Recommandations 01/2021 sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif

Adoptées le 2 février 2021

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

Historique des versions

Version 1.1	6 juillet 2021	Changement de présentation
Version 1.0	2 février 2021	Adoption des recommandations

Table des matières

Le comité européen de la protection des données,

vu l'article 51, paragraphe 1, point b), de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[1],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LES RECOMMANDATIONS SUIVANTES

1. INTRODUCTION

1. Le groupe de travail «Article 29» (GT29) a publié un document de travail[2] sur les critères de référence pour l'adéquation dans le cadre du règlement général sur la protection des données (RGPD)[3]. Ce document de travail a été approuvé par le comité européen de la protection des données (EDPB) lors de sa première session plénière.

2. Tel qu'indiqué dans la déclaration 21 annexée au Traité de Lisbonne, des règles spécifiques sur la protection des données à caractère personnel et sur la libre circulation de ces données dans les domaines de la coopération judiciaire en matière pénale et de la coopération policière se basant sur l'article 16 du traité sur le fonctionnement de l'Union européenne pourraient s'avérer nécessaires en raison de la nature spécifique de ces domaines.

3. C'est sur cette base que le législateur de l'Union a adopté la directive (UE) 2016/680 (ci-après la «directive en matière de protection des données dans le domaine répressif») qui établit les règles spécifiques relatives au traitement des données à caractère personnel par les autorités compétentes à des fins de **prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces**.

4. La directive en matière de protection des données dans le domaine répressif fixe les motifs autorisant le transfert de données à caractère personnel vers un pays tiers ou une organisation internationale dans ce contexte. Parmi les motifs d'un tel transfert, la Commission européenne

[1] JO L 119 du 4.5.2016, p. 89.
[2] WP254.rev01, adopté par le GT29 le 28 novembre 2017, tel que révisé, et adopté le 6 février 2018. Il actualise le chapitre I du 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» WP12, adopté par le GT29 le 24 juillet 1998.
[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du mardi 26 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

peut décider que le pays tiers ou l'organisation internationale en question garantit un niveau adéquat de protection.

5. Si le document de travail WP254.rev01 sur les critères de référence pour l'adéquation entend donner à la Commission européenne des orientations dans le cadre du RGPD quant au niveau de protection des données au sein des pays tiers et des organisations internationales, le présent document a pour but de fournir des orientations similaires dans le cadre de la directive en matière de protection des données dans le domaine répressif. Il instaure dans ce contexte les principes essentiels en matière 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 dans le contexte de la directive en matière de protection des données dans le domaine répressif (c'est-à-dire pour le traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales). En outre, il peut donner des orientations à des pays tiers et à des organisations internationales souhaitant obtenir l'adéquation.

6. Le présent document est uniquement axé sur les décisions d'adéquation. Il s'agit des actes d'exécution établis par la Commission européenne conformément à l'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif.

2. CONCEPT D'ADEQUATION

7. La directive en matière de protection des données dans le domaine répressif fixe les règles applicables au transfert de données à caractère personnel vers des pays tiers et des organisations internationales, dans la mesure où ces transferts relèvent de son champ d'application. Les règles applicables au transfert de données à caractère personnel sont énoncées au chapitre V de ladite directive, en particulier aux articles 35 à 39.

8. En vertu de l'article 36 de la directive en matière de protection des données dans le domaine répressif, le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu si un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale assure un niveau de protection adéquat. Il ressort de la jurisprudence de la Cour de justice de l'Union européenne[4] que cette disposition doit être lue à la lumière de l'article 35 de la directive en matière de protection des données dans le domaine répressif, qui s'intitule «Principes généraux applicables aux transferts de données à caractère personnel» et qui dispose que «[t]outes les dispositions du [chapitre V de la directive en matière de protection des données dans le domaine répressif] sont appliquées de manière que le niveau de protection des personnes physiques assuré par [cette] directive ne soit pas compromis».

9. Si la Commission européenne a décidé qu'un tel niveau de protection adéquat est assuré, les transferts de données à caractère personnel vers ce pays tiers, territoire, secteur ou cette organisation internationale peuvent avoir lieu, sans qu'il soit nécessaire d'obtenir une autorisation spécifique, sauf lorsqu'un autre État membre auprès duquel les données ont été collectées doit autoriser le transfert, conformément aux articles 35 et 36 ainsi qu'au considérant 66 de la directive en matière de protection des données dans le domaine répressif. Cette disposition est sans préjudice de la nécessité que le traitement des données par les autorités des États membres

[4] Arrêt du 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems, ECLI:EU:C:2020:559, point 92 (Schrems II).

concernés soit conforme aux dispositions nationales adoptées en application de la directive en matière de protection des données dans le domaine répressif.

10. Ce concept de «niveau adéquat de protection», qui existait déjà au titre de la directive 95/46[5] et de la décision-cadre 2008/977/JAI[6] du Conseil a été renforcé par la CJUE dans ce contexte et, récemment, dans le cadre du RGPD.

