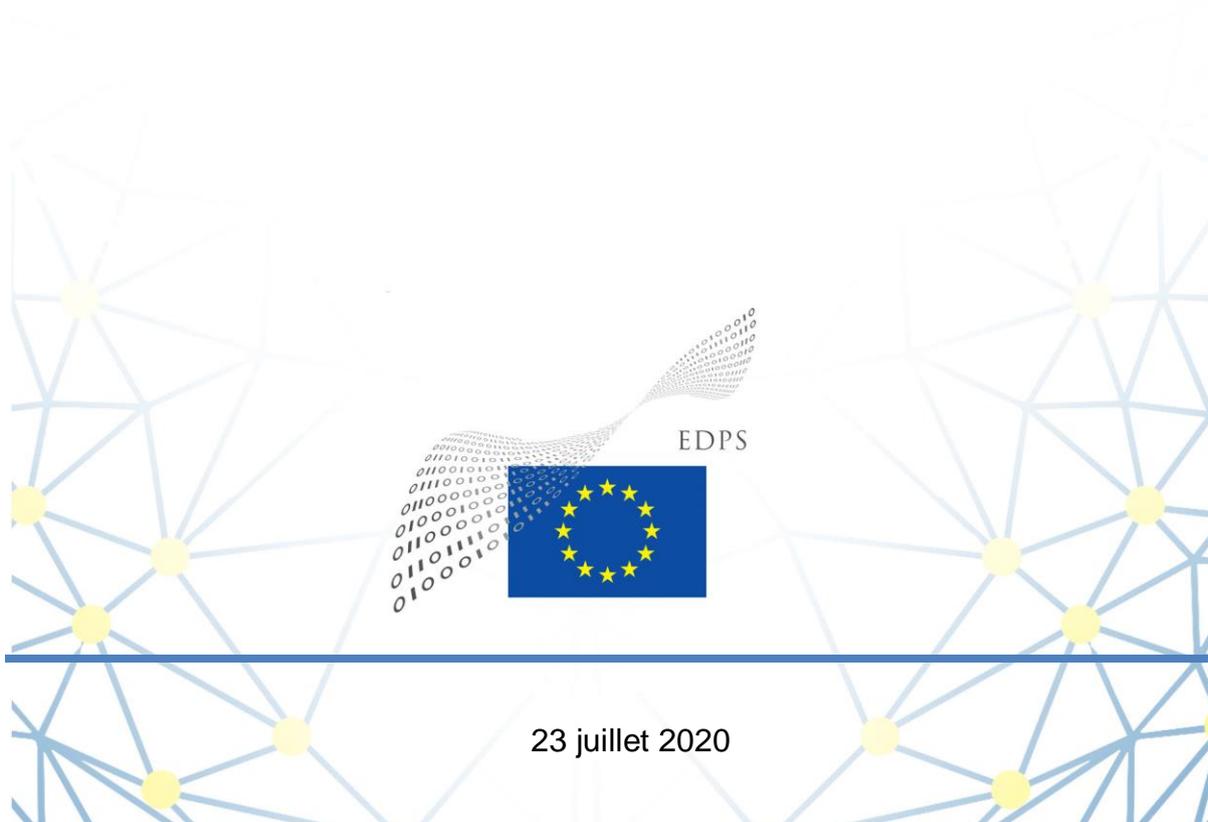


EUROPEAN DATA PROTECTION SUPERVISOR

# Avis 5/2020

**sur le plan d'action de la Commission européenne pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme**



23 juillet 2020

*Le Contrôleur européen de la protection des données (CEPD) est une autorité indépendante de l'Union européenne, qui est chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». En vertu de l'article 58, paragraphe 3, point c), du règlement (UE) 2018/1725, le CEPD dispose du pouvoir d'«émettre, de sa propre initiative ou sur demande, des avis à l'attention des institutions et organes de l'Union ainsi que du public, sur toute question relative à la protection des données à caractère personnel».*

*Wojciech Wiewiorowski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.*

## Synthèse

Le 7 mai 2020, la Commission a publié une communication sur un plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme [C(2020) 2800 final], qui définit une feuille de route pour la réalisation de ses objectifs en la matière. Dans le présent avis, le CEPD évalue les incidences en matière de protection des données des initiatives prévues dans le plan d'action de la Commission.

Bien que le CEPD reconnaisse l'importance de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC-FT) en tant qu'objectif d'intérêt général, il demande que la législation ménage un équilibre entre, d'une part, l'atteinte aux droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel et, de l'autre, les mesures nécessaires pour atteindre efficacement les objectifs d'intérêt général concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme (principe de proportionnalité).

Le CEPD recommande à la Commission de contrôler la mise en œuvre effective du cadre LBC-FT existant, tout en garantissant le respect du RGPD et du cadre de protection des données, ainsi que la conformité avec ces derniers. Cela est particulièrement pertinent en ce qui concerne les travaux relatifs à l'interconnexion des mécanismes centralisés pour les comptes bancaires et des registres des bénéficiaires effectifs, qui devraient largement s'inspirer des principes de minimisation des données, d'exactitude et de protection de la vie privée dès la conception et par défaut.

