GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

18/FR

WP 254 rev.01

Groupe de travail «Article 29»

Critères de référence pour l'adéquation

Adoptés le 28 novembre 2017

Version révisée et adoptée le 6 février 2018

Introduction

Le groupe de travail des autorités européennes chargées de la protection des données[1] (le GT29) a publié précédemment un document de travail sur les transferts de données personnelles vers des pays tiers (WP 12)[2]. Après le remplacement de la directive par le règlement général sur la protection des données (RGPD)[3], le GT29 réexamine le WP 12, son précédent document d'orientation, afin de le mettre à jour dans le cadre de la nouvelle législation et de la jurisprudence récente de la Cour européenne de justice[4].

Le présent document de travail vise à mettre à jour le chapitre premier du WP 12 relatif à la question essentielle du niveau adéquat de protection des données dans un pays tiers, un territoire ou un ou plusieurs secteurs déterminés au sein de ce pays tiers ou d'une organisation internationale (ci-après «pays tiers ou organisations internationales»). Ce document sera continuellement révisé et mis à jour si nécessaire dans les années à venir, en fonction de l'expérience concrète acquise dans le cadre de l'application du RGPD. Les chapitres 2 (*Application concrète de l'approche aux pays ayant ratifié la convention 108*) et 3 (*Application de l'approche aux codes d'autoréglementation sectoriels*) du document WP 12 devraient être mis à jour à un stade ultérieur.

Le présent document de travail porte uniquement sur des décisions d'adéquation, qui sont des actes d'exécution[5] de la Commission européenne, conformément à l'article 45 du RGPD. D'autres aspects des transferts de données à caractère personnel vers des pays tiers et des organisations internationales seront examinés dans de prochains documents de travail qui seront publiés séparément (BCR, dérogations).

Le présent document entend donner à la Commission européenne et au GT29 des orientations dans le cadre du RGPD pour évaluer le niveau de protection des données dans les pays tiers et les organisations internationales en instaurant des principes essentiels de protection des données qui doivent être présents dans le cadre juridique d'un pays tiers ou dans une organisation internationale afin de garantir l'équivalence fondamentale avec le cadre de l'Union. En outre, il peut donner des orientations à des pays tiers et à des organisations internationales souhaitant obtenir l'adéquation. Toutefois, les principes énoncés dans le présent document de travail ne s'adressent pas directement aux responsables du traitement des données ou aux sous-traitants.

Le présent document est composé de quatre chapitres:

Chapitre 1: Informations générales relatives au concept d'adéquation

Chapitre 2: Aspects procéduraux des décisions d'adéquation dans le cadre du RGPD

Chapitre 3: Principes généraux en matière de protection des données. Ce chapitre comprend les principes généraux fondamentaux en matière de protection des données visant à garantir que le niveau de protection des données dans un pays tiers ou une organisation internationale est substantiellement équivalent à celui établi par la législation européenne.

Chapitre 4: Garanties essentielles en matière d'application de la loi et d'accès pour raison de sécurité nationale afin de limiter les ingérences dans les droits fondamentaux. Ce chapitre comprend les garanties essentielles en matière d'application de la loi et d'accès pour raison de sécurité nationale à la suite de l'arrêt Schrems de la CJUE en 2015 et sur la base du document de travail du GT29 relatif aux garanties essentielles adopté en 2016.

---

[1] Tel qu'établi en vertu de l'article 29 de la directive 95/46/CE relative à la protection des données.

2 WP 12, «Document de travail: Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données» adopté par le groupe de travail le 24 juillet 1998.

3 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) (Texte présentant de l'intérêt pour l'EEE).

4 Y compris l'affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner, 6 octobre 2015.

[5] Voir les articles pertinents 45, paragraphe 3, et 93, paragraphe 2, du RGPD pour de plus amples informations sur les actes d'exécution.

Chapitre 1: Informations générales relatives au concept d'adéquation

L'article 45, paragraphe 1, du RGPD énonce le principe selon lequel les transferts de données vers un pays tiers ou à une organisation internationale ont lieu uniquement si le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans de ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat.

Ce concept de «niveau de protection adéquat», qui existait déjà dans le cadre de la directive 95/46, a été renforcé par la CJUE. À ce stade, il importe de rappeler la norme définie par la CJUE dans l'arrêt Schrems, à savoir que si le «*niveau de protection*» dans le pays tiers doit être «*substantiellement équivalent*» à celui garanti dans l'UE, «*les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de [l'Union]*»[6]. Par conséquent, l'objectif n'est pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles – fondamentales de cette législation.