11. Comme l'a précisé la Cour, si le niveau de protection offert par un pays tiers doit être substantiellement équivalent à celui garanti dans l'Union, «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», mais «ces moyens doivent néanmoins s'avérer, en pratique, effectifs»[7]. Par conséquent, le principe d'adéquation ne doit pas refléter point par point la législation de l'Union, mais établir les exigences essentielles, fondamentales de cette législation.

12. Dans ce contexte, la Cour a également précisé qu'une décision d'adéquation adoptée par la Commission devrait comporter toute constatation quant à l'existence, dans le pays tiers, 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 ledit pays tiers, ingérences que des entités publiques de ce pays seraient *autorisées* à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale[8].

13. L'objectif des décisions d'adéquation de la Commission européenne est de confirmer officiellement, avec des effets contraignants sur les États membres[9], ainsi que sur leurs autorités européennes chargées de la protection des données[10], 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. Le pays tiers devrait offrir des garanties assurant un niveau adéquat de protection essentiellement équivalent à celui qui est assuré au sein de l'Union, en particulier lorsque les données sont traitées dans un ou plusieurs secteurs spécifiques[11].

14. 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

[5] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).
[6] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60).
[7] Arrêt du 6 octobre 2015 dans l'affaire C−362/14, Maximillian Schrems c. Data Protection Commissioner, ECLI:EU:C:2015:650, points 73 et 74 (Schrems I).
[8] Schrems I, point 88.
[9] Article 288 du TFUE.
[10] Schrems I, point 52.
[11] Considérant 67 de la directive en matière de protection des données dans le domaine répressif.

garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données[12].

3. ASPECTS PROCEDURAUX DES CONSTATS D'ADEQUATION DANS LE CADRE DE LA DIRECTIVE EN MATIERE DE PROTECTION DES DONNEES DANS LE DOMAINE REPRESSIF

15. Pour s'acquitter de la mission qui lui incombe de conseiller la Commission européenne conformément à l'article 51, paragraphe 1, point g), de la directive en matière de protection des données dans le domaine répressif, l'EDPB devrait disposer de tous les documents nécessaires, y compris la correspondance pertinente et les conclusions de la Commission européenne. Il est absolument nécessaire que tous les documents pertinents soient transmis suffisamment à l'avance à l'EDPB et traduits en anglais pour permettre des discussions éclairées et utiles avant l'adoption définitive des décisions d'adéquation. 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 à l'EDPB d'évaluer l'analyse menée par la Commission concernant le niveau de protection des données dans le pays tiers ou l'organisation internationale.

16. L'EDPB rendra en temps voulu un avis sur les conclusions de la Commission européenne dans lequel il recense, le cas échéant, les insuffisances du cadre d'adéquation et fournit des recommandations possibles, si cela s'avère nécessaire.

17. Conformément à l'article 36, paragraphe 4, de la directive en matière de protection des données dans le domaine répressif, il incombe à la Commission européenne de suivre – de manière permanente – les évolutions qui pourraient porter atteinte au fonctionnement d'une décision d'adéquation.

18. L'article 36, paragraphe 3, de la directive en matière de protection des données dans le domaine répressif 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.

[12] Schrems I, points 72 à 74, et avis 1/15 de la Cour, sur le projet d'accord entre le Canada et l'Union européenne, 26 juillet 2017, ECLI:EU:C:2017:592 (avis 1/15), point 134: «Ce droit à la protection des données à caractère personnel exige, notamment, que la continuité du niveau élevé de protection des libertés et des droits fondamentaux conféré par le droit de l'Union soit assurée en cas de transfert de données à caractère personnel depuis l'Union vers un pays tiers. Même si les moyens visant à garantir un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union afin de garantir le respect des exigences découlant du droit de l'Union, ces moyens doivent néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union»

19. Compte tenu de la mission 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, l'EDPB 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, l'EDPB devrait être tenu informé de toute procédure d'examen et mission d'examen dans le pays tiers ou l'organisation internationale. L'EDPB recommande sa participation à ces procédures et missions d'examen, comme prévu dans la décision «bouclier de protection des données» et dans la décision d'adéquation concernant le Japon.

20. Il convient également de souligner qu'en vertu de l'article 36, paragraphe 5, de la directive en matière de protection des données dans le domaine répressif, la Commission européenne peut, lorsqu'un pays tiers ou une organisation internationale n'assure plus un niveau de protection adéquat, abroger, modifier ou suspendre les décisions d'adéquation existantes. L'EDPB joue un rôle dans la procédure d'abrogation, de modification ou de suspension, car son avis est sollicité conformément à l'article 51, paragraphe 1, point g), de ladite directive.

21. Par ailleurs, sans préjudice des pouvoirs des autorités chargées des poursuites, les autorités de contrôle devraient aussi avoir le pouvoir de porter les violations de la présente directive à l'attention des autorités judiciaires ou d'ester en justice[13]. Il ressort notamment de l'arrêt Schrems I de la CJUE que les autorités chargées de la protection des données doivent pouvoir ester en justice devant les juridictions nationales si elles constatent que la demande d'une personne contre une décision d'adéquation du niveau de protection est fondée[14]. L'arrêt Schrems II a confirmé cette appréciation[15].

