



**175/16/FR
WP 234**

Lignes directrices destinées aux États membres sur les critères à remplir pour assurer le respect des exigences en matière de protection des données dans le contexte de l'échange automatique de données à caractère personnel à des fins fiscales

Adoptées le 16 décembre 2015

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant traitant des questions ayant trait à la protection des données et à la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, Bureau n° MO-59 02/013.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

Contexte

L'objectif des présentes lignes directrices est de garantir le respect des exigences en matière de protection des données dans le contexte de l'échange automatique, entre les autorités compétentes de différents pays, de données à caractère personnel à des fins fiscales.

Les autorités de l'Union européenne chargées de la protection des données, qui sont représentées au sein du groupe de travail «Article 29», s'attachent à examiner les nouvelles tendances aux niveaux européen et international, y compris l'introduction de mécanismes permettant l'échange transfrontière automatique de données à caractère personnel à des fins fiscales et leur incidence sur la vie privée et la protection des données.

Au cours des dernières années, la nécessité de lutter contre l'évasion fiscale a conduit les gouvernements à se lancer dans l'élaboration d'outils d'échange d'informations.

Aux États-Unis, la loi sur la conformité fiscale des comptes étrangers («Foreign Account Tax Compliance Act» ou «FATCA») a été adoptée dans le but de lutter contre les actes d'évasion fiscale commis par des résidents fiscaux américains au moyen de comptes à l'étranger.

Le 15 juillet 2014, le Conseil de l'OCDE a approuvé la «norme d'échange automatique de renseignements relatifs aux comptes financiers - Norme commune de déclaration» (NCD), qui prévoit notamment des procédures de diligence raisonnable communes que les établissements financiers doivent appliquer pour déterminer les comptes déclarables.

Au niveau européen, la directive 2011/16/UE a été adoptée, puis modifiée par la directive 2014/107/UE du Conseil, afin de garantir, à l'échelle de l'Union, une approche globale de l'échange automatique d'informations visant à lutter contre l'évasion fiscale. Elle intègre essentiellement la NCD de l'OCDE dans le cadre juridique de l'UE.

Au cours des dernières années, le groupe de travail «Article 29» a examiné l'incidence de l'échange automatique d'informations sur le droit à la protection des données à caractère personnel dans les documents suivants:

- deux lettres, respectivement adoptées le 21 juin 2012¹ et le 1^{er} octobre 2012², concernant le FATCA
- une lettre adoptée le 18 septembre 2014 sur la NCD de l'OCDE³.

Plus récemment, le 4 février 2015⁴, le groupe de travail «Article 29» a adopté une «*déclaration sur les échanges interétatiques automatiques de données à caractère personnel à des fins fiscales*», afin d'attirer l'attention des gouvernements nationaux et des institutions européennes sur la nécessité de veiller à ce que ces échanges aient lieu dans le respect des exigences en

¹Voir: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf

²Voir: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121001_letter_to_taxud_fatca_en.pdf

³ La lettre peut être consultée à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_letter_on_oecd_common_reporting_standard.pdf.pdf, et l'annexe à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_annex_oecd_common_reporting_standard.pdf.pdf

⁴ La déclaration peut être consultée à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf

matière de protection des données prévues par le droit de l'UE, notamment en ce qui concerne les principes de nécessité et de proportionnalité, et en prenant dûment en compte les effets de l'arrêt de la Cour de justice du 8 avril 2014⁵ qui a invalidé la directive 2006/24/CE (la «directive sur la conservation des données») au motif que les législateurs de l'Union européenne avaient outrepassé les limites de la proportionnalité dans l'élaboration de la directive.

Comme annoncé dans ladite déclaration, le groupe de travail «Article 29» - également à la suite d'une demande de la Commission européenne - entend fournir des orientations supplémentaires afin que les accords bilatéraux/multilatéraux et/ou les législations nationales mettant en œuvre le cadre juridique sur la coopération administrative dans le domaine de la fiscalité (en application de la directive 2011/16 ou de la NCD de l'OCDE ou en reproduisant le FATCA) puissent offrir des garanties supplémentaires et cohérentes en matière de protection des données.

À cette fin, le groupe de travail «Article 29» considère qu'une première étape importante consiste à faire le point sur les cadres juridiques existants et à déceler les lacunes qui nuisent actuellement à la protection des données et/ou les différences majeures entre les instruments au niveau national. Aussi le groupe a-t-il préparé un questionnaire, envoyé par chaque autorité chargée de la protection des données aux autorités fiscales nationales (voir annexe) visant à évaluer le niveau de mise en œuvre des principes de la protection des données, conformément à la directive 95/46/CE, dans le contexte des accords interétatiques bilatéraux/multilatéraux qui prévoient l'échange automatique d'informations à des fins fiscales. Les réponses reçues font apparaître des aspects intéressants du processus conduisant à une coopération internationale contre l'évasion fiscale. Elles indiquent en effet que les États membres conviennent d'une sorte de programme de coopération (dans le cadre d'un accord bilatéral direct avec les États-Unis mettant en œuvre le FATCA, ou par la signature de l'*accord multilatéral entre autorités compétentes sur l'échange automatique d'informations relatives aux comptes financiers* ou les deux). Elles révèlent également que ces initiatives donnent lieu à un contrôle parlementaire et à la consultation des autorités chargées de la protection des données. Néanmoins, certains points critiques ressortent en ce qui concerne la mise en œuvre effective de garanties en matière de protection des données dans le contexte de la coopération fiscale. Quelques exemples se rapportent au fait que les personnes concernées ne sont pas toujours préalablement informées de ce que leurs données à caractère personnel seront utilisées ou transférées à l'étranger pour les besoins de la lutte contre l'évasion fiscale. En outre, nous constatons que les données échangées peuvent être utilisées à différentes fins tant que l'utilisation secondaire est conforme aux lois du pays émetteur (ce qui compromet donc gravement le principe d'une protection adéquate ou équivalente des données à caractère personnel inscrit dans la directive 95/46).

