont des exemples de mesures supplémentaires que l'exportateur de données pourrait envisager lorsqu'il parvient à l'étape 4: «Adoption de mesures supplémentaires». Cette liste n'est pas exhaustive. L'exportateur peut envisager d'autres mesures supplémentaires. Les développements technologiques, juridiques ou organisationnels futurs peuvent conduire à l'émergence de nouvelles mesures supplémentaires que l'exportateur pourra envisager. La sélection et la mise en œuvre d'une ou de plusieurs de ces mesures ne garantissent pas nécessairement et systématiquement que le transfert satisfera la norme d'équivalence essentielle établie par le droit de l'Union. L'exportateur devrait sélectionner les mesures supplémentaires qui peuvent effectivement garantir ce niveau de protection pour ses transferts.

75. Toute mesure supplémentaire ne peut être réputée efficace au sens de l'arrêt de la CJUE dans l'affaire Schrems II que si et dans la mesure où – seule ou en combinaison avec d'autres mesures – elle remédie aux lacunes relevées dans l'évaluation de la situation du pays tiers que l'exportateur a effectuée en ce qui concerne la législation et les pratiques applicables à son transfert. Si, en fin de compte, l'exportateur n'est pas en mesure de garantir un niveau de protection essentiellement équivalent, il ne doit pas transférer les données à caractère personnel.

76. En sa qualité de responsable du traitement ou de sous-traitant, l'exportateur peut déjà être tenu de mettre en œuvre certaines des mesures décrites dans la présente annexe afin de se conformer au RGPD. En d'autres termes, des mesures similaires pourraient devoir être mises en place pour les données à caractère personnel traitées dans l'EEE transférées à un importateur de données couvert par une décision d'adéquation ou vers d'autres pays tiers[77].

2.1 Mesures techniques

77. La présente section décrit une série non exhaustive d'exemples de mesures techniques susceptibles de compléter les garanties supplémentaires qu'offrent les instruments de transfert visés à l'article 46 du RGPD, afin de garantir le respect du niveau de protection requis par le droit de l'Union dans le cadre d'un transfert de données à caractère personnel vers un pays tiers. Ces mesures seront particulièrement nécessaires dans le cas où le droit dudit pays impose à l'importateur de données des obligations qui sont contraires aux garanties offertes par les instruments de transfert visés à l'article 46 du RGPD et qui sont, notamment, susceptibles de porter atteinte à la garantie contractuelle d'un niveau de protection essentiellement équivalent contre l'accès des autorités publiques de ce pays à ces données[78].

78. Pour plus de clarté, la présente section présente d'abord quelques exemples de scénarios pour lesquels certaines mesures techniques pourraient potentiellement garantir effectivement un niveau de protection essentiellement équivalent. La section présente ensuite différents scénarios dans lesquels les mesures techniques destinées à garantir ce niveau de protection ne sont pas identifiées.

[77] Article 5, paragraphe 2, et article 32 du RGPD.
[78] C-311/18 (Schrems II), point 135.

Exemples de scénarios faisant référence à des cas où des mesures *effectives* sont identifiées

79. Les mesures énumérées ci-dessous visent à garantir que l'accès des autorités publiques de pays tiers aux données transférées ne porte pas atteinte à l'efficacité des garanties appropriées que contiennent les instruments de transfert visés à l'article 46 du RGPD. Ces mesures seraient nécessaires pour garantir un niveau de protection essentiellement équivalent à celui garanti dans l'EEE, même si l'accès des autorités publiques est conforme à la législation du pays de l'importateur, où, en pratique, cet accès va au-delà de ce qui est nécessaire et proportionné dans une société démocratique[79]. Ces mesures visent à prévenir tout accès potentiellement illicite, en empêchant les autorités d'identifier les personnes concernées, de déduire des informations les concernant, de les distinguer dans un autre contexte ou d'associer les données transférées à d'autres ensembles de données qui pourraient contenir, notamment, des identifiants en ligne fournis par les appareils, applications, outils et protocoles utilisés par les personnes concernées dans d'autres contextes.

80. Les autorités publiques des pays tiers peuvent tenter d'accéder aux données transférées:

    a) lors du transit, en accédant aux lignes de communication utilisées pour transmettre les données au pays destinataire. Cet accès peut être passif, auquel cas le contenu de la communication, éventuellement après un processus de sélection, est simplement copié. L'accès peut toutefois également être actif en ce sens que les autorités publiques interviennent dans le processus de communication non seulement en lisant le contenu, mais également en manipulant ou en effaçant certaines parties de celui-ci;

    b) pendant que les données sont détenues par le destinataire prévu, soit en accédant aux installations de traitement proprement dites, soit en exigeant du destinataire des données qu'il localise et extraie les données présentant un intérêt et les remette aux autorités.

81. La présente section analyse des scénarios dans lesquels les mesures appliquées sont efficaces dans les deux cas. Différentes mesures supplémentaires peuvent s'appliquer et être suffisantes dans le cas d'un transfert précis, dès lors qu'un seul type d'accès est prévu par le droit du pays destinataire. L'exportateur de données doit donc analyser soigneusement, avec l'aide de l'importateur, les obligations qui incombent à ce dernier.

À titre d'exemple, les importateurs de données américains relevant de l'article 50 USC § 1881a (article 702 de la FISA) sont soumis à une obligation directe d'accorder un accès ou de transmettre aux autorités les données à caractère personnel qui sont en leur possession, sous leur garde ou sous leur contrôle. Cela peut couvrir toutes les clés cryptographiques nécessaires pour rendre les données intelligibles.

82. Les scénarios décrivent des circonstances particulières et les mesures prises afin de servir d'exemples. Toute modification apportée aux scénarios peut conduire à des conclusions

[79] Voir articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, article 23, paragraphe 1, du RGPD et recommandations 02/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020.

différentes. Les scénarios se réfèrent à des situations dans lesquelles il a été conclu que des mesures supplémentaires sont nécessaires d'emblée, c'est-à-dire lorsqu'en pratique, une législation problématique du pays tiers s'applique au transfert en question.

83. Les responsables du traitement peuvent être amenés à appliquer une partie ou l'ensemble des mesures décrites ici, quel que soit le niveau de protection prévu par la législation applicable à l'importateur de données, car celle-ci sont nécessaires dans le cadre de la mise en conformité aux articles 25 et 32 du RGPD dans les circonstances particulières du transfert. En d'autres termes, l'exportateur peut être tenu de mettre en œuvre les mesures décrites dans le présent document même si son importateur est couvert par une décision d'adéquation, tout comme les responsables du traitement et les sous-traitants peuvent être contraints de les mettre en œuvre lorsque les données sont traitées au sein de l'EEE.

Cas nº 1: stockage des données à des fins de sauvegarde et pour d'autres finalités qui ne nécessitent pas un accès aux données en clair

84. Un exportateur de données utilisera un fournisseur de services d'hébergement établi dans un pays tiers pour stocker des données à caractère personnel, par exemple à des fins de sauvegarde.

Si

1. les données à caractère personnel sont traitées au moyen d'un chiffrement solide avant leur transmission et l'identité de l'importateur est vérifiée,
2. l'algorithme de chiffrement et son paramétrage (par exemple, la longueur de clé, le mode opératoire, le cas échéant) sont conformes à l'état de la technique et peuvent être considérés comme résistants à une cryptanalyse réalisée par les autorités publiques du pays destinataire, compte tenu des ressources et des capacités techniques (par exemple, la puissance de calcul pour les attaques par force brute) dont elles disposent[80],

[80] Pour évaluer la force des algorithmes de chiffrement, leur conformité avec l'état de la technique et leur solidité face à la cryptanalyse dans le temps, les exportateurs de données peuvent s'appuyer sur les orientations techniques publiées par les autorités officielles de l'UE et de ses États membres en matière de cybersécurité. Voir, par exemple, le rapport de l'ENISA, «What is the "state of the art" in IT security?», 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; orientations de l'Office fédéral allemand pour la sécurité de l'information dans ses Directives techniques de la série TR-02102 «Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Projet 645421, D5.4, ECRYPT-CSA, 02/2018» disponibles à l'adresse suivante: https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

3. la solidité du chiffrement et la longueur de la clé tiennent compte de la durée spécifique pendant laquelle la confidentialité des données à caractère personnel chiffrées doit être préservée[81],
4. l'algorithme de chiffrement est correctement exécuté par un logiciel dûment mis à jour, sans vulnérabilités connues, dont la conformité par rapport à la spécification de l'algorithme choisi a été vérifiée, par exemple par une certification,
5. les clés sont gérées (générées, administrées, stockées, le cas échéant, liées à l'identité d'un destinataire prévu, et effacées) de manière fiable[82], et
6. les clés sont conservées uniquement sous le contrôle de l'exportateur de données, ou par une entité qui a la confiance de ce dernier dans l'EEE ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE,

le comité européen de la protection des données considère alors que le chiffrement effectué constitue une mesure supplémentaire efficace.