4. NORMES DE L'UE RELATIVES A L'ADEQUATION DANS LA COOPERATION POLICIERE ET JUDICIAIRE EN MATIERE PENALE

22. Sur le fond, les décisions d'adéquation devraient être axées sur l'évaluation de la législation existante du pays tiers concerné dans son ensemble, en théorie et en pratique, à la lumière des critères d'évaluation énoncés à l'article 36 de la directive en matière de protection des données dans le domaine répressif. Le système d'un pays tiers ou d'une organisation internationale doit contenir les principes et mécanismes de base, de procédure et d'application suivants en matière de protection des données.

[13] Voir article 47, paragraphe 5, et considérant 82 de la directive en matière de protection des données dans le domaine répressif.
[14] Voir Schrems I, point 65: «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.»
[15] Voir Schrems II, point 120: «Ainsi, même en présence d'une décision d'adéquation de la Commission, l'autorité nationale de contrôle compétente, saisie par une personne d'une réclamation relative à la protection de ses droits et de ses libertés à l'égard d'un traitement de données à caractère personnel la concernant, doit pouvoir 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 partagent les doutes de cette autorité quant à la validité de la décision d'adéquation, à un renvoi préjudiciel aux fins de l'examen de cette validité».

23. L'article 36, paragraphe 2, de la directive en matière de protection des données dans le domaine répressif 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.

24. En particulier, la Commission prend en considération l'état de droit, le respect des droits de l'homme et des libertés fondamentales[16], la législation pertinente, ainsi que la mise en œuvre de cette législation, les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées, l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes et les engagements internationaux souscrits par le pays tiers ou l'organisation internationale.

25. 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 de garantir leur mise en œuvre effective. Il incombe à la Commission européenne de vérifier – régulièrement – que les règles en vigueur sont effectives dans la pratique.

26. Les principes fondamentaux généraux des règles sur la protection des données et des exigences en matière de procédure et 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 (la Charte) et de la directive en matière de protection des données dans le domaine répressif. 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 concrètement au droit à la protection des données dans le domaine répressif Le pays tiers devrait offrir des garanties assurant un niveau adéquat de protection essentiellement équivalent à celui qui est assuré au sein de l'Union. Ces dispositions doivent être applicables.

27. Par ailleurs, en ce qui concerne le principe de proportionnalité[17], la CJUE a jugé, à l'égard de la législation des États membres, que la question de savoir si une limitation aux droits au respect de la vie privée et à la protection des données peut être justifiée doit être appréciée, d'une part, en mesurant la **gravité de l'ingérence** que comporte une telle limitation[18] et, d'autre part, en vérifiant que l'**importance de l'objectif d'intérêt général** poursuivi par cette limitation est en relation avec cette gravité[19].

[16] Lors de l'évaluation du cadre juridique du pays tiers, il convient de tenir compte de l'éventualité que la peine de mort ou toute forme de traitement cruel et inhumain soit imposée sur la base de données transférées depuis l'UE. En effet, si une telle peine ou un tel traitement était prévu dans la législation du pays tiers, des garanties supplémentaires devraient être prévues dans le cadre juridique du pays tiers afin de s'assurer que les données transférées depuis l'UE ne seront pas utilisées pour demander, prononcer ou exécuter une peine de mort ou toute forme de traitement cruel et inhumain (par exemple, un accord international imposant des conditions au transfert, l'engagement du pays tiers de ne pas imposer de peine de mort ou toute forme de traitement cruel et inhumain sur la base de données transférées depuis l'UE ou un moratoire sur la peine de mort).

[17] Article 52, paragraphe 1, de la charte des droits fondamentaux.

[18] La Cour a, par exemple, relevé que «l'ingérence que comporte le recueil en temps réel des données permettant de localiser un équipement terminal apparaît particulièrement grave, dès lors que ces données fournissent aux autorités nationales compétentes le moyen d'un suivi précis et permanent des déplacements des utilisateurs des téléphones mobiles. (...)» (arrêt du 6 octobre 2020 dans les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., ECLI:EU:C:2020:791, point 187 et jurisprudence citée).

[19] La Quadrature du Net e.a., point 131.

28. Selon la jurisprudence de la CJUE, une base légale qui permet des ingérences dans les droits fondamentaux doit, pour satisfaire au principe de proportionnalité, définir elle-même la portée de la limitation de l'exercice du droit concerné[20]. Les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire[21]. Pour satisfaire à cette exigence, en plus de prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause, la réglementation en cause doit imposer des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. «Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé[22]».