Compte tenu également de ces réponses au questionnaire, les présentes lignes directrices visent à fournir des indications sur les garanties en matière de protection des données⁶ devant être

⁵ Affaires C-293/12 et C-594/12, *Digital Rights Ireland, Seitlinger e.o.*, arrêt publié à l'adresse suivante: <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62012CJ0293>

⁶ Ces garanties sont liées au respect des droits des particuliers à la vie privée et à la protection des données, consacrés dans la Charte des droits fondamentaux de l'Union européenne (articles 7 et 8) et aux règles du cadre juridique de l'UE en matière de protection des données. Le cadre juridique qui régit le traitement des données à caractère personnel dans l'Union européenne se compose actuellement de quatre instruments principaux:

la directive 95/46/CE, ou directive relative à la protection des données, est l'élément central de la législation relative à la protection des données à caractère personnel en Europe. Elle énonce les règles générales relatives à la licéité du traitement des données à caractère personnel et aux droits des personnes dont les données sont traitées (personnes concernées), et impose à chaque État membre de se doter d'une autorité de contrôle indépendante chargée de surveiller la mise en œuvre de la directive;

le règlement (CE) n° 45/2001 couvre le traitement des données à caractère personnel par les institutions et organes de l'UE et institue le CEPD à titre d'autorité de contrôle indépendante;

appliquées dans trois cas de figure distincts: (i) l'échange de données à caractère personnel entre États membres de l'UE; (ii) l'échange de données à caractère personnel entre un État membre de l'UE et un pays tiers qui a fait l'objet d'une décision de la Commission européenne constatant le caractère adéquat de la protection, et (iii) l'échange de données à caractère personnel entre un État membre de l'UE et un pays tiers qui n'a pas fait l'objet d'une telle décision de la Commission européenne. Sont présentées ci-après un certain nombre de garanties qui devraient toujours être prévues dans le contexte de l'échange automatique, entre les autorités compétentes de différents pays, de données à caractère personnel à des fins fiscales.

1. L'échange de données entre États membres de l'UE

Dans ce cas, les données à caractère personnel (par exemple, les informations financières permettant d'identifier une personne physique) sont systématiquement transférées à intervalles réguliers de l'établissement financier d'un État membre de l'UE à l'établissement financier d'un autre État membre. Les deux États membres auront adopté des règles nationales transposant la directive 95/46/CE (la «directive»).

Afin que l'échange de données à caractère personnel soit licite, il est nécessaire qu'il soit conforme à ces règles nationales. En outre, le responsable du traitement des données applique toutes les garanties en matière de protection des données prévues par la directive et les mesures nationales la transposant.

Les garanties les plus communément applicables sont, entre autres, la nécessité et la proportionnalité de l'échange de données, la communication d'informations correctes à la personne concernée quant aux informations qui sont transférées et la finalité de l'échange, le droit d'accès et de rectification, le contrôle assuré par l'autorité nationale compétente chargée de la protection des données, les voies de recours dont dispose la personne concernée et d'autres garanties encore, comme il est plus amplement expliqué au point 3 ci-dessous.

Il est également possible que des données financières à caractère personnel soient échangées entre les autorités compétentes au sein d'un même État membre aux fins d'assurer le respect de la législation fiscale. Cette possibilité a fait l'objet d'un arrêt récent de la CJUE dans l'affaire *Bara*⁷. Dans son arrêt, la Cour a précisé que «*l'exigence de traitement loyal des données*

la directive 2002/58/CE concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, et établit des règles revêtant une importance particulière, notamment en ce qui concerne la confidentialité, les données relatives à la facturation et au trafic, et des règles concernant les communications commerciales non sollicitées;

la décision-cadre 2008/977/JAI du Conseil porte sur la coopération policière et judiciaire en matière pénale et prévoit notamment des règles applicables aux échanges de données à caractère personnel, y compris les bases de données nationales et de l'UE, ainsi que les transmissions aux autorités compétentes et aux particuliers 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.

À l'échelle internationale, le cadre juridique qui régit le traitement des données à caractère personnel se compose de deux instruments principaux:

la convention 108 se réfère à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel qui a été adoptée par le Conseil de l'Europe en 1981. Il s'agit du premier instrument international juridiquement contraignant dans le domaine de la protection des données;

les lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (dans leur version mise à jour en 2013) s'appliquent aux données à caractère personnel, du secteur tant public que privé, qui, en raison des modalités de leur traitement, ou en raison de leur nature ou du contexte dans lequel elles sont utilisées, constituent un risque pour la vie privée et les libertés individuelles.

⁷ Voir l'arrêt de la Cour du 1^{er} octobre 2015 dans l'affaire C-201/14, *Smaranda Bara et autres*.

personnelles prévue à l'article 6 de la directive 95/46 oblige une administration publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données». En outre, la Cour a précisé que les droits de la personne concernée pouvaient être limités à certaines fins, y compris pour des raisons fiscales, mais que la restriction devait être prévue par la loi, un simple accord de coopération administrative entre les autorités concernées n'étant pas suffisant⁸. Les principes de droit développés par la Cour s'appliquent également, mutatis mutandis, à l'échange international d'informations financières à caractère personnel.

2. L'échange de données entre un État membre de l'UE et un pays tiers faisant l'objet d'une décision constatant le caractère adéquat de la protection

Dans ce cas, les données à caractère personnel sont transférées systématiquement et à intervalles réguliers à un pays tiers qui fait l'objet d'une décision de la Commission constatant que le pays en question fournit une protection adéquate des données à caractère personnel conformément à l'article 25 de la directive («décision d'adéquation»). Les données à caractère personnel peuvent donc être transférées vers le pays destinataire, pour autant que les garanties citées dans la décision d'adéquation sont appliquées sous la responsabilité de l'administration fiscale à l'origine de la procédure. À cet égard, comme l'a récemment établi la jurisprudence de l'UE⁹, il incombe à l'autorité nationale chargée de la protection des données d'exercer une surveillance et, le cas échéant, d'intervenir en ouvrant une enquête, si elle dispose d'éléments lui permettant de déterminer que les garanties en matière de protection des données mises en œuvre par le pays tiers ne sont pas, ou plus, suffisantes.

Selon le même arrêt, toute décision d'adéquation doit strictement respecter les critères prévus à l'article 25. La Cour a souligné que même une décision sectorielle, comme la décision «sphère de sécurité» exigeait une analyse approfondie et continue des lois internes du pays tiers et de ses engagements internationaux.

Les principes de droit développés par la Cour dans cette affaire s'appliquent également, mutatis mutandis, à l'échange international d'informations financières à caractère personnel.