Cas nº 2: transfert de données pseudonymisées

85. Un exportateur de données commencera par pseudonymiser les données qu'il détient et les transfèrera ensuite à un pays tiers pour analyse, par exemple à des fins de recherche.

Si

1. Un exportateur de données transfère des données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise, ni être utilisées pour distinguer la personne concernée au sein d'un groupe plus vaste, sans avoir recours à des informations supplémentaires[83],
2. les informations supplémentaires sont détenues exclusivement par l'exportateur de données et conservées séparément dans un État membre ou dans un pays tiers par une entité qui a la

[81] La capacité de protection des algorithmes cryptographiques est susceptible de diminuer au fil du temps du fait de la découverte de nouvelles techniques de cryptanalyse, de l'émergence de nouveaux paradigmes informatiques, comme l'informatique quantique, et de l'augmentation générale de la puissance de calcul disponible, à moins que les algorithmes utilisés ne se révèlent théoriquement sûrs. Cette préoccupation concerne tout particulièrement les algorithmes de clés publiques couramment utilisés au moment de la rédaction. L'exportateur de données doit donc considérer que les autorités publiques peuvent s'engager à accéder aux données cryptées dans les circonstances décrites au paragraphe 80 et à les stocker jusqu'à ce que leurs ressources soient suffisantes pour les déchiffrer. La mesure supplémentaire ne peut être considérée comme efficace que si le déchiffrement et le traitement ultérieur qui en résulte ne constituent plus, à ce moment, une violation des droits des personnes concernées, par exemple, parce que les données ne peuvent plus être utilisées directement ou indirectement pour les identifier.

[82] NIST Special Publication 800-57, Recommendation for Key Management https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[83] Conformément à l'article 4, paragraphe 5, du RGPD: «on entend par "pseudonymisation" le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable». Les informations supplémentaires peuvent consister en des tableaux mettant les pseudonymes en regard avec des attributs d'identification qu'ils remplacent, des clés de chiffrement ou d'autres paramètres servant à la transformation des attributs, ou d'autres données permettant d'attribuer les données pseudonymisées à des personnes physiques identifiées ou identifiables.

confiance de l'exportateur dans l'EEE ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE,

3. la divulgation ou l'utilisation non autorisée de ces informations supplémentaires est empêchée par des garanties techniques et organisationnelles appropriées, et il est garanti que l'exportateur conserve le contrôle exclusif de l'algorithme ou du répertoire permettant une réidentification à l'aide des informations supplémentaires, et
4. le responsable du traitement a établi, au moyen d'une analyse approfondie des données en question, en tenant compte de toutes les informations dont les autorités publiques du pays destinataire pourraient disposer et qu'elles pourraient utiliser, que les données à caractère personnel pseudonymisées ne peuvent pas être attribuées à une personne physique identifiée ou identifiable même en procédant à des recoupements avec ces informations,

le comité européen de la protection des données considère alors que la pseudonymisation effectuée constitue une mesure supplémentaire efficace.

86. Il est à noter que, dans de nombreux cas, des facteurs tenant à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale d'une personne physique, à sa localisation physique ou à son interaction avec un service internet à des moments précis[84] peuvent permettre d'identifier cette personne même si son nom, son adresse ou d'autres identifiants simples sont omis.

87. C'est notamment le cas lorsque les données concernent l'utilisation de services d'information (moment d'accès, ordre des fonctions consultées, caractéristiques de l'appareil utilisé, etc.). Ces services pourraient, comme pour l'importateur de données à caractère personnel, être soumis à l'obligation d'accorder un accès aux mêmes autorités publiques compétentes sur leur territoire, lesquelles détiendront alors probablement des données sur l'utilisation de ces services d'information par la ou les personnes qu'elles visent.

88. En outre, puisque l'utilisation de ces services d'information est publique par nature ou compte tenu de leur caractère exploitable par des parties dotées de ressources considérables, les responsables du traitement devront faire preuve d'une attention supplémentaire, étant donné que les autorités publiques de leur territoire sont susceptibles de détenir des données sur l'utilisation de services d'information par une personne qu'elles visent.

89. Si, lors de la pseudonymisation, des attributs contenus dans les données à caractère personnel sont transformés à l'aide d'un algorithme cryptographique, les orientations figurant dans les notes de bas de page 80 et 81 s'appliquent. Il est désormais recommandé de renoncer à l'utilisation exclusive de la cryptographie et d'appliquer des conversions basées sur des tableaux de référence.

[84] L'article 4, paragraphe 1, du RGPD dispose que: «on entend par "données à caractère personnel" toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale».

Cas nº 3: Chiffrement de données afin de les protéger contre l'accès des autorités publiques du pays tiers de l'importateur lorsqu'elles transitent entre l'exportateur et son importateur

90. Un exportateur de données souhaite transférer des données vers une destination où la législation et/ou les pratiques autorisent l'accès des autorités publiques aux données alors qu'elles transitent entre le pays de l'exportateur et le pays de destination.

Si

1. Un exportateur de données transfère des données à caractère personnel à un importateur de données dans une juridiction où la législation et/ou la pratique autorisent les autorités publiques à accéder aux données alors qu'elles sont transmises par internet vers ce pays tiers sans les garanties essentielles européennes relatives à cet accès, le chiffrement de la transmission est utilisé, garantissant ainsi que les protocoles de chiffrement employés sont à la pointe de la technologie et offrent une protection efficace contre les attaques actives et passives au moyen de ressources dont disposent notoirement les autorités publiques du pays tiers,
2. les parties concernées par la communication conviennent d'une autorité ou d'une infrastructure de certification à clé publique digne de confiance,
3. des mesures de protection spécifiques et de pointe sont utilisées contre les attaques actives et passives dirigées contre les systèmes d'envoi et de réception qui assurent le chiffrement de la transmission, y compris des tests de vulnérabilité des logiciels et d'éventuelles portes dérobées,
4. au cas où le chiffrement du transfert ne permet pas en lui-même une sécurité suffisante en raison de la vulnérabilité de l'infrastructure ou du logiciel utilisé, les données à caractère personnel sont également chiffrées de bout en bout sur la couche application grâce à des méthodes de chiffrement de pointe,
5. l'algorithme de chiffrement et son paramétrage (par exemple la longueur de clé ou le mode opératoire, le cas échéant) sont conformes à l'état de la technique et peuvent être considérés comme résistants à une cryptanalyse réalisée par les autorités publiques lorsque les données transitent vers ce pays tiers, compte tenu des ressources et des capacités techniques (par exemple la puissance de calcul pour les attaques par force brute) dont elles disposent (voir note de bas de page 80 ci-dessus)[85],
6. la solidité du chiffrement tient compte de la durée spécifique pendant laquelle la confidentialité des données à caractère personnel chiffrées doit être préservée,
7. l'algorithme de chiffrement est correctement exécuté par un logiciel dûment mis à jour, sans vulnérabilités connues, et dont la conformité par rapport à la spécification de l'algorithme choisi a été vérifiée, par exemple par une certification,
8. les clés sont gérées de manière fiable (générées, administrées, stockées, le cas échéant, liées à l'identité du destinataire prévu et supprimées) par l'exportateur ou par une entité en laquelle l'exportateur a confiance située sur un territoire offrant un niveau de protection essentiellement équivalent;

[85] Voir note de bas de page 80 pour certaines références aux orientations techniques publiées par les autorités officielles de l'UE et de ses États membres en matière de cybersécurité.

le comité européen de la protection des données considère alors que le chiffrement du transfert, combiné, le cas échéant, à un chiffrement de bout en bout du contenu, constitue une mesure supplémentaire efficace.