29. L'EDPB a adopté des recommandations dans lesquelles il définit des garanties essentielles reflétant la jurisprudence de la CJUE et de la Cour européenne des droits de l'homme dans le domaine de la surveillance qui doivent être prévues dans le droit du pays tiers lors de l'appréciation des ingérences de ces mesures de surveillance de ces pays tiers dans les droits des personnes concernées lorsque les données sont transférées vers ce pays tiers au titre du RGPD[23]. Pour déterminer si les conditions énoncées à l'article 36, paragraphe 2, point a), de la directive en matière de protection des données dans le domaine répressif sont remplies, l'EDPB estime que les garanties énoncées dans ces recommandations doivent être prises en considération lors de l'évaluation de l'adéquation d'un pays tiers au titre de la directive en matière de protection des données dans le domaine répressif dans le domaine de la surveillance, en tenant compte d'autres conditions spécifiques dans le domaine de la surveillance dans ce contexte.

30. En ce qui concerne l'exigence visée à l'article 36, paragraphe 2, point b), le pays tiers devrait non seulement assurer un contrôle indépendant effectif de la protection des données, mais aussi prévoir des mécanismes de coopération avec les autorités de protection des données des États membres[24].

31. En ce qui concerne l'exigence prévue à l'article 36, paragraphe 2, point c), outre les engagements internationaux pris par le pays tiers ou l'organisation internationale, il devrait également être tenu compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en matière de protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. Il y a lieu, en particulier, de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel (la convention 108[25] et sa version modernisée, la convention 108+). Le respect par le pays tiers des principes consacrés dans des documents internationaux, tels que le guide pratique du Conseil de l'Europe sur l'utilisation de données à caractère personnel dans le secteur de la police: comment prendre en considération la protection des données à caractère personnel dans la lutte contre la criminalité, doit également être pris en considération.

[20] Schrems II, point 180.
[21] Schrems II, point 176 et jurisprudence citée
[22] Schrems II, point 176 et jurisprudence citée
[23] Voir recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020.
[24] Considérant 67 de la directive en matière de protection des données dans le domaine répressif.
[25] Considérant 68 de la directive en matière de protection des données dans le domaine répressif.

32. Une décision d'adéquation devrait garantir que, grâce au contenu des droits à la vie privée et à la protection des données et à leur mise en œuvre, contrôle et application efficaces, le système étranger dans son ensemble assure le niveau de protection requis, y compris pour les données en transit vers ce pays tiers. Comme l'a souligné la CJUE dans l'arrêt Schrems II, le niveau élevé de protection accordé devrait également être assuré pendant le transfert des données vers un pays tiers[26].

33. Enfin, lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, la Commission européenne devrait prendre en considération des critères clairs et objectifs, comme des références à des activités de traitement spécifiques et le champ d'application des normes juridiques applicables et du droit en vigueur dans le pays tiers[27].

A. Principes généraux et garanties

a) Concepts

34. Il devrait exister des concepts de base en matière de protection des données. Ceux-ci ne doivent pas refléter la terminologie de la directive en matière de protection des données dans le domaine répressif, mais ils devraient refléter les concepts consacrés par la législation européenne en matière de protection des données et être cohérents avec ces concepts. À titre d'exemple, la directive en matière de protection des données dans le domaine répressif inclut les concepts importants suivants: «données à caractère personnel», «traitement des données à caractère personnel», «autorités compétentes», «responsable du traitement», «sous-traitant», «destinataire», «données sensibles», «exactitude», «profilage», «protection des données dès la conception et par défaut», «autorité de contrôle» et «pseudonymisation».

b) Licéité et loyauté du traitement des données à caractère personnel (article 4 - considérant 26)

35. En vertu de l'article 8, paragraphe 2, de la Charte, les données à caractère personnel devraient, entre autres, être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi[28]. Néanmoins, dans le contexte de l'application de la loi, il convient de noter que, dans le cadre de l'exécution des missions de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales qui leur sont confiées de manière institutionnelle par la loi, les autorités compétentes peuvent demander ou ordonner aux personnes physiques de donner suite aux demandes qui leur sont adressées. Dans ce cas, le consentement de la personne concernée ne devrait pas constituer une base juridique pour le traitement de données à caractère personnel par les autorités compétentes[29].

[26] Voir point 93.
[27] Considérant 67 de la directive en matière de protection des données dans le domaine répressif.
[28] Voir Schrems II, point 173:
[29] Le considérant 35 de la directive en matière de protection des données dans le domaine répressif dispose également ce qui suit: «[l]orsqu'elle est tenue de respecter une obligation légale, la personne concernée ne dispose pas d'une véritable liberté de choix; sa réaction ne pourrait dès lors être considérée comme une manifestation libre de sa volonté. Cela ne devrait pas empêcher les États membres de prévoir par la loi que la personne concernée peut consentir au traitement de données à caractère personnel la concernant aux fins de la présente directive, par exemple pour des tests ADN dans des enquêtes pénales ou le suivi de sa localisation au moyen de dispositifs électroniques dans le cadre de l'exécution de sanctions pénales».

36. Cette base juridique devrait établir des règles claires et précises régissant la portée et l'application des activités de traitement des données concernées et imposer des garanties minimales[30]. En outre, la CJUE a rappelé que cette «réglementation doit être légalement contraignante en droit interne[31]».