3. L'échange de données entre un État membre de l'UE et un pays tiers ne faisant PAS l'objet d'une décision d'adéquation

Dans ce cas, les données à caractère personnel sont transférées systématiquement et à intervalles réguliers vers un pays tiers qui ne fait PAS l'objet d'une décision de la Commission constatant un niveau adéquat de protection. Il est dès lors crucial de s'assurer que le pays destinataire fournit une protection adéquate des données à caractère personnel grâce à l'adoption d'un accord *ad hoc* contenant des garanties contraignantes. Compte tenu de la nature globale et systématique du transfert de données concerné, les exceptions prévues à l'article 26, paragraphe 1, point d), de la directive 95/46/CE ne peuvent pas être appliquées.

En conséquence, l'article 7, point e), de ladite directive ne peut être que la seule base juridique. Dès lors, le critère à remplir pour que le transfert des données soit légitime est que «*le traitement est nécessaire à l'exécution d'une mission d'intérêt public (...)*», comme la lutte contre l'évasion fiscale.

⁸ Voir l'arrêt Barra, point 40.

⁹ Voir l'arrêt de la Cour du 6 octobre 2015 dans l'affaire C-362/14, *Schrems/ Data Protection Commissioner*.

Nous nous pencherons ci-dessous sur un certain nombre de garanties qui devraient toujours être prévues lorsqu'il existe une base juridique législative pour l'échange de données à caractère personnel.

Toutefois, ces recommandations ne constituent pas une liste exhaustive des garanties dont la mise en œuvre serait, à elle seule, suffisante pour assurer le respect de la directive. Comme le précise son article 25, paragraphe 2, on apprécie *au cas par cas* les garanties qui devraient être prévues, après avoir examiné le contexte dans lequel se déroule l'échange de données, les règles en matière de protection des données qui sont déjà en vigueur dans le pays destinataire, et les risques auxquels l'échange est potentiellement exposé.

4. Les garanties qui devraient toujours être prévues dans le contexte de l'échange automatique de données à caractère personnel à des fins fiscales

Base juridique

L'échange de données à caractère personnel doit être régi par une base juridique claire, que ce soit un acte législatif ou un accord international. Il est essentiel que toute loi ou tout accord soit accessible aux citoyens et prévisible dans son application, conformément aux exigences de l'article 8 de la CEDH. Ces instruments doivent contenir des dispositions matérielles qui mettent en œuvre (au lieu de simplement s'y référer) la directive et/ou le droit national en matière de protection des données qui la transpose. Il importe également que les procédures nationales prévoyant la participation des parlements respectifs - et par la suite des autorités nationales chargées de la protection des données - soient pleinement respectées afin de créer une base juridique démocratique, claire et prévisible.

Limitation de la finalité

Conformément à l'article 6 de la directive, tout accord international devrait préciser clairement les finalités pour lesquelles les données sont collectées et valablement utilisées. La formulation relative à la finalité («évasion fiscale»/«amélioration du respect des obligations fiscales»), par exemple, peut paraître vague et insuffisamment claire, et de nature à donner trop de souplesse à l'autorité compétente. Il n'est pas aisé de déterminer si parmi ces finalités figurent, par exemple, les actes légaux tendant à l'évasion fiscale, les actes illégaux d'évasion fiscale ou les infractions financières (graves).

Les citoyens doivent toujours être conscients de la finalité exacte du traitement dont font l'objet les données les concernant et cette finalité doit servir de paramètre pour apprécier la nécessité et la proportionnalité (et, partant, la légalité) de l'échange de données.

Nécessité et proportionnalité

La nécessité et la proportionnalité du traitement des données ont fait l'objet d'une attention toute particulière dans l'arrêt rendu par la Cour de justice dans l'affaire *Digital Rights Ireland* (voir ci-dessus).

Tandis que cette affaire portait sur la nécessité et la proportionnalité de certaines mesures de lutte contre le terrorisme, le groupe «Article 29» est d'avis que l'exercice de mise en balance prescrit par la Cour de justice s'applique à toute politique publique mise en œuvre (notamment les politiques de coopération en matière fiscale) ayant une incidence sur les droits à la protection des données à caractère personnel. Aussi est-il impératif, dans les accords de coopération en matière

fiscale, de faire la démonstration que l'échange de données prévu est nécessaire et qu'il porte sur la quantité minimale de données requise pour atteindre l'objectif visé¹⁰.

En conséquence, les accords de coopération en matière fiscale devraient comporter des dispositions et des critères qui lient explicitement l'échange d'informations et, en particulier, la communication de données à caractère personnel concernant des comptes financiers à une possible évasion fiscale et qui dispensent les comptes à faible risque des obligations déclaratives. À cet égard, ces critères devraient être applicables *ex ante* pour déterminer les comptes (et les informations) qu'il conviendrait de déclarer.

Dans ce contexte, le recours à des mécanismes électroniques de diligence raisonnable, si leur application n'est pas limitée, pourrait conduire à un traitement disproportionné des données à caractère personnel. Compte tenu du fait qu'une recherche électronique peut avoir une incidence non-négligeable sur les données à caractère personnel, nous proposons que soient clairement indiquées - dans les dispositions d'un accord de coopération - les circonstances susceptibles de nécessiter l'exécution d'une recherche électronique et les objectifs d'une telle opération (par exemple, la localisation du lieu de résidence d'un titulaire de compte).

Conservation des données

La proportionnalité devrait également guider la conservation des données. Le groupe de travail «Article 29» rappelle que, compte tenu de la jurisprudence de la CJUE, les législations et les pratiques nationales en matière de conservation des données devraient garantir que toute décision de conserver des données à caractère personnel fait l'objet d'une différenciation, de limitations ou d'exceptions appropriées, et indique clairement le lieu de stockage des données. La Cour a également souligné que la conservation de données hors de l'Union empêcherait le plein exercice du contrôle, explicitement exigé par l'article 8, paragraphe 3, de la Charte, par une autorité indépendante, qui constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel¹¹.

L'indication d'un délai de conservation explicite pour les données à caractère personnel collectées et échangées garantit que ces données sont conservées durant le temps strictement nécessaire à la poursuite d'objectifs légitimes et, qu'une fois ce résultat atteint, elles sont supprimées, les droits individuels étant ainsi pleinement restaurés. Si tel n'était pas le cas, l'échange massif et continu d'informations fiscales sur les citoyens se traduirait par des archives volumineuses qui seraient difficiles à maîtriser et qui pourraient leur porter préjudice.