Cas nº 4: destinataire protégé

91. Un exportateur de données transfère des données à caractère personnel à un importateur de données dans un pays tiers spécifiquement protégé par le droit national, par exemple dans le but de fournir conjointement un traitement médical à un patient ou des services juridiques à un client.

Si

1. la législation d'un pays tiers exempte un importateur de données résident d'enfreindre potentiellement l'accès à des données détenues par ce destinataire pour la finalité donnée, par exemple en vertu d'une obligation de secret professionnel s'appliquant à l'importateur de données,
2. cette exemption s'étend à toutes les informations que détient l'importateur de données qui pourraient être utilisées pour contourner la protection des informations privilégiées (clés cryptographiques, mots de passe, autres identifiants, etc.),
3. l'importateur de données n'utilise pas les services d'un sous-traitant d'une manière qui permette aux autorités publiques d'accéder aux données pendant qu'elles sont détenues par le sous-traitant, et l'importateur ne transfère pas les données à une autre entité non protégée au moyen des instruments de transfert visés à l'article 46 du RGPD,
4. les données à caractère personnel sont chiffrées avant d'être transmises selon une méthode conforme aux standards garantissant que le déchiffrement sera impossible sans connaître la clé de déchiffrement (chiffrement de bout en bout) pendant toute la période durant laquelle les données doivent être protégées,
5. la clé de chiffrement est confiée à la garde exclusive de l'importateur de données protégé et, éventuellement, à l'exportateur lui-même ou à une autre entité ayant la confiance de l'exportateur établie dans l'EEE ou dans une juridiction offrant un niveau de protection essentiellement équivalent à celui garanti dans l'EEE, et adéquatement protégée contre une utilisation ou une divulgation non autorisée par des mesures techniques et organisationnelles conformes à l'état de la technique, et
6. l'exportateur de données a établi de manière fiable que la clé de chiffrement qu'il a l'intention d'utiliser correspond à la clé de déchiffrement détenue par le destinataire,

le comité européen de la protection des données considère alors que le chiffrement effectué constitue une mesure supplémentaire efficace.

Cas nº 5: traitement fractionné ou multipartite

92. L'exportateur de données souhaite que les données à caractère personnel soient traitées conjointement par deux ou plusieurs sous-traitants indépendants situés dans des territoires différents, sans leur divulguer le contenu des données. Avant le transfert, il fractionne les données de manière à ce qu'aucun des sous-traitants ne reçoive suffisamment de données pour reconstituer les données à caractère personnel en totalité ou en partie. L'exportateur de données reçoit les résultats du traitement de chacun des sous-traitants de manière

indépendante et rassemble les pièces reçues pour parvenir au résultat final, qui peut être constitué de données à caractère personnel ou de données agrégées.

Si

1. un exportateur de données traite des données à caractère personnel de manière à ce que celles-ci soient scindées en deux ou plusieurs parties qui ne peuvent plus être interprétées ou attribuées à une personne concernée spécifique sans avoir recours à des informations supplémentaires,
2. chacune des pièces est transférée à un sous-traitant distinct situé sur un territoire différent,
3. les sous-traitants traitent éventuellement les données conjointement, par exemple en utilisant des calculs sécurisés multipartites, de sorte qu'aucune information qu'ils ne possèdent pas avant le calcul ne soit révélée à l'un d'entre eux,
4. l'algorithme utilisé pour le calcul partagé est protégé contre les adversaires actifs,
5. le responsable du traitement a établi, au moyen d'une analyse approfondie relative aux données en question, et compte tenu des éléments d'information manquants dont les autorités publiques des pays destinataires pourraient disposer et qu'elles pourraient utiliser, que les éléments des données à caractère personnel qu'il transmet aux sous-traitants ne peuvent pas être attribuées à une personne physique identifiée ou identifiable, même en procédant à des recoupements avec ces informations,
6. il n'existe aucune preuve d'une potentielle collaboration entre les autorités publiques des territoires respectifs dans lesquels les sous-traitants se trouvent, qui leur permettrait d'accéder à tous les ensembles de données à caractère personnel détenus par les sous-traitants et de reconstituer et d'exploiter le contenu des données à caractère personnel en clair, dans des conditions où une telle exploitation ne serait pas conforme au principe essentiel des droits et libertés fondamentaux des personnes concernées. De même, les autorités publiques de ces pays ne devraient pas être habilitées à accéder aux données à caractère personnel détenues par les sous-traitants dans tous les territoires concernés,

le comité européen de la protection des données considère que le traitement fractionné des données effectué constitue une mesure supplémentaire efficace.

Exemples de scénarios faisant référence à des cas où des mesures *effectives* ne sont pas identifiées

93. Les mesures décrites dans certains des scénarios ci-dessous ne permettraient pas de garantir un niveau de protection essentiellement équivalent des données transférées vers le pays tiers. Elles ne seraient donc pas considérées comme des mesures supplémentaires appropriées.

Cas nº 6: transfert à des fournisseurs de services informatiques en nuage ou à d'autres sous-traitants nécessitant un accès à des données en clair

94. Un exportateur de données transfère des données à caractère personnel par voie électronique ou en les mettant à la disposition d'un fournisseur de services informatiques en nuage ou d'un autre sous-traitant afin que ces données soient traitées selon les instructions de ces derniers dans un pays tiers (par exemple pour la fourniture d'un support technique ou tout autre type de traitement cloud), et ces données ne sont pas – ou ne peuvent pas – être pseudonymisées tel

qu'indiqué dans le cas nº 2, ou chiffrées tel qu'indiqué dans le cas nº 1 du fait que le traitement nécessite d'accéder aux données en clair,

Si

1. un responsable du traitement transfère des données à caractère personnel à un fournisseur de services informatiques en nuage ou à un autre sous-traitant,
2. le fournisseur de services informatiques en nuage ou un autre sous-traitant doit accéder aux données en clair afin d'exécuter la tâche qui lui a été assignée, et
3. le pouvoir conféré aux autorités publiques du pays destinataire d'accéder aux données transférées en question va au-delà de ce qui est nécessaire et proportionné dans une société démocratique lorsque, dans la pratique, la législation problématique du pays tiers s'applique aux transferts en cause (voir étape 3)[86],

compte tenu des standards en vigueur, le comité européen de la protection des données n'est alors pas en mesure d'envisager une mesure technique efficace pour empêcher que cet accès porte atteinte aux droits fondamentaux des personnes concernées. Le comité européen de la protection des données n'exclut pas qu'un développement technologique futur puisse offrir des mesures permettant d'atteindre les objectifs commerciaux visés, sans nécessiter un accès aux données en clair.

95. Dans les scénarios présentés, lorsque des données à caractère personnel non chiffrées sont techniquement nécessaires à la prestation du service par le sous-traitant, le chiffrement du transfert ainsi que le chiffrement des données statiques, même considérés ensemble, ne constituent pas une mesure supplémentaire garantissant un niveau de protection essentiellement équivalent si l'importateur de données est en possession des clés cryptographiques.