37. Pour être licite, le traitement des données[32] devrait être nécessaire à l'exécution d'une mission par une autorité compétente à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris les garanties contre les menaces pour la sécurité publique et la prévention de telles menaces[33]. Ces finalités devraient être prévues dans le droit national.

38. Les données à caractère personnel sont traitées loyalement. En matière de protection des données, le principe de traitement loyal est une notion distincte du droit à accéder à un tribunal impartial au sens de l'article 47 de la Charte et de l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH)[34].

c) Le principe de limitation de la finalité (article 4)

39. Les finalités spécifiques du traitement des données à caractère personnel devraient être explicites et légitimes, et déterminées au moment de la collecte des données à caractère personnel[35].

40. Les données à caractère personnel devraient être collectées pour des finalités déterminées, explicites et légitimes relevant de la prévention et de la détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales[36], y compris de protection contre les menaces pour la sécurité publique dans le pays tiers puis utilisées à ces fins, dans la mesure où cela n'est pas incompatible avec la finalité initiale du traitement (par exemple, pour des procédures d'exécution parallèles ou à des fins archivistiques dans l'intérêt public, à des fins scientifiques, statistiques ou historiques) et sous réserve de garanties appropriées pour les droits et libertés des personnes concernées. Si des données à caractère personnel sont traitées par le même responsable du traitement ou un autre (autorité compétente[37]) pour une finalité de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales autre que celle pour laquelle elles ont été collectées, un tel traitement devrait

[30] Voir Schrems II, points 175 et 180, et avis 1/15, point 139, et la jurisprudence citée.
[31] Voir l'arrêt du 6 octobre 2020 dans l'affaire C-623/17, Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e.a., ECLI:EU:C:2020:790, point 68. Il convient également de préciser que, dans la version française de l'arrêt, la CJUE utilise le terme «réglementation», dont le sens ne se limite pas aux seuls actes du Parlement.
[32] Le traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.
[33] Les autorités compétentes sont toutes les autorités publiques compétentes à ces fins ou tout autre organisme ou entité auquel la loi confie l'exercice de l'autorité publique et des prérogatives de puissance publique à ces fins.
[34] Considérant 26 de la directive en matière de protection des données dans le domaine répressif.
[35] Considérant 26 de la directive en matière de protection des données dans le domaine répressif.
[36] Cela comprend: «les activités de police effectuées sans savoir au préalable si un incident constitue une infraction pénale ou non. Ces activités peuvent également comprendre l'exercice de l'autorité par l'adoption de mesures coercitives, par exemple les activités de police lors de manifestations, de grands événements sportifs et d'émeutes. Parmi ces activités figure également le maintien de l'ordre public lorsque cette mission est confiée à la police ou à d'autres autorités répressives lorsque cela est nécessaire à des fins de protection contre les menaces pour la sécurité publique et pour les intérêts fondamentaux de la société protégés par la loi, et de prévention de telles menaces, qui sont susceptibles de déboucher sur une infraction pénale» (considérant 12 de la directive en matière de protection des données dans le domaine répressif). La distinction doit être faite par rapport à un objectif de sécurité nationale ou à des activités relevant du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne (considérant 14 de la directive en matière de protection des données dans le domaine répressif).
[37] Voir note de bas de page nº 33.

être permis à condition qu'il soit autorisé conformément aux dispositions légales applicables et qu'il soit nécessaire et proportionné au regard de cette autre finalité[38]. Il convient également de tenir compte de l'existence d'un mécanisme permettant d'informer les autorités compétentes des États membres concernés de ce traitement ultérieur des données[39]. En outre, en tout état de cause, le niveau de protection des personnes physiques prévu dans l'Union par la directive en matière de protection des données dans le domaine répressif ne devrait pas être compromis, y compris en cas de transferts de données à caractère personnel au départ du pays tiers à des responsables du traitement ou à des sous-traitants dans le même pays tiers[40].

d) Conditions spécifiques applicables au traitement ultérieur à d'autres fins (article 9)

41. Le traitement ultérieur ou la divulgation de données transférées depuis l'Union à d'autres fins que répressives telles que des fins de sécurité nationale, devraient également être prévus par la loi, être nécessaires et proportionnés. Il convient également de tenir compte de l'existence d'un mécanisme permettant d'informer les autorités compétentes des États membres concernés de ce traitement ultérieur des données[41]. Là encore, une fois traitées ou divulguées ultérieurement, les données devraient bénéficier du même niveau de protection que lorsqu'elles ont été traitées initialement par l'autorité compétente destinataire.

e) Le principe de minimisation des données

42. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées. En particulier, il convient de tenir compte de l'application d'exigences en matière de protection des données dès la conception et par défaut, telles que des champs de saisie limités (communications structurées) ou des contrôles de qualité automatisés et non automatisés.

f) Le principe d'exactitude des données

43. Les données doivent être exactes et, si nécessaire, mises à jour. Néanmoins, il convient d'appliquer le principe d'exactitude des données tout en tenant compte de la nature et de la finalité du traitement concerné. Dans le cadre des procédures judiciaires notamment, les déclarations contenant des données à caractère personnel sont fondées sur les perceptions subjectives des personnes physiques et ne sont pas toujours vérifiables. Le principe d'exactitude ne devrait, par conséquent, pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une déclaration déterminée a été faite[42].