Les accords de coopération en matière fiscale devraient, dès lors, clairement indiquer pour combien de temps les informations fiscales devraient être conservées, afin de lutter contre l'évasion fiscale. Ils doivent aussi prévoir explicitement la suppression de ces informations dès l'arrivée à expiration du délai de conservation.

Transparence, traitement loyal et droits de la personne concernée

Il conviendrait de faire en sorte que grâce à des informations claires et appropriées, les personnes

¹⁰ Voir l'avis 01/2014 du groupe de travail sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_fr.pdf

¹¹ Voir l'arrêt de la Cour de justice du 8 avril 2014, dans les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 68.

concernées soient en mesure de comprendre ce qu'il advient de leurs données à caractère personnel et comment elles peuvent exercer leurs droits, comme le prévoient les articles 10 et 11 de la directive. Toute limitation de ces dispositions (ou d'un droit de la personne concernée) ou toute exception à ceux-ci doit être circonscrite et dûment justifiée, ainsi que respecter les critères stricts énoncés à l'article 13 de la directive. Elle doit, en outre, être prescrite par la loi, comme indiqué par la jurisprudence *Bara* susmentionnée.

Responsabilité

Les responsables du traitement des données (et, le cas échéant, les sous-traitants des données) devraient être clairement identifiés/désignés dans l'accord portant sur l'échange de données. Une attribution correcte de la responsabilité constitue, en effet, une étape capitale garantissant la possibilité de demander des comptes aux entités qui procèdent au traitement des données. Il sera, dès lors, plus aisé d'assurer le respect des principes qui sous-tendent la protection des données et les personnes concernées pourront plus facilement exercer leurs droits¹².

Transferts ultérieurs

Les responsables du traitement des données impliqués dans l'échange de données devraient être informés et adopter des garanties à l'égard d'éventuels transferts de données ayant lieu après le premier échange. Ils doivent veiller en particulier à ce que les données ne soient pas utilisées à des fins de poursuite pénale en général, sans garanties appropriées. L'autorité de contrôle compétente et les personnes concernées devront également avoir connaissance des informations relatives aux transferts ultérieurs, de sorte qu'il leur sera plus facile de faire valoir des droits de recours et d'accès.

Mesures de sécurité

L'échange transfrontière de données à caractère personnel peut entraîner une augmentation exponentielle des risques inhérents au traitement des données à caractère personnel au vu de la masse d'informations recueillies. Des mesures de sécurité strictes doivent être prises, notamment afin d'éviter la destruction accidentelle ou illicite, la diffusion ou l'accès non autorisés, et toute autre forme de traitement illicite conformément à l'article 17 de la directive.

À la lumière du nouveau cadre qui se dessine dans la proposition de règlement général sur la protection des données¹³, le groupe de travail «Article 29» souligne l'importance que revêt l'introduction de notifications de violation de données aux personnes concernées et aux autorités chargées de la protection des données du pays effectuant le transfert.

Compte tenu de la nature sensible des informations fiscales (qui peuvent révéler des aspects de la vie et des activités des citoyens), les accords de coopération en matière fiscale doivent énoncer explicitement les normes de sécurité auxquelles doivent se conformer les autorités procédant à des échanges de données systémiques.

Ainsi que la Cour l'a déclaré (voir le point ci-dessus sur la conservation des données, au vu des

¹² (Voir l'avis 1/2010, WP 169, du groupe de travail «Article 29» qui expose dans les grandes lignes la notion de «responsable du traitement des données» et son interaction avec celle de «sous-traitant des données», ainsi que les implications qui en découlent en ce qui concerne l'attribution des responsabilités; l'avis en question peut être consulté à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf)

¹³ Voir la proposition de règlement général sur la protection des données, document COM/2012/011 final - 2012/0011 (COD).

normes de sécurité élevées prévues par la directive 95/46/CE, il conviendrait d'héberger le serveur traitant ces données sur le territoire de l'UE (ou d'utiliser le système de traitement des données de la Commission au titre de la directive 2014/107/UE modifiant la directive 2011/16/UE).

La démarche consistant à combiner la technologie et la protection des données et à concevoir dès le départ un système respectueux de la vie privée - plutôt qu'à appliquer les règles en matière de protection des données *ex post* - illustre l'approche du *respect de la vie privée dès la conception* propre à améliorer le niveau de protection des données.

Analyse d'impact sur la vie privée

Chaque État membre devrait envisager de mettre en œuvre une analyse d'impact sur la vie privée afin de veiller à ce que les garanties en matière de protection des données soient correctement prises en compte et qu'une norme cohérente soit appliquée aux accords de coopération en matière fiscale par tous les pays de l'UE¹⁴.

Le traitement des informations fiscales à d'autres fins

Les données à caractère personnel ne peuvent être traitées que pour une finalité explicite, précise et légitime. Le traitement ultérieur à d'autres fins n'est possible que si ces finalités sont compatibles avec la finalité initiale (article 6 de la directive). Il est donc nécessaire de préciser la finalité du traitement et d'adopter des règles qui limitent la circulation des données et en empêchent l'utilisation à des fins secondaires.

Les informations échangées, y compris les données à caractère personnel, ne doivent être communiquées selon le principe du «besoin d'en connaître» qu'aux personnes ou autorités concernées, dans cette juridiction, par l'établissement, la perception ou le recouvrement de l'impôt, l'exécution des décisions, l'engagement des poursuites ou la détermination des recours en matière fiscale, ou encore la surveillance à laquelle ces tâches sont soumises. Seules les personnes ou les autorités mentionnées ci-dessus peuvent utiliser les informations et uniquement aux fins indiquées dans la phrase précédente.

À l'inverse, les informations échangées ne devraient pas être utilisées à d'autres fins qui seraient incompatibles - pas même lorsque cela est possible en vertu de la législation du pays qui fournit les informations et que l'autorité compétente de ce pays en a donné l'autorisation. Le problème, à cet égard, ne tient pas tant au fait que d'autres utilisations sont possibles dans le pays émetteur qu'au fait que, en application de cette disposition, d'autres utilisations deviennent possibles dans le pays destinataire selon des modalités potentiellement préjudiciables aux droits individuels. Une telle malléabilité des finalités restreint les droits individuels à la protection des données à caractère personnel, car la finalité du traitement des données devrait être déterminée, explicite et légitime, et communiquée *ex ante* à la personne concernée.