Cas nº 7: transfert de données à caractère personnel à des fins commerciales, y compris au moyen d'un accès à distance

96. Un exportateur de données transfère des données à caractère personnel à des entités — dans un pays tiers à des fins commerciales partagées – par voie électronique ou en les mettant à disposition au moyen d'un accès à distance de l'importateur de données – et ces données ne sont pas – ou ne peuvent pas être – pseudonymisées comme décrit dans le cas nº 2 ou chiffrées comme décrit dans le cas nº 1 car le traitement nécessite d'accéder aux données en clair. Une configuration typique peut consister en un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre qui transfère des données à caractère personnel à un responsable du traitement ou à un sous-traitant dans un pays tiers appartenant au même groupe d'entreprises ou à un groupe d'entreprises exerçant une activité économique conjointe. L'importateur de données peut, par exemple, utiliser les données qu'il reçoit pour fournir des services de personnel à l'exportateur de données, services pour lesquels il aurait besoin de données relatives aux ressources humaines, ou de communiquer par téléphone ou par courrier électronique avec des clients de l'exportateur de données vivant dans l'Union européenne.

Si

1. un exportateur de données transfère des données à caractère personnel à un importateur de données dans un pays tiers en les mettant à disposition au moyen d'un système informatique

[86] Voir articles 47 et 52 de la Charte des droits fondamentaux de l'Union européenne, article 23, paragraphe 1, du RGPD et recommandations 02/2020 du comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020.

d'une manière qui permet à l'importateur d'accéder directement aux données de son choix ou en les transmettant directement, individuellement ou en vrac, au moyen d'un service de communication,

2. l'importateur[87] traite les données en clair dans le pays tiers (y compris à ses propres fins lorsqu'il est un responsable du traitement),
3. le pouvoir conféré aux autorités publiques du pays destinataire d'accéder aux données transférées en question va au-delà de ce qui est nécessaire et proportionné dans une société démocratique lorsque, dans la pratique, la législation problématique du pays tiers s'applique aux transferts en question (voir étape 3),

alors, le comité européen de la protection des données n'est pas à même d'envisager une mesure technique efficace pour empêcher que cet accès porte atteinte aux droits fondamentaux de la personne concernée.

97. Dans les scénarios présentés, lorsque des données à caractère personnel non chiffrées sont techniquement nécessaires à la prestation du service par le sous-traitant, le chiffrement du transfert et le chiffrement des données statiques, même considérés ensemble, ne constituent pas une mesure supplémentaire garantissant un niveau de protection essentiellement équivalent si l'importateur de données est en possession des clés cryptographiques.

2.2 Mesures contractuelles supplémentaires

98. Ces mesures consisteront généralement en des engagements contractuels[88] unilatéraux, bilatéraux ou multilatéraux[89]. En cas de recours à un instrument de transfert visé à l'article 46 du RGPD, dans la plupart des cas, celui-ci contiendra déjà un certain nombre d'engagements (essentiellement contractuels) de l'exportateur et de l'importateur de données destinés à protéger les données à caractère personnel[90].

99. Dans certaines situations, ces mesures peuvent compléter et renforcer les garanties que peuvent offrir l'instrument de transfert et la législation pertinente du pays tiers, lorsque, compte tenu des circonstances du transfert, ils ne remplissent pas toutes les conditions requises pour garantir un niveau de protection essentiellement équivalent à celui garanti au sein de l'EEE. Sous réserve du caractère des mesures contractuelles, qui ne sont généralement pas susceptibles de lier les autorités du pays tiers lorsqu'elles ne sont pas parties au contrat[91], il est fréquent que ces mesures doivent être combinées avec d'autres mesures techniques et organisationnelles afin d'offrir le

[87] Qu'il s'agisse d'un responsable du traitement ou d'un sous-traitant établi dans un pays tiers qui reçoit ou a accès aux données à caractère personnel transférées depuis l'EEE.

[88] Ils auront un caractère privé et ne seront pas considérés comme des accords internationaux au sens du droit international public. Par conséquent, ils ne lieront normalement pas les autorités publiques du pays tiers, puisque ces dernières ne sont pas parties au contrat conclu avec des organismes privés dans des pays tiers, comme l'a souligné la Cour dans son arrêt dans l'affaire C-311/18 (Schrems II), point 125.

[89] Par exemple dans les règles d'entreprise contraignantes, qui devraient, en tout état de cause, réglementer certaines des mesures énumérées ci-dessous.

[90] Voir arrêt C-311/18 (Schrems II), point 137, où la Cour a reconnu que les CCT comportent «des mécanismes effectifs permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts de données à caractère personnel, fondés sur de telles clauses, soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer»» (voir aussi point 148).

[91] C-311/18 (Schrems II), point 125.

niveau requis de protection des données. La sélection et la mise en œuvre d'une ou de plusieurs de ces mesures ne garantissent pas nécessairement et systématiquement que le transfert répondra à la norme d'équivalence essentielle établie par le droit de l'Union.

100. En fonction des mesures contractuelles déjà incluses dans l'instrument de transfert visé à l'article 46 du RGPD qui est utilisé, des mesures contractuelles supplémentaires peuvent également être utiles pour permettre aux exportateurs de données établis dans l'EEE de prendre connaissance des nouveaux développements touchant à la protection des données transférées vers des pays tiers.

101. Comme indiqué précédemment, ces mesures ne permettront pas d'exclure l'application de la législation d'un pays tiers qui ne satisfait pas à la norme du comité européen de la protection des données concernant les garanties essentielles européennes dans les cas où cette législation impose aux importateurs de se conformer aux injonctions de divulgation des données que leur adressent les autorités publiques[92].

102. Quelques exemples de ces mesures contractuelles potentielles sont mentionnés ci-dessous et classés en fonction de leur nature.

Clause prévoyant une obligation contractuelle de recourir à des mesures techniques spécifiques

103. En fonction des circonstances particulières des transferts (notamment l'application pratique de la législation du pays tiers), le contrat peut devoir stipuler que des mesures techniques spécifiques devraient être mises en œuvre pour que les transferts aient lieu (voir les mesures techniques suggérées ci-dessus).

104. Conditions d'efficacité:

- Cette clause pourrait se révéler efficace dans les cas où l'exportateur a constaté la nécessité de mesures techniques. Elle devrait alors revêtir une forme juridique afin de garantir que l'importateur s'engage également à mettre en place les mesures techniques nécessaires, le cas échéant.

Obligations de transparence:

105. L'exportateur pourrait ajouter des annexes au contrat contenant des informations que l'importateur aurait fournies avant la conclusion du contrat, dans toute la mesure du possible, sur l'accès des autorités publiques aux données, notamment dans le domaine des renseignements, pour autant que la législation soit conforme aux garanties essentielles européennes du comité européen de la protection des données dans le pays de destination. Cela pourrait aider l'exportateur de données à satisfaire à son obligation de documenter son évaluation du niveau de protection dans le pays tiers. Cela peut également souligner l'obligation faite à l'importateur d'aider l'exportateur dans son évaluation et d'engager la responsabilité de l'importateur dans la fourniture à l'exportateur d'informations objectives, fiables, pertinentes, vérifiables et accessibles au public ou d'informations accessibles autrement.

[92] CJUE, C-311/18 (Schrems II), point 132.

106. L'importateur pourrait, par exemple, être tenu:

(1) d'énumérer les dispositions législatives et réglementaires du pays de destination applicables à l'importateur ou à ses sous-traitants (ultérieurs), qui permettraient aux autorités publiques d'accéder aux données à caractère personnel faisant l'objet du transfert, notamment dans les domaines du renseignement, de l'application de la loi et du contrôle administratif et réglementaire applicable aux données transférées;

(2) en l'absence de législation régissant l'accès des autorités publiques aux données, de fournir des informations et des statistiques fondées sur l'expérience de l'importateur ou sur des rapports émanant de diverses sources (partenaires, sources ouvertes, jurisprudence nationale et décisions des organismes de contrôle, par exemple) concernant l'accès des autorités publiques à des données à caractère personnel dans des situations similaires à celles du transfert en cause (c'est-à-dire dans le domaine réglementaire donné, sur le type d'entités auquel appartient l'importateur de données, etc.);

(3) d'indiquer les mesures prises pour empêcher l'accès aux données transférées (le cas échéant);

(4) de fournir des informations suffisamment détaillées sur toutes les demandes d'accès des autorités à des données à caractère personnel que l'importateur a reçues au cours d'une période déterminée[93], en particulier dans les domaines mentionnés au point 1) ci-dessus, et comprenant des informations sur les demandes reçues, les données demandées, l'organisme demandeur, la base juridique de la divulgation et la mesure dans laquelle l'importateur a divulgué la demande de données[94];

(5) de préciser si et dans quelle mesure la loi interdit à l'importateur de fournir les informations visées aux points 1 à 5 ci-dessus.