44. Il convient de veiller à ce que les données à caractère personnel qui sont inexactes, incomplètes ou qui ne sont plus à jour ne soient pas transmises ou mises à disposition[43] et que des procédures soient prévues pour corriger ou effacer les données inexactes. En particulier, tout système de classification des informations traitées, en ce qui concerne la fiabilité de la source et le niveau de vérification des faits[44], devrait être pris en considération.

[38] Considérant 29 de la directive en matière de protection des données dans le domaine répressif.
[39] Un tel mécanisme pourrait être, par exemple, des codes de traitement convenus d'un commun accord, une obligation de notification au titre d'un instrument international, ainsi que d'éventuelles notifications automatisées, ou d'autres mesures similaires en matière de transparence.
[40] Considérant 64 de la directive en matière de protection des données dans le domaine répressif.
[41] Voir note de bas de page nº 39.
[42] Considérant 30 de la directive en matière de protection des données dans le domaine répressif.
[43] Considérant 32 de la directive en matière de protection des données dans le domaine répressif.
[44] Par exemple, des grilles 4x4 pour les évaluations de la fiabilité et les codes de traitement.

g) Le principe de conservation des données

45. Les données ne devraient pas être conservées plus longtemps que ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Il convient de mettre en place des mécanismes appropriés pour l'effacement des données à caractère personnel; il peut s'agir d'un examen à période fixe ou d'un examen périodique de la nécessité de conserver des données à caractère personnel (ou une combinaison des deux: période maximale fixe et réexamen périodique à une certaine fréquence)[45]. Les données à caractère personnel conservées pendant des périodes plus longues à des fins archivistiques dans l'intérêt public, à des fins scientifiques, statistiques ou historiques devraient faire l'objet de garanties appropriées (par exemple en ce qui concerne l'accès à ces données)[46].

h) Le principe de sécurité et de confidentialité (article 29, considérants 28 et 71)

46. Toute entité procédant au traitement de données à caractère personnel devrait veiller à ce que les données soient traitées de façon à garantir la sécurité des données à caractère personnel, y compris en empêchant tout accès non autorisé à ces données et à l'équipement utilisé pour leur traitement ainsi que l'utilisation non autorisée de ces données et de cet équipement. Cela comprend la protection contre le traitement illicite, et les mesures appropriées pour y répondre, et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. Lors de la détermination du niveau de sécurité, il convient de tenir compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du risque de probabilité et de gravité variables pour les droits et libertés des personnes physiques.

47. Il convient de veiller à l'existence de canaux de communication sécurisés entre les autorités des États membres qui transfèrent les données à caractère personnel et les autorités destinataires des États tiers.

i) Le principe de transparence (article 13, considérants 26, 39, 42, 43, 44, 46)

48. Les personnes physiques devraient être informées des risques, règles, garanties et droits en ce qui concerne le traitement de données à caractère personnel les concernant et des modalités d'exercice de leurs droits par rapport au traitement[47].

49. Il convient de mettre à la disposition des personnes physiques des informations sur tous les principaux éléments du traitement de leurs données à caractère personnel. Ces informations devraient être aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples De telles informations devraient inclure la finalité du traitement, l'identité du responsable du traitement, les droits à leur disposition[48] et d'autres informations dans la mesure où cela est nécessaire pour garantir un traitement loyal.

50. Dans certaines conditions, il peut y avoir des exceptions à ce droit à l'information. Cette limitation devrait toutefois être autorisée par une mesure législative et être nécessaire et proportionnée pour éviter de gêner des recherches, des enquêtes ou des procédures officielles ou judiciaires, éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales, pour protéger la sécurité publique

[45] Article 5 de la directive en matière de protection des données dans le domaine répressif.
[46] Considérant 26 de la directive en matière de protection des données dans le domaine répressif.
[47] Considérant 26 de la directive en matière de protection des données dans le domaine répressif.
[48] Tant les droits matériels (droit d'accès, de rectification, etc.) que le droit de recours.

ou la sécurité nationale ou pour protéger les droits et libertés de tiers, pour autant qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, dans le respect des droits fondamentaux et des intérêts légitimes de la personne physique concernée. Ces restrictions devraient également être envisagées et évaluées en tenant compte de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel. En tout état de cause, toute restriction éventuelle devrait être temporaire et non générale et devrait être encadrée par des conditions, des garanties et des limitations similaires à celles exigées par la Charte et la CEDH telles qu'interprétées respectivement dans la jurisprudence de la CJUE et par la Cour européenne des droits de l'homme, et respecter en particulier le contenu essentiel de ces droits et libertés.

j) Le droit d'accès, de rectification, et d'effacement (articles 14 et 16)

51. La personne concernée devrait avoir le droit d'obtenir confirmation de l'existence ou non d'un traitement de données la concernant et, le cas échéant, avoir accès à ses données. Ce droit devrait comprendre au moins certaines informations sur le traitement, telles que les finalités du traitement ainsi que sa base juridique, le droit d'introduire une réclamation auprès de l'autorité de contrôle ou les catégories de données à caractère personnel concernées[49]. Ce droit est particulièrement important si la transparence est assurée par un avis général (par exemple, des informations sur le site web de l'autorité).