L'échange de données à caractère personnel et les droits de la personne concernée

Les accords de coopération en matière fiscale devraient préciser que la personne concernée doit être informée d'un échange de données dans un délai raisonnable avant qu'il ait effectivement lieu (de sorte qu'elle ait le temps de se défendre le cas échéant). Les informations fournies

¹⁴ Voir l'annexe de la lettre du groupe «Article 29» du 18.09.2014 sur la norme commune de déclaration de l'OCDE: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140918_annex_oecd_common_reporting_standard.pdf.pdf

devraient, au minimum, informer les personnes concernées du fait que leurs données à caractère personnel seront transmises à une autorité compétente aux fins de lutter contre l'évasion fiscale, comporter une liste de la catégorie de données envoyées, une liste des autorités destinataires dans plusieurs pays et les coordonnées du responsable du traitement dans leur pays de résidence, et les informer quant à leur droit d'opposition et leur droit de recours.

Clauses diverses

Lors de la rédaction d'un accord de coopération fiscale reposant sur l'échange de données à caractère personnel, les parties devraient également envisager l'introduction de mécanismes de surveillance et de mise en conformité, comprenant les éléments suivants:

- une clause du tiers bénéficiaire (afin que la personne concernée puisse agir contre une violation des obligations du responsable du traitement et du destinataire des données);
- une définition claire des obligations du responsable du traitement et du destinataire (par exemple, l'obligation de répondre aux demandes d'information, de fournir un exemplaire des clauses aux personnes concernées, de se soumettre à un examen, un audit, etc.);
- une clause de responsabilité;
- la désignation du droit applicable;
- le pouvoir pour l'autorité de protection des données compétente de bloquer ou de suspendre les échanges.

Si la législation en matière de protection des données en vigueur dans les États membres destinataires ne le prévoit pas déjà, il convient d'adopter d'autres engagements en matière de surveillance et de mise en conformité concernant à la fois le responsable du traitement et le destinataire, tels que:

- la vérification directe par les autorités (par exemple, sous la forme d'inspections conjointes, d'audits effectués par des organismes indépendants, etc.) ou par le responsable du traitement (par exemple, sous la forme d'audits);
- l'obligation de désigner un délégué à la protection des données indépendant;
- un examen indépendant des réclamations (désignation de points de contact pour les demandes d'information);
- des sanctions dissuasives, des voies de recours appropriées et le respect des décisions de justice;
- une clause de responsabilité (obligation de fournir une preuve de conformité à l'autorité compétente en matière de protection des données, soit à sa demande, soit à intervalles réguliers);
- la transparence des garanties (par exemple, à travers la publication des instruments sur l'internet);
- la dénonciation de l'accord, de la convention, etc. en cas de violation.

En conclusion, étant donné que la rédaction de clauses spéciales peut s'avérer très complexe, nous recommandons aux autorités fiscales compétentes qui négocient des accords de coopération fiscale avec d'autres pays de consulter les autorités nationales chargées de la

protection des données¹⁵ afin d'assurer l'application cohérente des garanties en matière de protection des données mentionnées plus haut.

ANNEXE

Questionnaire adressé aux autorités fiscales nationales sur l'échange automatique de données à des fins fiscales

Veillez noter que les questions suivantes se rapportent aux accords bilatéraux/multilatéraux existants qui prévoient l'échange automatique d'informations à des fins fiscales. Toutefois, dans la mesure du possible, une réponse tenant également compte d'éventuelles négociations en cours pour des accords futurs serait appréciée.

1. Le FATCA et les autres outils internationaux - Le statut des accords internationaux dans votre pays et la coopération avec les établissements financiers et les compagnies d'assurance

1.1. L'autorité fiscale de votre pays a-t-elle signé un accord (bilatéral ou multilatéral) avec le gouvernement des États-Unis d'Amérique en vertu du Foreign Account Tax Compliance Act (FATCA), ou avec toute autre autorité extérieure à l'UE sur l'échange automatique d'informations à des fins fiscales?

1.2. Dans l'affirmative, veuillez fournir une liste de ces autorités et une copie des accords.

1.3 Dans l'affirmative, cet accord, ou du moins ses dispositions relatives au transfert automatique d'informations, est-il contraignant tant pour votre autorité que pour l'autorité destinataire, notamment en ce qui concerne le caractère opposable des droits des personnes concernées dans le pays destinataire?

1.4. Dans la négative, quel est l'état actuel des négociations portant sur des accords concernant le transfert automatique d'informations?

1.5. Veuillez indiquer dans quelle mesure l'autorité compétente de votre pays a coopéré avec les représentants locaux des établissements financiers et des compagnies d'assurance qui sont soumis à la législation internationale sur l'échange automatique d'informations à des fins fiscales.

1.6. Dans ce contexte, des accords ou des arrangements (publics) ont-ils été conclus avec le secteur privé, et comment ces discussions se traduisent-elles dans votre législation nationale?

2. La norme commune de déclaration de l'OCDE

2.1. La norme commune de déclaration de l'OCDE (NCD) fixe des normes de diligence raisonnable permettant aux établissements financiers de déterminer les «comptes déclarables», et prévoit un «modèle d'accord entre autorités compétentes» que les États peuvent utiliser pour l'échange d'informations à des fins fiscales. Votre cadre juridique national prévoit-il/envisage-t-il de prévoir la mise en œuvre de l'échange automatique d'informations à des fins fiscales comme prévu par la NCD?

¹⁵ Les coordonnées des autorités chargées de la protection des données sont disponibles à l'adresse suivante: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_fr.htm

2.2. Dans l'affirmative, veuillez fournir une copie de l'accord.

2.3. L'autorité compétente de votre pays fait-elle/envisage-t-elle de faire usage du modèle d'accord entre autorités compétentes comme base à l'échange de données?

2.4. Dans l'affirmative, quelle définition votre cadre juridique donne-t-il des «comptes à faible risque» à exclure de la collecte de données?

3. Les instruments de coopération administrative de l'UE dans le domaine de la fiscalité (directive 2011/16/UE et directive 2014/107/UE)

3.1. Votre pays a-t-il transposé la directive 2011/16/UE relative à la coopération administrative dans le domaine fiscal?