107. Ces informations pourraient être fournies au moyen de questionnaires structurés que l'importateur remplirait et signerait et seraient renforcées par l'obligation contractuelle faite à l'importateur de déclarer, dans un délai déterminé, toute modification éventuelle à ces informations, comme le veut la pratique en vigueur pour les procédures de due diligence.

108. Conditions d'efficacité:

- L'importateur doit être en mesure de fournir ces informations à l'exportateur, dans la mesure où il les connaît et après avoir mis tout en œuvre pour les obtenir.
- Cette obligation faite à l'importateur est un moyen de faire en sorte que l'exportateur prenne conscience des risques associés au transfert de données vers un pays tiers et les garde à l'esprit. Elle permettra ainsi à l'exportateur de s'abstenir de conclure le contrat, ou si les informations changent après sa conclusion, de remplir son obligation de suspendre le transfert et/ou de résilier le contrat si le droit du pays tiers, les garanties contenues dans l'instrument de transfert visé à l'article 46 du RGPD et toute mesure supplémentaire qu'il pourrait avoir adoptée ne peuvent plus garantir un niveau de protection essentiellement équivalent à celui garanti dans l'EEE. Cette obligation ne peut toutefois justifier la divulgation des données à

[93] La durée de la période devrait dépendre du risque pour les droits et libertés des personnes concernées dont les données font l'objet du transfert en question – par exemple, l'année précédant la clôture de l'instrument d'exportation des données avec l'exportateur.

[94] Le respect de cette obligation n'équivaut pas à offrir un niveau de protection adéquat. En outre, toute divulgation inappropriée qui s'est effectivement produite implique la mise en œuvre de mesures supplémentaires.

caractère personnel par l'importateur, ni faire naître l'attente qu'il n'y aura plus d'autres demandes d'accès.

***

109. L'exportateur pourrait également ajouter des clauses par lesquelles l'importateur certifie: 1) qu'il n'a pas créé intentionnellement de portes dérobées ou des programmations similaires pouvant servir à accéder au système et/ou aux données à caractère personnel; 2) qu'il n'a pas créé ou modifié intentionnellement ses processus opérationnels de manière à faciliter l'accès aux systèmes ou aux données à caractère personnel; et 3) que le droit national ou la politique gouvernementale n'impose pas à l'importateur de créer ou de maintenir des portes dérobées ou de faciliter l'accès aux données à caractère personnel ou aux systèmes ou de détenir ou transmettre la clé de chiffrement[95].

110. Conditions d'efficacité:

- L'existence d'une législation ou de politiques gouvernementales empêchant les importateurs de divulguer ces informations peut rendre cette clause inopérante. L'importateur ne sera donc pas en mesure de conclure le contrat ou devra informer l'exportateur de son incapacité à continuer de respecter ses engagements contractuels.
- Le contrat doit inclure des pénalités et/ou la possibilité pour l'exportateur de résilier le contrat à brève échéance dans les cas où l'importateur ne révèle pas l'existence d'une porte dérobée ou d'une programmation similaire, de processus opérationnels manipulés ou de toute exigence de mettre en œuvre l'un de ces procédés ou n'informe pas immédiatement l'exportateur dès qu'il a connaissance de leur existence.
- lorsque l'importateur de données a divulgué des données à caractère personnel transférées en violation des engagements contenus dans l'instrument de transfert choisi, le contrat peut également prévoir une indemnisation à verser par l'importateur à la personne concernée pour tout préjudice matériel et moral subi.

***

111. L'exportateur pourrait renforcer son pouvoir de réaliser des audits[96] ou des inspections des installations de traitement des données de l'importateur, sur place et/ou à distance, afin de vérifier si des données ont été divulguées aux autorités publiques et dans quelles conditions (accès n'allant pas au-delà de ce qui est nécessaire et proportionné dans une société démocratique), par exemple en prévoyant un préavis court et des mécanismes garantissant l'intervention rapide d'organismes d'inspection et renforçant l'autonomie de l'exportateur dans le choix des organismes d'inspection.

112. Conditions d'efficacité:

[95] Cette clause est importante pour garantir un niveau adéquat de protection des données à caractère personnel transférées et devrait généralement être exigée.

[96] Voir, par exemple, la clause 5, point f), de la décision 2010/87/UE relative aux CCT entre responsables du traitement et sous-traitants; les audits pourraient également être prévus dans un code de conduite ou au moyen d'une certification.

- Pour être pleinement efficace, la portée de l'audit devrait légalement et techniquement couvrir tout traitement des données transmises dans le pays tiers effectué par des sous-traitants ou des sous-traitants ultérieurs de l'importateur.
- Les journaux d'accès et d'autres pistes similaires devraient être inviolables (par exemple, ils devraient être rendus inaltérables par des techniques de chiffrement de pointe, comme le hachage, et également transmis systématiquement à l'exportateur à intervalles réguliers) de sorte que les auditeurs puissent trouver des preuves de la divulgation. Les journaux d'accès et d'autres pistes similaires devraient également opérer une distinction entre les accès dus à des opérations régulières et les accès résultant d'injonctions ou de demandes d'accès.

***

113. Lorsque le droit et la pratique du pays tiers de l'importateur ont été initialement évalués et considérés comme offrant un niveau de protection essentiellement équivalent à celui qui est garanti dans l'UE pour les données transférées par l'exportateur, ce dernier pourrait encore renforcer l'obligation faite à l'importateur de l'informer immédiatement, en cas de changement de la situation, de son incapacité à se conformer à ses engagements contractuels et, partant, de se conformer à la condition imposant un «niveau de protection essentiellement équivalent»[97].

114. Cette incapacité peut résulter de changements intervenus dans la législation ou la pratique du pays tiers[98]. Les clauses pourraient fixer des délais et des procédures précis et stricts pour la suspension rapide du transfert des données et/ou la résiliation du contrat et le renvoi ou l'effacement par l'importateur des données reçues. Garder une trace des demandes reçues, de leur portée et de l'efficacité des mesures adoptées pour les bloquer devrait donner à l'exportateur des indications suffisantes pour exercer son obligation de suspendre le transfert ou d'y mettre fin et/ou de résilier le contrat.

115. Conditions d'efficacité:

- La notification doit intervenir avant que l'accès aux données ne soit accordé. À défaut, lorsque l'exportateur reçoit la notification, les droits de la personne peuvent déjà avoir été violés si la demande est fondée sur une législation du pays tiers qui va au-delà de ce que permet le niveau de protection des données accordé par le droit de l'Union. La notification peut encore servir à empêcher des violations futures et à permettre à l'exportateur de s'acquitter de son obligation de suspendre le transfert de données à caractère personnel vers le pays tiers et/ou de résilier le contrat.
- L'importateur doit surveiller les développements légaux ou politiques susceptibles de l'empêcher de respecter ses obligations et il doit informer immédiatement l'exportateur de

[97] Clause 5, points a) et d), i), de la décision 2010/87/UE relative aux CCT.

[98] Voir C-311/18 (Schrems II), point 139, où la Cour affirme que «si la même clause 5, sous d), i), permet au destinataire du transfert de données à caractère personnel, en cas de législation lui en faisant défense, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière, de ne pas communiquer au responsable du traitement établi dans l'Union une demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, il est néanmoins tenu, conformément à la clause 5, sous a), de l'annexe de la décision CPT d'informer le responsable du traitement de son incapacité de se conformer aux clauses types de protection des données».

ces changements et développements, si possible avant leur mise en œuvre, afin que l'exportateur puisse récupérer les données auprès de l'importateur.