52. La personne concernée devrait avoir le droit d'obtenir la rectification de ses données pour des raisons précises, par exemple lorsqu'il s'avère que celles-ci sont inexactes ou incomplètes. La personne concernée devrait également avoir le droit d'obtenir l'effacement de ses données lorsque, par exemple, leur traitement n'est plus nécessaire ou est illicite.

53. L'exercice de ces droits ne devrait pas être excessivement lourd pour la personne concernée.

k) Limitations applicables aux droits des personnes concernées

54. D'éventuelles restrictions de ces droits pourraient exister afin d'éviter de gêner des recherches, des enquêtes ou des procédures officielles ou judiciaires, éviter de nuire à la prévention et à la détection d'infractions pénales, aux enquêtes et aux poursuites en la matière, ou à l'exécution de sanctions pénales, pour protéger la sécurité publique ou la sécurité nationale ou pour protéger les droits et libertés de tiers, pour autant qu'une telle limitation partielle ou complète constitue une mesure nécessaire et proportionnée dans une société démocratique, dans le respect des droits fondamentaux et des intérêts légitimes de la personne physique concernée. Ces restrictions devraient également être envisagées et évaluées en tenant compte de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle ou de former un recours juridictionnel.

l) Restrictions concernant les transferts ultérieurs (article 35, considérants 64 et 65)

55. Les transferts ultérieurs de données à caractère personnel par le destinataire initial vers un autre pays tiers ou une organisation internationale ne doivent pas porter atteinte au niveau de protection, prévu dans l'Union, des personnes physiques dont les données sont transférées. Par conséquent, ces transferts ultérieurs de données ne devraient être autorisés que si la continuité du niveau de protection garanti par le droit de l'Union est assurée[50]. En particulier, le destinataire

[49] Article 14 de la directive en matière de protection des données dans le domaine répressif.
[50] Voir également avis 1/15.

ultérieur (c'est-à-dire le destinataire du transfert ultérieur) devrait être une autorité compétente à des fins en matière de protection des données dans le domaine répressif[51] et de tels transferts ultérieurs de données ne peuvent avoir lieu qu'à des fins limitées et précises et pour autant qu'il existe une base juridique pour ce traitement.

56. Il convient également de tenir compte de l'existence d'un mécanisme permettant aux autorités compétentes de l'État membre concerné d'être informées et d'autoriser un tel transfert ultérieur de données. Le destinataire initial des données transférées depuis l'UE devrait être responsable et pouvoir prouver que l'autorité compétente concernée de l'État membre a autorisé le transfert ultérieur[52] et que des garanties appropriées sont prévues pour les transferts ultérieurs de données en l'absence d'une décision d'adéquation concernant le pays tiers vers lequel les données seraient transférées ultérieurement[53].

m) Principe de responsabilité (article 4, paragraphe 4)

57. Le responsable du traitement devrait être responsable du respect des principes de protection des données énoncés à l'article 4 de la directive en matière de protection des données dans le domaine répressif, et être en mesure de démontrer que ces principes sont respectés.

[51] Voir note de bas de page nº 33.
[52] Dans ce contexte, il convient de tenir compte de l'existence d'une obligation ou d'un engagement de mettre en œuvre les codes de traitement pertinents définis par les autorités des États membres de transfert.
[53] Les exigences ci-dessus sont sans préjudice des conditions spécifiques applicables aux transferts ultérieurs vers un pays adéquat énoncées dans la directive en matière de protection des données dans le domaine répressif [article 35, paragraphe 1, points c) et e)].

B. Exemples de principes supplémentaires touchant au contenu à appliquer à certains types de traitement

a) Catégories particulières de données (article 10 et considérant 37)

58. Des garanties spécifiques devraient exister concernant des «catégories particulières de données[54]» et elles devraient répondre aux risques spécifiques inhérents[55]. Ces catégories devraient correspondre à celles énoncées à l'article 10 de la directive en matière de protection des données dans le domaine répressif. Le traitement de catégories particulières de données devrait donc faire l'objet de garanties spécifiques et être autorisé uniquement lorsque cela s'avère strictement nécessaire dans certaines conditions, par exemple pour protéger l'intérêt vital d'une personne.

b) Prise de décision automatisée et profilage (article 11 et considérant 38)

59. Les décisions prises sur le seul fondement d'un traitement automatisé (prise de décision individuelle automatisée), ainsi que sur le profilage, et qui produisent des effets juridiques défavorables pour la personne concernée ou qui affecte celle-ci de manière significative, devraient avoir lieu dans certaines conditions prévues dans le cadre légal du pays tiers[56].