L'objectif des décisions d'adéquation de la Commission européenne est de confirmer officiellement, avec des effets contraignants sur les États membres[7], que le niveau de protection des données dans un pays tiers ou une organisation internationale est substantiellement équivalent au niveau de protection des données dans l'Union européenne[8]. L'adéquation peut être obtenue en combinant les droits des personnes concernées et les obligations de ceux qui traitent les données ou qui exercent un contrôle sur ce traitement et la supervision par des organes indépendants. Toutefois, les règles sur la protection des données ne sont efficaces que si elles sont applicables et suivies en pratique. Il convient donc de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers ou une organisation internationale, mais également du système mis en place afin de garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données.

L'article 45, paragraphe 2, du RGPD définit les éléments dont la Commission européenne doit tenir compte lorsqu'elle évalue le caractère adéquat du niveau de protection dans un pays tiers ou une organisation internationale.

La Commission doit notamment prendre en considération l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes et les engagements internationaux pris par le pays tiers ou l'organisation internationale.

Il apparaît donc clairement que toute analyse pertinente du niveau de protection adéquat doit comprendre les deux éléments essentiels suivants: le contenu des règles applicables et les moyens de garantir leur application effective. Il incombe à la Commission européenne de vérifier – régulièrement – que les règles en vigueur sont effectives dans la pratique.

Les principes fondamentaux touchant au «contenu» des règles sur la protection des données et aux exigences en matière de «procédure/d'application», qui pourraient être considérés comme une condition minimale pour que l'on puisse parler d'un niveau de protection adéquat, sont tirés de la charte des droits fondamentaux de l'Union et du RGPD. En outre, il convient de tenir également compte d'autres accords internationaux sur la protection des données, notamment la convention 108[9].

Il faut également tenir compte du cadre juridique prévu pour l'accès des autorités publiques aux données à caractère personnel. Des orientations supplémentaires à ce sujet sont données dans le document de travail 237 (à savoir le document sur les garanties essentielles)[10] sur les garanties dans le cadre de la surveillance.

---

[6] Affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner, 6 octobre 2015 (points 73, 74).

[7] Article 288, paragraphe 2, TFUE.

[8] Affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner, 6 octobre 2015 (point 52).

9 Considérant 105 du RGPD.

[10] Document de travail 01/2016 sur la justification des ingérences dans les droits fondamentaux à la vie privée et à la protection des données découlant de mesures de surveillance lors du transfert de données à caractère personnel (garanties essentielles européennes), 16/EN WP 237, 13 avril 2016.

Des dispositions générales relatives à la protection des données et à la vie privée dans le pays tiers ne suffisent pas. Au contraire, il convient d'inclure dans le cadre juridique du pays tiers ou de l'organisation internationale des dispositions spécifiques répondant aux besoins concrets d'aspects pertinents, d'un point de vue pratique, du droit à la protection des données. Ces dispositions doivent être applicables.

Chapitre 2: Aspects procéduraux des constats d'adéquation dans le cadre du RGPD

Pour s'acquitter de la mission qui lui incombe de conseiller la Commission européenne conformément à l'article 70, paragraphe 1, point s), du RGPD, le comité européen de la protection des données devrait disposer de tous les documents nécessaires, y compris la correspondance pertinente et les conclusions de la Commission européenne. Si le cadre juridique est complexe, les documents devraient comprendre tout rapport relatif au niveau de protection des données du pays tiers ou de l'organisation internationale. Dans tous les cas, les informations fournies par la Commission européenne devraient être exhaustives et permettre au comité de procéder à sa propre évaluation concernant le niveau de protection des données dans le pays tiers. Le comité rendra en temps voulu un avis sur les conclusions de la Commission européenne et, le cas échéant, recensera les insuffisances du cadre d'adéquation. Le comité s'efforcera également de proposer des modifications ou des amendements pour remédier aux éventuelles insuffisances.

Conformément à l'article 45, paragraphe 4, du RGPD, il incombe à la Commission européenne de suivre – de manière permanente – les évolutions qui pourraient porter atteinte au fonctionnement d'une décision d'adéquation.

L'article 45, paragraphe 3, du RGPD prévoit qu'un examen périodique doit avoir lieu au moins tous les quatre ans. Il s'agit toutefois d'un calendrier général qui doit être adapté à chaque pays tiers ou organisation internationale pour lequel ou laquelle il existe une décision d'adéquation. En fonction des circonstances particulières, un cycle d'examen plus court pourrait être justifié. De même, des incidents ou d'autres informations sur le cadre juridique ou des modifications de ce dernier dans le pays tiers ou l'organisation internationale en question pourraient nécessiter de procéder à un examen plus tôt. Il semble également nécessaire de procéder assez rapidement à un premier examen d'une décision d'adéquation totalement nouvelle et d'adapter progressivement le cycle d'examen en fonction du résultat.