- Les clauses devraient prévoir un mécanisme rapide par lequel l'exportateur de données autorise l'importateur à sécuriser ou à lui renvoyer immédiatement les données, ou si cela n'est pas possible, à les effacer ou à les chiffrer de manière sécurisée sans nécessairement attendre les instructions de l'exportateur dès qu'un seuil spécifique[99] à convenir entre l'exportateur et l'importateur est atteint. L'importateur devrait mettre en place ce mécanisme dès le début du transfert des données et le tester régulièrement afin de s'assurer qu'il peut être exécuté à bref délai.
- D'autres clauses pourraient permettre à l'exportateur de contrôler le respect par l'importateur de ces obligations au moyen d'audits, d'inspections et d'autres mesures de contrôle et de les faire respecter en infligeant des pénalités à l'importateur et/ou en recourant à la capacité de l'exportateur de suspendre le transfert et/ou de résilier le contrat avec effet immédiat.

***

116. Dans la mesure où le droit national du pays tiers le permet, le contrat pourrait renforcer les obligations en prévoyant une méthode «Warrant Canary», par laquelle l'importateur s'engage à publier régulièrement (par exemple au moins toutes les 24 heures) un message signé par cryptographie informant l'exportateur qu'à une date et à une heure donnée, il n'a reçu aucune injonction de divulguer des données à caractère personnel ou autres. L'absence de mise à jour de cette notification indiquera à l'exportateur que l'importateur peut avoir reçu une injonction.

117. Conditions d'efficacité:

- La réglementation du pays tiers doit permettre à l'importateur de fournir cette forme de notification passive à l'exportateur.
- L'exportateur de données doit surveiller automatiquement les notifications de type «Warrant Canary».
- L'importateur doit veiller à ce que sa clé privée de signature du «Warrant Canary» soit conservée en sécurité et qu'il ne puisse pas être contraint d'émettre de fausses notifications «Warrant Canary» par la réglementation du pays tiers. À cet effet, il pourrait être utile que plusieurs signatures de personnes différentes soient utilisées et/ou que le «Warrant Canary» soit émis par une personne se trouvant hors du territoire du pays tiers.

Obligations de prendre des mesures spécifiques

118. L'importateur pourrait s'engager à examiner, en vertu du droit du pays de destination, la légalité de toute injonction de divulguer des données, notamment si elle reste dans le cadre des pouvoirs conférés à l'autorité publique demandeuse, et à contester l'injonction si, après un examen minutieux, il conclut qu'il n'y a pas lieu de le faire en vertu du droit du pays de destination. Lorsqu'il conteste une injonction, l'importateur de données devrait demander des mesures provisoires afin de suspendre les effets de l'injonction jusqu'à ce que le juge ait statué sur le fond. L'importateur serait dans l'obligation de ne pas divulguer les données à caractère personnel demandées jusqu'à ce qu'il soit tenu de le faire en vertu des règles procédurales applicables. Il

[99] Ce seuil devrait garantir que les personnes concernées continuent de bénéficier d'un niveau de protection équivalent à celui garanti au sein de l'EEE.

s'engagerait également à fournir le minimum d'informations autorisé lorsqu'il répond à l'injonction, en se fondant sur une interprétation raisonnable de celle-ci.

119. Conditions d'efficacité:

- L'ordre juridique du pays tiers doit offrir des voies de droit effectives pour contester les injonctions de divulgation des données.
- Cette clause offrira toujours une protection supplémentaire très limitée, étant donné qu'une injonction de divulgation de données peut être licite dans l'ordre juridique du pays tiers, mais que cet ordre juridique peut ne pas répondre aux normes de l'UE. Cette mesure contractuelle devra nécessairement être complétée par d'autres mesures supplémentaires.
- La contestation d'une injonction doit avoir un effet suspensif dans le droit du pays tiers. Dans le cas contraire, les autorités publiques auraient toujours accès aux données des personnes physiques et toute action ultérieure en faveur de la personne concernée aurait pour effet limité de lui permettre de réclamer des dommages et intérêts pour les conséquences négatives découlant de la divulgation des données.
- L'importateur devra être en mesure de documenter et de démontrer à l'exportateur les mesures qu'il a prises, en mettant tout en œuvre pour respecter cet engagement.

***

120. Dans une situation telle que celle décrite ci-dessus, l'importateur pourrait s'engager à informer l'autorité publique demandeuse de l'incompatibilité de l'injonction avec les garanties contenues dans l'instrument de transfert visé à l'article 46 du RGPD[100] et du conflit d'obligations qui en résulte pour l'importateur. L'importateur informerait simultanément et dans les meilleurs délais l'exportateur et/ou l'autorité de contrôle compétente de l'EEE, dans la mesure permise par l'ordre juridique du pays tiers.

121. Conditions d'efficacité:

- Ces informations sur la protection conférée par le droit de l'Union et le conflit d'obligations devraient produire des effets juridiques dans l'ordre juridique du pays tiers, tels qu'un contrôle juridictionnel ou administratif de l'injonction ou de la demande d'accès, l'exigence d'un mandat judiciaire et/ou une suspension temporaire de l'injonction afin d'apporter une protection supplémentaire aux données.
- Le système juridique du pays ne doit pas empêcher l'importateur d'informer l'exportateur ou, à tout le moins, l'autorité de contrôle compétente de l'EEE de l'injonction ou de la demande d'accès qu'il a reçue.
- L'importateur devra être en mesure de documenter et de démontrer à l'exportateur les mesures qu'il a prises, en mettant tout en œuvre pour respecter cet engagement.

[100] À titre d'exemple, les CCT prévoient que le traitement de données, y compris leur transfert, a été et continuera d'être effectué conformément au «*droit applicable en matière de protection des données*». Ce droit est défini comme ««*la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi*». La CJUE confirme que les dispositions du RGPD, lues à la lumière de la Charte des droits fondamentaux de l'Union européenne, font partie de cette législation, voir CJUE, C-311/18 (Schrems II), point 138.

Donner aux personnes concernées les moyens d'exercer leurs droits

122. Le contrat pourrait prévoir que les données à caractère personnel transmises en texte clair dans le cours normal des affaires (y compris dans les cas de soutien) ne peuvent être consultées qu'avec le consentement exprès ou implicite de l'exportateur et/ou de la personne concernée pour un accès spécifique aux données.

123. Conditions d'efficacité:

- Cette clause pourrait être efficace dans les cas où des importateurs reçoivent des autorités publiques des demandes de coopérer sur une base volontaire, par opposition, par exemple, à un accès des autorités publiques aux données se produisant à l'insu de l'importateur de données ou contre sa volonté.
- Dans certains cas, la personne concernée peut ne pas être en mesure de s'opposer à l'accès aux données la concernant ou de donner un consentement répondant à toutes les conditions prévues par le droit de l'Union (libre, spécifique, éclairé et univoque) (dans le cas d'employés, par exemple)[101].
- La réglementation ou les politiques nationales obligeant l'importateur à ne pas divulguer l'injonction d'accès peuvent rendre cette clause inopérante, à moins qu'elle ne puisse être soutenue par des mesures techniques nécessitant l'intervention de l'exportateur ou de la personne concernée pour que les données en texte clair soient accessibles. Ces mesures techniques visant à restreindre l'accès peuvent notamment être envisagées lorsqu'un accès n'est accordé que dans des cas spécifiques de soutien ou de service, mais que les données proprement dites sont stockées dans l'EEE.

***

124. Le contrat pourrait contraindre l'importateur et/ou l'exportateur à informer immédiatement la personne concernée de la demande ou de l'injonction reçue des autorités publiques du pays tiers, ou de l'incapacité de l'importateur à se conformer aux engagements contractuels, afin de permettre à la personne concernée de demander des informations et une voie de recours effective (par exemple en introduisant une réclamation auprès de l'autorité de contrôle compétente et/ou d'une autorité judiciaire et en démontrant sa qualité pour agir devant les juridictions du pays tiers), notamment une indemnisation à verser de la part de l'importateur de données pour tout préjudice matériel et moral subi du fait de la divulgation des données à caractère personnel transférées au moyen de l'instrument de transfert choisi en violation des engagements qu'il contient.