60. Dans le cadre de l'Union européenne, ces conditions sont notamment la fourniture d'informations spécifiques à la personne concernée et le droit d'obtenir une intervention humaine de la part du responsable du traitement, en particulier d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation ou de contester la décision.

61. La législation du pays tiers devrait, en tout état de cause, prévoir les garanties nécessaires pour les droits et libertés de la personne concernée. À cet égard, il convient également de tenir compte de l'existence d'un mécanisme permettant d'informer les autorités compétentes de l'État membre concerné de tout traitement ultérieur, tel que l'utilisation des données transférées aux fins d'un profilage à grande échelle.

c) Protection des données dès la conception et protection des données par défaut (article 20)

62. Lors de l'évaluation de l'adéquation, il convient de tenir compte de l'existence d'une obligation pour les responsables du traitement d'adopter des politiques internes et de mettre en œuvre des mesures qui respectent les principes de protection des données dès la conception et de protection des données par défaut, compte tenu de l'état de la technique, du coût de la mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques d'une probabilité et d'une gravité variables pour les droits et libertés des personnes physiques posés par le traitement, à la fois au moment de la détermination des moyens de traitement et au moment du traitement proprement dit, à l'adoption de pseudonymes appropriés pour le traitement.

[54] Ces catégories particulières sont également appelées «données sensibles» au considérant 37 de la directive en matière de protection des données dans le domaine répressif.
[55] Ces garanties supplémentaires pourraient être, par exemple, des mesures de sécurité spécifiques, des droits d'accès limités au personnel, des restrictions concernant le traitement ultérieur, la prise de décision automatisée, le partage ultérieur ou les transferts ultérieurs.
[56] Avis 1/15, point 173.

C. Mécanismes en matière de procédure et d'application

63. 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[57], un système cohérent avec le système européen doit se caractériser par l'existence des éléments suivants:

a) Autorité de contrôle indépendante compétente [article 36, paragraphe 2, point b) et article 36, paragraphe 3, et considérant 67]

64. Une ou plusieurs autorités de contrôle indépendantes, chargées 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 en matière de protection des données dans le domaine répressif adéquats pour assurer le respect des droits en matière de protection des données et favoriser la sensibilisation. Il convient également de tenir compte du personnel et du budget de l'autorité de contrôle. L'autorité de contrôle devrait également être en mesure de mener, de sa propre initiative, des enquêtes. Elle devrait également être chargée d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits [voir également le point c) ci-dessous]. Les décisions d'adéquation devraient définir, le cas échéant, la ou les autorités de contrôle et les mécanismes de coopération avec les autorités de contrôle des États membres pour faire respecter les règles en matière de protection des données.

b) Mise en œuvre effective des règles en matière de protection des données

65. Le système d'un pays tiers devrait garantir un niveau élevé 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.

66. 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 devraient consister notamment en la tenue de registres ou de journaux d'activités de traitement des données pour une période appropriée. Elles peuvent également comprendre, par exemple, des analyses d'impact de la protection des données, la désignation d'un responsable de la protection des données ou la protection des données dès la conception et par défaut.

c) Le système de protection des données facilite l'exercice des droits des personnes concernées (articles 12, 17 et 46 de la directive en matière de protection des données dans le domaine répressif)

67. Le cadre de protection des données d'un pays tiers devrait obliger les responsables du traitement à faciliter l'exercice des droits des personnes concernées visés à la section A, point j), ci-dessus,

[57] Schrems I, point 74.

et prévoir que son autorité de contrôle informe toute personne concernée, sur demande, de l'exercice de ses droits[58].

d) Le système de protection des données fournit des mécanismes de recours appropriés

68. Bien qu'il n'existe actuellement aucune jurisprudence relative à l'adéquation du système juridique d'un pays tiers dans le cadre de la directive en matière de protection des données dans le domaine répressif, la CJUE a interprété le droit fondamental à une protection juridictionnelle effective tel qu'il est consacré à l'article 47 de la Charte. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal[59] dans le respect des conditions prévues à cet article.

69. Selon une jurisprudence constante de la CJUE, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence de l'état de droit. Ainsi, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte[60].

70. 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.

71. 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.

72. Si les règles ne sont pas respectées, la personne concernée dont les données à caractère personnel sont transférées vers le pays tiers 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.

[58] L'exercice des droits des personnes concernées pourrait être direct ou indirect.
[59] La CJUE considère qu'une protection juridictionnelle effective peut être assurée non seulement par une juridiction, mais également par un organe qui offre des garanties substantiellement équivalentes à celles requises à l'article 47 de la Charte (voir arrêt Schrems II, point 197). Ce constat pourrait s'avérer pertinent en particulier pour les organisations internationales.
[60] Schrems II, point 187 et 194 et jurisprudence citée.