Compte tenu du mandat consistant à rendre un avis à la Commission européenne sur la question de savoir si le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers ou une organisation internationale n'assure plus le niveau de protection adéquat, le comité doit, en temps voulu, recevoir des informations pertinentes concernant le suivi des évolutions importantes dans ce pays tiers ou l'organisation internationale par la Commission européenne. Par conséquent, le comité devrait être tenu informé de toute procédure d'examen et mission d'examen dans le pays tiers ou l'organisation internationale. Le comité souhaiterait être invité à participer à ces procédures et missions d'examen.

Il convient également de souligner qu'en vertu de l'article 45, paragraphe 5, du RGPD, la Commission européenne a le droit d'abroger, de modifier ou de suspendre les décisions d'adéquation en vigueur. La procédure d'abrogation, de modification ou de suspension devrait alors prévoir la participation du comité en sollicitant son avis conformément à l'article 70, paragraphe 1, point s).

En outre, ainsi que le reconnaît désormais l'article 58, paragraphe 5, du RGPD et conformément à l'arrêt Schrems de la CJUE, les autorités de protection des données doivent pouvoir ester en justice si elles constatent qu'une action intentée par une personne contre une décision d'adéquation est fondée: «*À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.*»[11]

[11] Affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner, 6 octobre 2015 (point 65).

Chapitre 3: Principes généraux en matière de protection des données visant à garantir que le niveau de protection dans un pays tiers, un territoire ou un ou plusieurs secteurs déterminés au sein de ce pays tiers ou d'une organisation internationale est substantiellement équivalent à celui garanti par la législation européenne

Le système d'un pays tiers ou d'une organisation internationale doit comporter les principes et mécanismes fondamentaux suivants touchant au contenu des règles sur la protection des données et aux exigences en matière de procédure/d'application:

A. Principes touchant au contenu:

1) Notions

Des notions et/ou principes fondamentaux en matière de protection des données devraient exister. Ils ne doivent pas reprendre la terminologie du RGPD, mais devraient refléter les notions ancrées dans la législation européenne relative à la protection des données et être cohérents avec ces dernières. À titre d'exemple, le RGPD inclut les notions importantes suivantes: «données à caractère personnel», «traitement de données à caractère personnel», «responsable du traitement», «sous-traitant», «destinataire» et «données sensibles».

2) Fondements du traitement loyal et licite pour des finalités légitimes

Les données doivent être traitées de manière loyale, licite et légitime.

Les fondements légitimes au titre desquelles des données à caractère personnel peuvent être traitées loyalement, licitement et légitimement, devraient être définis de façon suffisamment claire. Le cadre européen reconnaît plusieurs de ces fondements légitimes, notamment des dispositions de la législation nationale, le consentement de la personne concernée, l'exécution d'un contrat ou l'intérêt légitime du responsable du traitement ou d'une tierce partie qui ne l'emporte pas sur les intérêts de la personne concernée.

3) Le principe de limitation de la finalité

Les données devraient être traitées dans un but précis et être ensuite utilisées uniquement dans la mesure où cela n'est pas incompatible avec la finalité du traitement.

4) Le principe de qualité et de proportionnalité des données

Les données à caractère personnel doivent être exactes et, au besoin, actualisées. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

5) Le principe de conservation des données

En règle générale, les données à caractère personnel ne devraient pas être conservées plus longtemps que ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

6) Le principe de sécurité et de confidentialité

Toute entité procédant au traitement de données à caractère personnel doit veiller à ce que les données soient traitées de façon à garantir la sécurité des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine

accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. Le niveau de sécurité devrait tenir compte de l'état des connaissances et des coûts correspondants.

7) Le principe de transparence

Chaque personne devrait être informée de façon claire, aisément accessible, concise, transparente et compréhensible des principaux éléments du traitement des données à caractère personnel la concernant. Ces informations devraient comprendre la finalité du traitement, l'identité du responsable du traitement, les droits mis à sa disposition et d'autres informations dans la mesure où celles-ci sont nécessaires pour garantir un traitement loyal. Dans certaines conditions, il peut y avoir des exceptions à ce droit à l'information, notamment pour protéger des enquêtes criminelles, la sécurité nationale, l'indépendance de la justice et des procédures judiciaires ou d'autres objectifs importants d'intérêt public général, conformément à l'article 23 du RGPD.