3.2. La directive 2011/16/UE relative à la coopération administrative dans le domaine fiscal a été modifiée récemment par la directive 2014/107/UE. Quand et comment la transposition de cette directive est-elle prévue?

4. L'objectif d'harmonisation au niveau de l'UE

4.1. Prévoyez-vous ou salueriez-vous des actions d'harmonisation à l'échelle de l'UE vis-à-vis des approches adoptées dans d'autres États membres?

4.2. Dans l'affirmative, comment cette harmonisation à l'échelle de l'UE pourrait/devrait-elle être réalisée, selon vous, sur le plan de la protection des données?

a. Orientation assurée par le groupe «Article 29» sur le contenu relatif à la protection des données du cadre juridique de l'UE et/ou accords bilatéraux en matière fiscale

b. Application de la procédure prévue à l'article 218 du TFUE (la Commission présente une recommandation au Conseil d'ouvrir des négociations tout en consultant le groupe de travail «Article 29»). Pensez-vous qu'il soit nécessaire de modifier davantage la législation de l'UE, par exemple en y ajoutant des dispositions matérielles sur la protection des données? Dans l'affirmative, existe-t-il des articles dans le cadre juridique de l'UE portant sur le transfert automatique d'informations à des fins fiscales qu'il conviendrait, selon vous, de clarifier?

c. Adoption du nouveau règlement relatif à la protection des données en 2015

d. Approche informelle: discussions pratiques avec des représentants du groupe de travail «Article 29» et de la Commission européenne sur l'incidence de la jurisprudence de l'UE¹⁶ sur le contenu d'un tel régime et le contenu minimal en matière de protection des données des accords internationaux en matière fiscale afin de réduire le risque de décisions de justice négatives.

¹⁶ Par exemple: l'incidence de la décision de la grande chambre de la Cour de justice sur la directive sur la conservation des données: affaires C-293/12 et C-594/12, Digital Rights Ireland, Seitlinger e.o., publiée à l'adresse suivante <http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62012CJ02937>. Comme rappelé dans la note explicative du présent questionnaire, la décision de la Cour de justice a invalidé la directive 2006/24/CE (la «directive sur la conservation des données») au motif que les législateurs de l'Union européenne avaient outrepassé les limites de la proportionnalité lors de l'élaboration de cette directive.

5. L'existence de garanties en matière de protection des données

Comme l'a également précisé le groupe de travail «Article 29» dans l'annexe de la lettre adoptée le 18 septembre (voir la note explicative ci-dessus), il existe plusieurs principes en matière de protection des données - tels qu'interprétés aussi par la Cour de justice de l'Union européenne dans l'affaire relative à la conservation des données¹⁷ - que les pouvoirs publics et les institutions compétentes doivent prendre en compte pour s'assurer que l'échange automatique d'informations à des fins fiscales soit réalisé dans le respect des obligations relatives à la protection des données prévues par la directive 95/46/CE.

À cet égard, quelles sont les mesures actuellement conclues ou proposées (ou mises au point dans les négociations) afin de garantir la protection des données conformément au droit national et au droit de l'UE? Veuillez répondre en vous référant notamment aux principes suivants:

5.1. L'existence de garanties en matière de protection des données - Analyses d'impact relatives à la protection des données

5.1.1. Une analyse d'impact relative à la protection des données ou une consultation formelle de l'autorité nationale chargée de la protection des données est-elle envisagée et à quel stade?

5.1.2. Avez-vous réalisé une analyse d'impact relative à la protection des données durant les négociations d'accords internationaux en:

a. prenant contact avec l'autorité de votre pays chargée de la protection des données pour de plus amples informations

b. effectuant votre propre évaluation (veuillez indiquer le type d'orientation auquel vous avez eu recours: recommandations d'un conseil interne ou externe - cabinet d'avocats par ex. - opinion publique ou tout autre moyen.) Merci de bien vouloir nous communiquer également une copie ou un résumé du contenu de ces instructions afin que nous puissions vérifier au moins la synthèse de l'analyse d'impact relative à la protection des données.

c. autres (veuillez préciser)

5.2. L'existence de garanties en matière de protection des données - Base juridique en droit interne

5.2.1. Des accords bilatéraux ou multilatéraux, tels que des conventions fiscales, sont-ils conclus aux fins d'un échange d'informations, sous réserve d'une procédure de ratification formelle par votre parlement national?

5.2.2. Votre pays a-t-il adopté une loi nationale prévoyant la possibilité d'effectuer un transfert automatique de données à caractère personnel à des fins de lutte contre l'évasion fiscale vers des pays tiers?

5.2.3. Dans l'affirmative, veuillez indiquer les références de cette loi et préciser quels instruments au niveau international sont transposés.

¹⁷ Voir la note de bas de page précédente.

5.2.4. Dans la négative, avez-vous élaboré un premier projet de base juridique pour le transfert automatique? L'autorité de votre pays chargée de la protection des données a-t-elle pris part à ce processus? Dans la négative, à quel stade envisagez-vous sa participation? Existe-t-il un calendrier pour la procédure législative? Quand l'entrée en vigueur de la loi est-elle prévue?

5.3. L'existence de garanties en matière de protection des données - Les données à échanger

5.3.1. Pour chaque personne, la collecte de données concerne-t-elle uniquement la totalité des comptes détenus à une date donnée ou couvre-t-elle également chaque mouvement effectué sur les comptes?

5.3.2. Quelles sont les données collectées (comptes courants; comptes de dépôt; cartes de crédit; participations; biens personnels et biens immobiliers, etc.) et quels sont les critères permettant de déterminer les données qui doivent être collectées?

5.3.3. L'autorité compétente de votre pays a-t-elle créé une base de données (et, de ce fait, reproduit) les données collectées?

5.3.4. Votre droit interne contient-il des dispositions relatives à:

a. la détermination du champ d'application (les données à échanger)

b. la qualité des données (c'est-à-dire les principes de proportionnalité, de minimisation des données, d'exactitude des données, le délai maximal de conservation, etc. - *le contenu relatif à ces principes est développé plus en détail ci-dessous*).