125. Conditions d'efficacité:

- Cette notification pourrait avertir la personne concernée d'accès potentiels des autorités publiques du pays tiers à ses données. Elle pourrait donc permettre à la personne concernée de demander des informations complémentaires à l'exportateur et d'introduire une réclamation auprès de l'autorité de contrôle compétente. Cette clause pourrait également résoudre certaines des difficultés que peut rencontrer une personne pour démontrer sa qualité pour agir devant les juridictions du pays tiers afin de contester l'accès des autorités publiques à ses données et prévoir une réparation.

[101] Article 4, paragraphe 11, du RGPD.

- La réglementation et les politiques nationales peuvent empêcher cette notification à la personne concernée. L'exportateur et l'importateur pourraient néanmoins s'engager à informer la personne concernée dès la levée des restrictions de divulgation des données et à tout mettre en œuvre pour obtenir la levée de l'interdiction de divulgation. À tout le moins, l'exportateur ou l'autorité de contrôle compétente pourrait informer la personne concernée de la suspension ou de la cessation du transfert de ses données à caractère personnel en raison de l'incapacité de l'importateur de se conformer à ses engagements contractuels à la suite de la réception d'une demande d'accès.

***

126. L'exportateur et l'importateur pourraient s'engager contractuellement à aider la personne concernée à exercer ses droits devant la juridiction du pays tiers au moyen de mécanismes de recours ad hoc et d'une assistance juridique.

127. Conditions d'efficacité:

- Certaines réglementations nationales peuvent ne pas autoriser l'importateur de données à fournir ce type d'assistance directement aux personnes concernées, bien qu'elles puissent permettre à l'importateur de données de leur procurer une telle assistance.
- La réglementation et les politiques nationales peuvent imposer des conditions susceptibles de compromettre l'efficacité des mécanismes de recours ad hoc prévus.
- Une assistance juridique pourrait être utile à la personne concernée, en particulier si l'on considère la difficulté et le coût que peuvent représenter pour cette dernière la compréhension du système juridique du pays tiers et les actions en justice menées depuis l'étranger, potentiellement dans une langue étrangère. Toutefois, cette clause apportera toujours une protection supplémentaire limitée, étant donné que la fourniture d'une assistance et de conseils juridiques aux personnes concernées ne saurait, à elle seule, remédier au fait que l'ordre juridique d'un pays tiers ne prévoit pas un niveau de protection essentiellement équivalent à celui garanti au sein de l'EEE. Cette mesure contractuelle devra nécessairement être complétée par d'autres mesures supplémentaires.
- Cette mesure supplémentaire ne serait efficace que si le droit du pays tiers prévoit un recours devant ses juridictions nationales ou s'il existe un mécanisme de recours ad hoc, notamment contre des mesures de surveillance.

2.3 Mesures organisationnelles

128. Les mesures organisationnelles supplémentaires peuvent consister en des politiques internes, des méthodes organisationnelles et des normes que les responsables du traitement et les sous-traitants pourraient s'appliquer à eux-mêmes et imposer aux importateurs de pays tiers. Elles peuvent contribuer à garantir la cohérence de la protection des données à caractère personnel tout au long du cycle du traitement. Les mesures organisationnelles peuvent également améliorer la prise de conscience des exportateurs quant aux risques et aux tentatives d'accès aux données dans des pays tiers ainsi que leur capacité à réagir. La sélection et la mise en œuvre d'une ou de plusieurs de ces mesures ne garantissent pas nécessairement et systématiquement que le transfert satisfera à la norme d'équivalence essentielle établie par le droit de l'Union. En fonction des circonstances particulières du transfert et de l'évaluation de la législation du pays tiers, des mesures organisationnelles sont nécessaires pour compléter les mesures contractuelles et/ou techniques afin de garantir un niveau de protection des données à caractère personnel essentiellement équivalent à celui garanti au sein de l'EEE.

129. L'évaluation des mesures les plus appropriées doit se faire au cas par cas, en gardant à l'esprit la nécessité pour les responsables du traitement et leurs sous-traitants de respecter le principe de responsabilité. Le comité européen de la protection des données présente ci-après quelques exemples de mesures organisationnelles que les exportateurs peuvent mettre en œuvre, mais cette liste n'est pas exhaustive et d'autres mesures peuvent également être appropriées.

Politiques internes de gouvernance des transferts, en particulier avec des groupes d'entreprises

130. Adoption de politiques internes adéquates prévoyant une répartition claire des responsabilités en matière de transfert de données, de canaux de signalement et de procédures opérationnelles standard en cas de demandes formelles ou informelles d'accès aux données émanant d'autorités publiques. Dans le cas de transferts entre groupes d'entreprises en particulier, ces politiques peuvent notamment inclure la désignation d'une équipe spécifique, composée de spécialistes de l'informatique et de la législation en matière de protection des données et de protection de la vie privée, pour traiter les demandes impliquant des transferts de données à caractère personnel depuis l'EEE, la notification à l'encadrement supérieur juridique et à la direction générale ainsi qu'à l'exportateur de données dès réception de ces demandes, les étapes de la procédure visant à contester les demandes disproportionnées ou illicites et la fourniture d'informations transparentes aux personnes concernées.

131. Des procédures de formation spécifiques pour le personnel chargé de la gestion des demandes d'accès des autorités publiques aux données à caractère personnel devraient être élaborées et régulièrement mises à jour pour refléter l'évolution de la législation et de la jurisprudence dans le pays tiers et dans l'EEE. Les procédures de formation devraient inclure les exigences du droit de l'Union en matière d'accès des autorités publiques aux données à caractère personnel, en particulier en vertu de l'article 52, paragraphe 1, de la Charte des droits fondamentaux. Il conviendrait de sensibiliser davantage le personnel, notamment en évaluant des exemples pratiques de demandes d'accès des autorités publiques et en appliquant la norme découlant de l'article 52, paragraphe 1, de la Charte des droits fondamentaux à ces exemples pratiques. Cette formation devrait tenir compte de la situation spécifique de l'importateur de données,

notamment de la législation et la réglementation du pays tiers auxquelles celui-ci est soumis, et devrait être élaborée, dans la mesure du possible, en collaboration avec l'exportateur de données.

132. Conditions d'efficacité:

- Ces politiques ne peuvent être envisagées que dans les cas où la demande des autorités publiques du pays tiers est compatible avec le droit de l'Union[102]. Lorsque la demande est incompatible, ces politiques ne suffiraient pas à garantir un niveau de protection équivalent des données à caractère personnel et, comme indiqué plus haut, les transferts doivent être interrompus ou des mesures supplémentaires appropriées doivent être mises en place pour éviter l'accès aux données.

Mesures de transparence et de responsabilité

133. Documenter et enregistrer les demandes d'accès reçues des autorités publiques et la réponse fournie, ainsi que le raisonnement juridique et les acteurs concernés (par exemple, si l'exportateur a été notifié, quelle a été sa réponse, l'évaluation de l'équipe chargée de traiter ces demandes, etc.). Ces registres devraient être mis à la disposition de l'exportateur de données, qui devrait lui-même les fournir aux personnes concernées.

134. Conditions d'efficacité:

- La législation nationale du pays tiers peut empêcher la divulgation des demandes ou des informations importantes de celles-ci et, partant, rendre cette mesure inopérante. L'importateur de données devrait informer l'exportateur de son incapacité à fournir ces documents et registres afin de donner à ce dernier la possibilité d'interrompre les transferts si cette incapacité empêche de fournir un niveau de protection adéquat.

***

135. Publication régulière de rapports sur la transparence ou de résumés des demandes d'accès aux données formulées par le gouvernement et le type de réponse fournie, dans la mesure où la publication est autorisée par le droit national.

136. Conditions d'efficacité:

- Les informations fournies devraient être pertinentes, claires et aussi détaillées que possible. La législation nationale du pays tiers peut interdire la divulgation d'informations détaillées. En pareil cas, l'importateur de données devrait mettre tout en œuvre pour publier des informations statistiques ou un type similaire d'informations agrégées.