Le CEPD se félicite de l'harmonisation envisagée du cadre LBC-FT, car celle-ci permettra une application plus cohérente des principales règles par les États membres ainsi qu'une interprétation uniforme de la part de la Cour de justice de l'Union européenne. Le CEPD invite la Commission à suivre l'approche fondée sur les risques lorsqu'elle décide des nouvelles mesures du corpus réglementaire renforcé, étant donné que cette approche est aussi conforme aux principes en matière de protection des données.

Le CEPD recommande à la Commission de prévoir, dans sa proposition d'instauration de l'autorité de surveillance LBC-FT de l'Union européenne, une base juridique spécifique lui permettant de traiter des données à caractère personnel ainsi que les garanties nécessaires en matière de protection des données conformément au RGPD et au règlement (UE) 2018/1725, en particulier concernant le partage d'informations et les transferts internationaux de données.

Le CEPD se réjouit de l'initiative de la Commission de stimuler le développement de FIU.net et de trouver une solution valable pour sa gestion qui soit conforme au RGPD et au cadre de protection des données. Par ailleurs, le CEPD recommande que, dans la proposition de création d'un mécanisme de coordination et de soutien pour les cellules de renseignement financier (CRF), les conditions d'accès aux informations sur les transactions financières et de partage de ces dernières par les CRF soient clarifiées.

Le CEPD soutient la création de partenariats public-privé (PPP) pour la recherche et l'analyse des typologies et des tendances relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, dans le respect des limites du RGPD. En revanche, et bien que le CEPD ne souhaite exprimer aucun jugement de fond sur les objectifs stratégiques sous-tendant l'initiative, il considère que les PPP visant au partage d'informations

**opérationnelles – des services répressifs aux entités assujetties – sur les suspects détectés par le renseignement entraîneraient un risque élevé pour les droits au respect de la vie privée et à la protection des données. De plus, les opérations de traitement concernant des informations sur de possibles infractions découlant de transactions financières devraient rester dans les limites des autorités compétentes et ne pas être partagées avec des entités privées.**

**Le CEPD salue les efforts consentis par la Commission pour jouer un rôle plus important au sein du Groupe d'action financière et pour parler d'une seule voix. Il encourage la Commission à s'efforcer de faire des principes en matière de protection des données une partie intégrante des processus relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme lorsqu'elle fixe des normes internationales en la matière.**

**Enfin, le CEPD s'attend à être consulté, conformément à l'article 42 du règlement (UE) 2018/1725, à la suite de l'adoption de propositions d'acte législatif ayant une incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel. Parmi celles-ci figurent notamment les futures propositions de règlement sur les mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme, établissant un mécanisme de coordination et de soutien pour les CRF et instaurant l'autorité de surveillance de l'Union européenne.**

## TABLE DES MATIÈRES

### Table des matières

1. INTRODUCTION ET CONTEXTE.....	6
2. OBSERVATIONS GÉNÉRALES .....	7
2.1 Le principe de proportionnalité. Ménager un équilibre entre la protection des données à caractère personnel et la lutte contre le blanchiment de capitaux et le financement du terrorisme.....	7
3. COMMENTAIRES ET RECOMMANDATIONS .....	8
3.1. Premier pilier: veiller à la mise en œuvre effective du cadre de l'UE existant en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.....	8
3.2. Deuxième pilier: mettre en place un corpus réglementaire renforcé .....	10
3.3. Troisième pilier: instaurer une surveillance de niveau européen .....	12
3.4. Quatrième pilier: créer un mécanisme de coordination et de soutien pour les CRF.....	13
3.5. Cinquième pilier: faire appliquer les dispositions de droit pénal et les dispositions en matière d'échange d'informations arrêtées au niveau de l'Union européenne .....	15
3.6. Sixième pilier: renforcer le rôle de l'Union européenne sur la scène mondiale.....	17
4. CONCLUSIONS .....	17
Notes .....	18

## **LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,**

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)<sup>1</sup>,

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données<sup>2</sup>, et en particulier son article 58, paragraphe 3, point c),