5.4. L'existence de garanties en matière de protection des données - Proportionnalité¹⁸

5.4.1. Quel est le dispositif prévu pour éviter que les parties aient recours à la «pêche aux informations» ou réclament des informations peu susceptibles de présenter un intérêt pour les affaires fiscales d'une personne donnée ou d'un groupe ou d'une catégorie de personnes déterminé?¹⁹

5.4.2. Comment l'échange automatique d'informations a-t-il lieu en pratique? Veuillez décrire la technique employée et ce qu'elle signifie en pratique (des mécanismes de filtrage sont-ils déjà en place pour l'échange de données ou des identifiants uniques sont-ils utilisés?, etc.).

¹⁸ Sur la base de la décision de la Cour de justice invalidant la directive sur la conservation des données (voir la note de bas de page précédente), afin de ne pas violer le principe de proportionnalité, il est nécessaire de faire la démonstration que le traitement prévu est nécessaire et que les données requises constituent le minimum nécessaire pour atteindre le but recherché et éviter ainsi des opérations de collecte et de transfert indifférenciées et massives.

¹⁹ Observations sur l'article 4 de la convention du 25 janvier 1988 de l'OCDE et du Conseil de l'Europe concernant l'assistance administrative mutuelle en matière fiscale, publiées à l'adresse suivante: <http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/127>

5.4.3. Quel est votre avis sur la nécessité du transfert automatique d'informations visant à lutter contre l'évasion fiscale?

5.4.4. Des mécanismes bilatéraux d'échange automatique sont-ils bien en place avec tous vos homologues dans les pays étrangers? En d'autres termes, recevez-vous automatiquement de la part de tous les pays les données relatives aux personnes concernées relevant de la législation de votre pays²⁰?

5.5. L'existence de garanties en matière de protection des données - Conservation des données

5.5.1. Votre législation prévoit-elle un délai de conservation des données précis? Dans l'affirmative, veuillez indiquer les délais de conservation minimaux et maximaux.

5.5.2. Combien de temps stockez-vous les données reçues des établissements, des compagnies d'assurance, etc.? Combien de temps stockez-vous les données que vous recevez automatiquement d'autres pays qui participent également à l'échange automatique?

5.5.3. Existe-t-il une procédure de suppression ou de correction des données obsolètes ou erronées?

5.6. L'existence de garanties en matière de protection des données - Le responsable du traitement des données

5.6.1. Quelles décisions l'autorité compétente de votre pays prend/a-t-elle pris pour la transmission des données aux fins de lutter contre l'évasion fiscale?

5.6.2. En particulier: l'autorité compétente de votre pays fournit/prévoit-elle de fournir des services de stockage de données pour le transfert automatique d'informations à ses homologues étrangers? En d'autres termes, dans quelle mesure l'autorité compétente de votre pays stocke-t-elle les données transmises par les établissements nationaux (banques, compagnies d'assurance, etc.) lorsque ces établissements sont soumis aux législations étrangères concernant le transfert automatique d'informations à des fins fiscales (par exemple, le FATCA ou autres)?

5.6.3. En particulier: l'autorité compétente de votre pays fournit/prévoit-elle de fournir des services de stockage pour les données que vous recevez automatiquement de la part d'autres pays? Dans l'affirmative, veuillez décrire le traitement ultérieur de ces données.

5.6.4. En pareil cas, l'autorité compétente de votre pays assume-t-elle l'entière responsabilité dévolue au «responsable du traitement des données»²¹ prévue par la directive 95/46/CE à l'égard des personnes concernées?

²⁰ C'est-à-dire les personnes concernées qui sont soumises à la législation fiscale de votre pays bien qu'elles exercent des activités économiques ou perçoivent un revenu hors de votre pays.

²¹ Voir l'article 2, point d), de la directive 95/46/CE.

5.6.5. Dans la négative, estimez-vous que (seuls) les établissements ou d'autres parties sont assimilables à des responsables du traitement des données au sens de la directive 95/46/CE? Pourquoi?

5.7. L'existence de garanties en matière de protection des données - Transparence/Obligation d'informer et réciprocité vis-à-vis des personnes concernées relevant de la législation de votre pays

5.7.1. Toutes vos lois nationales et dispositions internationales ayant trait au transfert automatique de données à caractère personnel sont-elles publiées? Veuillez nous en transmettre une liste.

5.7.2. Exigez-vous des autorités étrangères qu'elles informent les personnes concernées qui sont soumises à la législation fiscale de votre pays du fait que leurs données sont traitées aux fins de lutter contre l'évasion fiscale?

5.7.3. Dans la négative, informez-vous vous-mêmes les personnes concernées dès réception des informations communiquées par vos homologues étrangers?

5.7.4. Dans la négative, quelle est la raison de l'inapplication de l'obligation d'informer les personnes concernées qui sont soumises à votre propre législation fiscale?

5.8. L'existence de garanties en matière de protection des données - Définition et limitation de la finalité

5.8.1. Votre régime fiscal national prévoit-il une définition claire et précise de l'«infraction fiscale»?

5.8.2. Dans la négative, pourquoi pas?

5.8.3. Votre législation relative à l'échange automatique d'informations prévoit-elle une limitation claire de l'utilisation des informations échangées à des fins fiscales uniquement? En d'autres termes, l'utilisation des informations échangées à des fins autres que fiscales est-elle exclue (blanchiment de capitaux, corruption, financement du terrorisme, etc.)? Les conditions d'utilisation à d'autres fins éventuelles sont-elles prévues? Dans l'affirmative, lesquelles?

5.8.4. Dans la négative, votre législation nationale accorde-t-elle une attention suffisante à d'autres instruments juridiques qui existent déjà au niveau national ou de l'UE, et auxquels il conviendrait de recourir en cas d'utilisation d'informations en matière pénale? Autrement dit, votre législation nationale prend-elle en compte la possibilité d'échanger des informations de droit pénal fiscal sur la base de traités bilatéraux ou multilatéraux²² en matière d'entraide judiciaire (dans la mesure où ils s'appliquent également aux infractions fiscales), ainsi que sur la base de la législation interne régissant l'octroi de cette entraide²³?

²² Voir, entre autres, la convention européenne du 20 avril 1959 concernant l'assistance mutuelle en matière pénale, publiée à l'adresse suivante: <http://www.conventions.coe.int/Treaty/fr/Treaties/Html/030.htm>

²³ Voir la remarque relative à l'article 1^{er}, paragraphe 1, de la convention du 25 janvier 1988 de l'OCDE et du Conseil de l'Europe concernant l'assistance administrative mutuelle en matière fiscale, publiée à l'adresse

5.8.5. Cette garantie limitant la finalité s'applique-t-elle aussi aux transferts ultérieurs effectués par l'autorité destinataire à des autorités tierces?