8) Le droit d'accès, de rectification, d'effacement et d'opposition

La personne concernée devrait avoir le droit d'obtenir la confirmation que les données la concernant sont ou ne sont pas traitées et avoir accès à ses données, y compris obtenir une copie de toutes les données la concernant qui sont traitées.

La personne concernée devrait avoir le droit d'obtenir la rectification des données la concernant, le cas échéant, pour des raisons spécifiques, notamment si elles s'avèrent inexactes ou incomplètes, et l'effacement de ses données à caractère personnel si, par exemple, leur traitement n'est plus nécessaire ou est illicite.

La personne concernée devrait avoir le droit de s'opposer, pour des raisons légitimes impérieuses tenant à sa situation particulière, à tout moment, au traitement des données la concernant selon des conditions spécifiques définies dans le cadre juridique du pays tiers. Dans le cadre du RGPD, par exemple, ces conditions correspondent notamment aux cas où le traitement est nécessaire pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

L'exercice de ces droits ne devrait pas être excessivement lourd pour la personne concernée. Ces droits pourraient éventuellement être limités, notamment pour protéger des enquêtes criminelles, la sécurité nationale, l'indépendance de la justice et des procédures judiciaires ou d'autres objectifs importants d'intérêt public général conformément à l'article 23 du RGPD.

9) Restrictions concernant les transferts ultérieurs

Les transferts ultérieurs des données à caractère personnel par le destinataire initial du transfert original de données ne devraient être autorisés que si le nouveau destinataire (c'est-à-dire le destinataire du transfert ultérieur) est également soumis à des règles (y compris des règles contractuelles) assurant un niveau de protection adéquat et suivant les instructions pertinentes lors du traitement des données pour le compte du responsable du traitement. Le niveau de protection des personnes physiques dont les données sont transférées ne doit pas être compromis par le transfert ultérieur. Le destinataire initial des données transférées depuis l'UE doit s'assurer que les garanties appropriées sont prévues pour les transferts ultérieurs de données en l'absence d'une décision d'adéquation. Ces transferts ultérieurs de données ne devraient avoir lieu qu'à des fins limitées et précises et tant que ce traitement a un fondement juridique.

B. <u>Exemples de principes supplémentaires touchant au contenu à appliquer à certains types de traitement:</u>

1) Catégories particulières de données

Des garanties spécifiques devraient exister concernant des «catégories particulières de données»[12]. Ces catégories devraient correspondre à celles énoncées aux articles 9 et 10 du RGPD. Cette protection devrait être mise en place dans le cadre d'exigences plus strictes concernant le traitement des données, prévoyant notamment que la personne concernée donne son consentement explicite au traitement ou dans le cadre de mesures de sécurité supplémentaires.

2) Démarchage

Si les données sont traitées à des fins de démarchage, la personne concernée devrait avoir le droit de s'opposer à tout moment, sans frais, au traitement des données la concernant à ces fins.

3) Prise de décision automatisée et profilage

Les décisions prises sur le seul fondement d'un traitement automatisé (prise de décision individuelle automatisée), y compris le profilage, qui produisent des effets juridiques ou affectent la personne concernée de manière significative ne sont possibles que dans certaines conditions définies dans le cadre juridique du pays tiers. Dans le cadre européen, ces conditions correspondent notamment à la nécessité d'obtenir le consentement explicite de la personne concernée ou à la nécessité de cette décision pour la conclusion d'un contrat. Si la décision ne respecte pas les conditions telles qu'elles sont définies dans le cadre juridique du pays tiers, la personne concernée devrait avoir le droit de ne pas être soumise à la décision. La législation du pays tiers devrait, dans tous les cas, prévoir les garanties nécessaires, notamment le droit d'être informé des raisons particulières sous-tendant la décision et la logique concernée, de corriger des informations inexactes ou incomplètes et de contester la décision si elle est adoptée sur une base factuelle incorrecte.

C. <u>Mécanismes en matière de procédure et d'application:</u>

Bien que les moyens auxquels le pays tiers a recours pour assurer un niveau de protection adéquat puissent être différents de ceux mis en œuvre au sein de l'Union européenne[13], un système cohérent avec le système européen doit se caractériser par l'existence des éléments suivants:

1) Autorité de contrôle indépendante compétente

Une ou plusieurs autorités de contrôle indépendantes, chargées de surveiller et d'assurer le respect des dispositions relatives à la protection des données et à la vie privée dans le pays tiers et de les faire appliquer, devraient exister. L'autorité de contrôle exerce en toute indépendance et impartialité les fonctions et les pouvoirs dont elle est investie et, ce faisant, ni ne sollicite ni n'accepte d'instructions. Dans ce contexte, l'autorité de contrôle devrait se voir confier tous les pouvoirs et missions nécessaires et disponibles pour assurer le respect des droits en matière de protection des données et favoriser la sensibilisation. Il convient de prendre également en considération les effectifs et le budget de l'autorité de contrôle. L'autorité de contrôle devrait également être en mesure de mener, de sa propre initiative, des enquêtes.