Méthodes organisationnelles et mesures de minimisation des données

137. Les exigences organisationnelles qui existent déjà en vertu du principe de responsabilité, telles que l'adoption de politiques strictes et détaillées concernant l'accès aux données et la confidentialité ou encore les bonnes pratiques, basées sur l'application stricte du besoin d'en connaître, contrôlées par des audits réguliers et appliquées au moyen de mesures disciplinaires,

[102] Voir C-362/14 («Schrems I»), point 94, et C-311/18 (Schrems II), points 168, 174, 175 et 176.

peuvent également être utiles dans le cadre d'un transfert. La minimisation des données devrait être envisagée afin de limiter l'exposition des données à caractère personnel à un accès non autorisé. À titre d'exemple, dans certains cas, il pourrait ne pas être nécessaire de transférer certaines données (par exemple, en cas d'accès à distance aux données de l'EEE, comme dans les cas de soutien, lorsqu'un accès restreint est accordé au lieu d'un accès total ou lorsque la fourniture d'un service nécessite uniquement le transfert d'un ensemble limité de données, et non d'une base de données complète).

138. Conditions d'efficacité:

- Des audits réguliers et des mesures disciplinaires solides devraient être mis en place afin de contrôler et de faire respecter les mesures de minimisation des données, y compris dans le cadre d'un transfert.
- L'exportateur de données procède à une évaluation des données à caractère personnel en sa possession avant que le transfert n'ait lieu afin de détecter les ensembles de données qui ne sont pas nécessaires aux fins du transfert et qui ne seront donc pas partagés avec l'importateur de données.
- Les mesures de minimisation des données devraient être assorties de mesures techniques, de manière à garantir que les données ne font pas l'objet d'un accès non autorisé. À titre d'exemple, la mise en œuvre de mécanismes de calcul multipartites sécurisés et la diffusion d'ensembles de données chiffrées entre différentes entités de confiance peuvent empêcher, dès la conception, qu'un accès unilatéral n'aboutisse à la divulgation de données identifiables.

***

139. Élaboration de bonnes pratiques visant à faire intervenir le délégué à la protection des données, s'il en existe un, et les services juridiques et d'audit interne et à leur donner accès aux informations relatives aux questions liées aux transferts internationaux de données à caractère personnel, et ce, de manière appropriée et en temps utile.

140. Conditions d'efficacité:

- Le délégué à la protection des données, s'il en existe un, et l'équipe juridique et chargée de l'audit interne reçoivent toutes les informations pertinentes avant le transfert puis sont consultés sur la nécessité du transfert et les garanties supplémentaires, le cas échéant.
- Les informations pertinentes devraient inclure, par exemple, l'évaluation de la nécessité du transfert des données à caractère personnel visées, un aperçu de la législation applicable du pays tiers et les garanties que l'importateur s'engage à mettre en œuvre.

Adoption de normes et de bonnes pratiques

141. Adoption de politiques strictes en matière de sécurité et de confidentialité des données, fondées sur une certification de l'UE, des codes de conduite européens ou des normes internationales (par exemple, des normes ISO) et des bonnes pratiques (par exemple, ENISA), en tenant dûment compte de l'état de la technique et en fonction des risques liés aux catégories de données traitées.

Autres

142. Adoption et contrôle régulier des politiques internes afin d'évaluer l'adéquation des mesures complémentaires mises en œuvre et d'identifier et de mettre en place des solutions supplémentaires ou de remplacement, si nécessaire, en vue de garantir le maintien d'un niveau de protection des données à caractère personnel transférées essentiellement équivalent à celui garanti au sein de l'EEE.

***

143. Engagements de l'importateur de données de ne procéder à aucun transfert de données à caractère personnel au sein du même pays tiers ou d'autres pays tiers, ou d'interrompre les transferts en cours lorsqu'un niveau de protection des données à caractère personnel essentiellement équivalent à celui accordé au sein de l'EEE ne peut pas être garanti dans le pays tiers[103].

[103] C-311/18 (Schrems II), points 135 et 137.

ANNEXE 3: SOURCES D'INFORMATION POSSIBLES AUX FINS DE L'ÉVALUATION D'UN PAYS TIERS

144. L'importateur de données devrait être en mesure de fournir à l'exportateur les sources et les informations pertinentes relatives au pays tiers dans lequel il est établi, y compris la législation et les pratiques applicables à l'importateur et aux données transférées. L'exportateur et l'importateur peuvent se référer à plusieurs sources d'information, telles que celles énumérées de manière non exhaustive ci-après et présentées par ordre de préférence:

- jurisprudence de la Cour de justice de l'Union européenne (CJUE) et de la Cour européenne des droits de l'homme (CEDH)[104], citée dans les recommandations sur les garanties essentielles européennes[105];
- décisions d'adéquation dans le pays de destination si le transfert repose sur une base juridique différente[106];
- résolutions et rapports d'organisations intergouvernementales, telles que le Conseil de l'Europe[107], d'autres organismes régionaux[108], et des organes et agences des Nations unies (par exemple, le Conseil des droits de l'homme des Nations unies[109], le Comité des droits de l'homme[110]);
- rapports et analyses des réseaux réglementaires compétents, tels que la Global Privacy Assembly (GPA)[111];
- jurisprudences nationales ou décisions prises par des autorités judiciaires ou administratives indépendantes de pays tiers en matière de respect de la vie privée et de protection des données;
- rapports d'organes de contrôle indépendants ou d'organes parlementaires;
- rapports fondés sur l'expérience pratique de demandes antérieures de divulgation émanant d'autorités publiques, ou sur l'absence de telles demandes, émanant d'entités actives dans le même secteur que l'importateur;
- «Warrant Canaries» d'autres entités traitant des données dans le même domaine que l'importateur;

---

[104] Voir la fiche thématique de la jurisprudence de la CEDH sur la surveillance de masse: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] C-311/18 (Schrems II), point 141; voir décisions d'adéquation à l'adresse: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108]Voir, par exemple, rapports par pays de la Commission interaméricaine des droits de l'homme (CIDH), https://www.oas.org/en/iachr/reports/country.asp.

[109] Voir: https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] Voir: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] Voir, par exemple, https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- rapports établis ou commandés par les chambres de commerce, les entreprises, les associations professionnelles et commerciales, les instances diplomatiques, commerciales et d'investissement du gouvernement de l'exportateur ou d'autres pays tiers exportant vers le pays tiers vers lequel le transfert est effectué;
- rapports d'universités et d'organisations de la société civile (ONG, par exemple).
- rapports de fournisseurs privés de renseignements commerciaux sur les risques financiers, réglementaires et pour la réputation des entreprises;
- «Warrant Canaries» de l'importateur proprement dit[112];
- rapports de transparence, à condition qu'ils mentionnent expressément le fait qu'aucune demande d'accès n'a été reçue. Les rapports de transparence qui ne mentionnent pas ce point ne seraient pas considérés comme une preuve suffisante, étant donné qu'ils sont le plus souvent axés sur les demandes d'accès émanant des autorités répressives et ne fournissent des chiffres que sur cet aspect tout en n'évoquant pas les demandes d'accès reçues à des fins de sécurité nationale. Cela ne signifie pas qu'aucune demande d'accès n'a été reçue, mais plutôt que ces informations ne peuvent pas être partagées[113];
- déclarations ou registres internes de l'importateur indiquant expressément qu'aucune demande d'accès n'a été reçue pendant une période suffisamment longue; avec une préférence pour les déclarations et registres engageant la responsabilité de l'importateur et/ou émis par des positions internes dotées d'une certaine autonomie, tels que les auditeurs internes, les DPD, etc.[114].

[112] Voir les conditions de la prise en compte de l'expérience pratique avérée de l'importateur en matière de demandes d'accès antérieures reçues des autorités publiques du pays tiers au paragraphe 47.
[113] *Ibid.*
[114] *Ibid.*