5.9. L'existence de garanties en matière de protection des données - Les droits des personnes concernées

5.9.1. Votre législation nationale prévoit-elle la possibilité de faire valoir des droits directs d'accès, de rectification et d'opposition en vertu des articles 12 à 14 de la directive 95/46/CE à l'égard de l'autorité compétente de votre pays? Dans l'affirmative, veuillez décrire cette procédure.

5.9.2. Existe-t-il des restrictions/exceptions aux droits des personnes concernées? Dans l'affirmative, pourquoi et quelles sont les garanties encadrant l'application d'une exception? En particulier, votre législation prévoit/envisage-t-elle de prévoir de limiter la portée des obligations et des droits prévus à l'article 10, à l'article 11, paragraphe 1, et aux articles 12 et 21 de la directive 95/46/CE, comme l'exige l'article 25 de la directive 2011/16/UE?

5.9.3. Votre législation nationale prévoit-elle la possibilité de faire valoir des droits directs d'accès, de rectification et d'opposition en vertu des articles 12 à 14 de la directive 95/46/CE à l'égard des établissements financiers, des compagnies d'assurance, etc.?

5.10. L'existence de garanties en matière de protection des données - La sécurité des données²⁴

5.10.1. Quelles mesures de sécurité sont (devraient être) en place? Veuillez les décrire succinctement.

5.10.2. Quel type de contrôle (préventif et/ou ex post) est réalisé pour assurer l'adoption en bonne et due forme de mesures de sécurité?

5.10.3. Veuillez décrire les paramètres techniques applicables aux mesures de cryptage/d'intégrité/de traçabilité des échanges qui existent pour garantir le transfert et le stockage de données à caractère personnel.

5.11. L'existence de garanties en matière de protection des données - La responsabilité assurée au moyen de la notification des atteintes à la sécurité

5.11.1. Votre législation nationale prévoit-elle l'obligation d'informer l'autorité compétente (autorité chargée de la protection des données ou autre) et/ou les personnes concernées en cas

suivante: <http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/127>, et sur l'accord bilatéral conclu en matière d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique du 25 juin 2003, JO L 181 du 19 juillet 2003, p. 34.

²⁴ Il convient de ne pas perdre de vue les implications potentielles des options techniques qui pourraient être retenues pour mettre en œuvre l'échange automatique d'informations, notamment à la lumière de l'arrêt de la CJUE du 8 avril 2014 concernant la directive sur la conservation des données.

de manquement à la sécurité concernant les données traitées à des fins fiscales? Une telle obligation est-elle prévue pour les infractions au niveau du stockage des données?

5.11.2. Cette obligation s'applique-t-elle au secteur privé (établissements financiers, compagnies d'assurance, etc.) et/ou au secteur public (votre administration fiscale)?

5.12. L'existence de garanties en matière de protection des données - Le délégué à la protection des données

5.12.1. L'autorité compétente de votre pays a-t-elle désigné un délégué à la protection des données («DPD») chargé de traiter des questions, réclamations, demandes d'accès/de rectification concernant le transfert automatique d'informations des personnes concernées?

5.12.2. Dans l'affirmative, la description des fonctions et les compétences du DPD sont-elles établies par la loi?

5.12.3. Dans la négative, pourquoi pas?

5.12.4. Le DPD prend-il part au processus législatif pour signaler des problèmes en matière de protection des données à un stade précoce?

5.12.5. À votre connaissance, les établissements et les compagnies d'assurance ont-ils désigné un DPD pour traiter de questions semblables à celles mentionnées ci-dessus?

5.13. L'existence de garanties en matière de protection des données - Les catégories particulières de données - La protection des données à caractère personnel en cas de soupçon de fraude

5.13.1. Quelles sont les garanties applicables à l'échange de catégories particulières de données, telles que prévues à l'article 8 de la directive 95/46, en particulier des données relatives à des infractions, des condamnations pénales ou des sanctions? Quelles sont les garanties prévues pour l'échange d'informations en cas de soupçon de fraude?

5.14. L'existence de garanties en matière de protection des données - Les possibilités de recours

5.14.1. Les données faisant l'objet d'un échange automatique sont-elles soumises à un contrôle légal au niveau national (DPD national ou autorité judiciaire ou administrative nationale)?

5.14.2. En particulier, un recours est-il possible en cas de traitement et de transmission erronés/illicites?

5.14.3. Comment la responsabilité est-elle répartie entre les établissements financiers et les autorités fiscales?

5.14.4. Le plein exercice du contrôle par une autorité indépendante est-il assuré dans le cas d'un transfert de données vers un pays tiers, comme requis expressément par l'article 8,

paragraphe 3, de la Charte des droits fondamentaux de l'UE et souligné par la Cour de justice dans cette affaire de conservation des données²⁵?

5.15. L'existence de garanties en matière de protection des données - Les autres garanties

5.15.1. Existe-t-il une clause de caducité²⁶/dénonciation dans les accords bilatéraux pour mettre fin aux accords conclus en cas de survenance de l'un des événements suivants: entrée en vigueur du règlement européen sur la protection des données, entrée en vigueur d'une autre mesure d'harmonisation au niveau de l'UE et/ou autre?

5.15.2. Prévoyez-vous une action de suivi dans les années à venir pour tenir compte des changements qui devraient être mis en œuvre par le règlement de l'UE annoncé sur la protection des données?

²⁵Dans sa décision du 8 avril 2014 invalidant la directive sur la conservation des données, la Cour a souligné que la conservation de données hors de l'UE empêcherait le plein exercice du contrôle expressément prévu par l'article 8, paragraphe 3, de la Charte, par une autorité indépendante, qui est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

²⁶Une disposition ou clause de caducité est une mesure prévue dans une loi, un règlement ou un autre instrument normatif qui prévoit que la loi cesse de produire ses effets à partir d'une certaine date, à moins que de nouvelles mesures législatives soient prises pour en prolonger la validité. La plupart des lois ne contenant pas de clauses de caducité, elles restent en vigueur sans limitation de durée.