2) Le système de protection des données doit assurer un niveau de conformité satisfaisant

[12] Ces catégories particulières sont également appelées «données sensibles» au considérant 10 du RGPD.
[13] Affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner, 6 octobre 2015, point 74.

Le système d'un pays tiers devrait garantir un niveau élevé de responsabilité et de connaissance, parmi les responsables du traitement et ceux procédant au traitement de données à caractère personnel pour leur compte, de leurs obligations, missions et responsabilités et, parmi les personnes concernées, de leurs droits et des moyens de les exercer. L'existence de sanctions effectives et dissuasives peut jouer un rôle important pour garantir le respect des règles, tout comme les systèmes de vérification directe par les autorités, les auditeurs ou des responsables indépendants de la protection des données.

3) Responsabilité

Le cadre de protection des données d'un pays tiers devrait obliger les responsables du traitement et/ou ceux procédant au traitement de données à caractère personnel pour leur compte à le respecter et à être en mesure de démontrer qu'il est respecté, notamment auprès de l'autorité de contrôle. Ces mesures peuvent notamment consister en des analyses d'impact de la protection des données, la tenue de registres ou de journaux des activités de traitement des données pour une période appropriée, la désignation d'un responsable de la protection des données ou la protection des données dès la conception et par défaut.

4) Le système de protection des données doit soutenir et aider les personnes concernées dans l'exercice de leurs droits et fournir des mécanismes de recours appropriés

La personne devrait être en mesure d'exercer des voies de recours pour faire valoir ses droits rapidement et effectivement, sans coût prohibitif, et pour assurer le respect des règles. Pour ce faire, il convient de mettre en place des mécanismes de contrôle permettant d'enquêter sur les plaintes de manière indépendante et de détecter et de sanctionner en pratique toute infraction du droit à la protection des données et au respect de la vie privée.

Si les règles ne sont pas respectées, la personne concernée devrait également disposer de recours judiciaires et administratifs effectifs, y compris pour la réparation du préjudice subi en raison du traitement illicite des données à caractère personnel la concernant. Il s'agit d'un élément essentiel qui nécessite un système d'arbitrage indépendant permettant de réparer le dommage et d'imposer des sanctions le cas échéant.

Chapitre 4: Garanties essentielles dans les pays tiers en matière d'application des lois et d'accès pour raison de sécurité nationale afin de limiter les ingérences dans les droits fondamentaux

Lorsqu'elle évalue le caractère adéquat du niveau de protection, en vertu de l'article 45, paragraphe 2, point a), la Commission doit tenir compte «*de la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation (...)*».

Dans l'arrêt Schrems, la CJUE souligne que «*l'expression "niveau de protection adéquat" doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte*». Même si les moyens auxquels ce pays tiers a recours, à cet égard, peuvent être différents de ceux mis en œuvre au sein de l'Union, ils doivent néanmoins s'avérer, en pratique, effectifs[14].

Dans ce contexte, la Cour souligne également de manière critique que la précédente décision relative à la sphère de sécurité «*ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale*».

Dans son avis WP 237 adopté le 13 avril 2016, le GT29 a défini des garanties essentielles reflétant la jurisprudence de la CJUE et de la CEDH dans le domaine de la surveillance. Si les recommandations formulées dans le WP 237 restent valables et devraient être prises en compte lors de l'évaluation de l'adéquation d'un pays tiers dans le domaine de la surveillance, l'application de ces garanties peut être différente dans les domaines de l'application de la loi et de l'accès aux données pour raison de sécurité nationale. Toutefois, les quatre garanties suivantes doivent être respectées pour que l'accès aux données, que ce soit à des fins de sécurité nationale ou à des fins d'application de la loi, par tous les pays tiers soit considéré comme adéquat:

1) **le traitement devrait reposer sur des règles claires, précises et accessibles (base juridique);**

2) **la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis devraient être démontrées;**

3) **le traitement doit faire l'objet d'un contrôle indépendant;**

4) **les particuliers devraient disposer de voies de recours effectives.**

[14] Affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner, 6 octobre 2015, point 74.