### **A ADOPTÉ L'AVIS SUIVANT:**

#### **1. INTRODUCTION ET CONTEXTE**

1. Le 7 mai 2020, la Commission européenne a adopté sa communication sur un plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme [C(2020) 2800 final] (le «plan d'action»). Ce plan d'action est une initiative prévue par l'objectif stratégique n° 21 du programme de travail de la Commission pour 2020, «Achèvement de l'union bancaire».
2. Le plan d'action se compose de six piliers, à savoir: 1) veiller à la mise en œuvre effective du cadre de l'UE existant en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme; 2) mettre en place un corpus de règles LBC-FT unique à l'échelle de l'UE; 3) instaurer une surveillance de niveau européen en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme; 4) créer un mécanisme de coordination et de soutien pour les cellules de renseignement financier; 5) faire appliquer les dispositions de droit pénal et en matière d'échange d'informations arrêtées au niveau de l'Union; et 6) renforcer la dimension internationale du cadre LBC-FT de l'UE. Afin de recueillir l'avis des citoyens et des parties prenantes sur ces mesures, le 7 mai, la Commission a lancé, parallèlement à l'adoption du plan d'action, une consultation publique<sup>3</sup> ouverte jusqu'au 29 juillet 2020.
3. Le plan d'action concrétise ces piliers par un certain nombre de mesures spécifiques, dont plusieurs propositions législatives concernant le corpus de règles LBC-FT unique à l'échelle de l'Union européenne, instaurant une autorité de surveillance LBC-FT de l'Union européenne et élaborant un mécanisme de coordination et de soutien pour les cellules de renseignement financier (les «CRF»). Le présent avis suit la structure en six piliers et présente l'avis du CEPD sur certaines mesures du plan d'action et, en particulier, sur leur atteinte potentielle aux droits au respect de la vie privée et à la protection des données des personnes physiques, tels qu'ils sont garantis par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. Le présent avis s'entend sans préjudice de l'obligation de la Commission de consulter le CEPD, conformément à l'article 42 du règlement (UE) 2018/1725, sur toute proposition législative susceptible d'être soumise dans le cadre du plan d'action ayant une incidence sur la protection du droit des personnes physiques à la protection des données à caractère personnel.

## 2. OBSERVATIONS GÉNÉRALES

### 2.1 Le principe de proportionnalité. Ménager un équilibre entre la protection des données à caractère personnel et la lutte contre le blanchiment de capitaux et le financement du terrorisme

4. Le CEPD reconnaît qu'il importe d'établir un cadre fort et de mettre en place des structures appropriées et efficaces dotées des moyens technologiques nécessaires pour accomplir leurs tâches relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Toutefois, ces objectifs légitimes et importants ne doivent pas être réalisés au détriment de la protection des droits relatifs à la vie privée et aux données à caractère personnel des personnes physiques, qui restent pleinement applicables. En effet, les exigences en matière de protection des données devraient être perçues comme des exigences fondamentales qui doivent être remplies dans le contexte des obligations ayant trait à la lutte contre le blanchiment de capitaux.
5. La jurisprudence de la Cour de justice européenne a confirmé que la lutte contre la criminalité grave constitue un objectif d'intérêt général<sup>4</sup> susceptible de justifier une atteinte aux droits fondamentaux au respect de la vie privée et à la protection des données garantis par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. Parallèlement, le pouvoir d'appréciation du législateur de l'Union est réduit, et la législation doit ménager un équilibre entre l'atteinte qui est réellement nécessaire et les droits au respect de la vie privée et à la protection des données à caractère personnel des personnes physiques (**proportionnalité**). Pour davantage d'orientations sur le principe de proportionnalité dans le contexte de la protection des données, le CEPD attire l'attention sur son **guide sur la nécessité**<sup>5</sup>, ainsi que sur ses **lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel**<sup>6</sup>.
6. Pour ce qui est du cadre législatif de l'Union relatif à la lutte contre le blanchiment de capitaux et le financement du terrorisme, il a évolué rapidement et s'est étendu au cours de ces dernières années. Des étapes majeures ont été introduites par les quatrième et cinquième directives anti-blanchiment (ci-après respectivement la «**quatrième directive anti-blanchiment**» et la «**cinquième directive anti-blanchiment**»), et l'avancée se poursuivra avec la transposition de la sixième directive anti-blanchiment<sup>7</sup> (ci-après la «**sixième directive anti-blanchiment**») d'ici 2021<sup>8</sup>. Le CEPD se félicite des modifications essentielles apportées par la sixième directive anti-blanchiment, qui sont conformes aux droits au respect de la vie privée et à la protection des données à caractère personnel, telles que l'obligation pour les autorités chargées des enquêtes ou des poursuites d'utiliser des outils d'enquête ciblés, de suivre une approche fondée sur les risques<sup>9</sup> (c'est-à-dire que les situations moins risquées justifient des procédures moins intrusives), ainsi que de tenir compte du principe de proportionnalité et de la nature et de la gravité des infractions qui font l'objet de l'enquête<sup>10</sup>.
7. Le CEPD a prodigué des conseils au cours de ces évolutions législatives et a adressé des recommandations spécifiques dans ses avis de 2013<sup>11</sup> et de 2017<sup>12</sup> (ci-après respectivement l'«**avis de 2013 sur le projet de quatrième directive anti-blanchiment**» et l'«**avis 1/2017**»), en vue de veiller à ce que les garanties en matière de protection des données soient dûment prises en considération dans les propositions de quatrième et cinquième directives anti-blanchiment.

8. En particulier, dans son avis de 2013 sur le projet de quatrième directive anti-blanchiment, le CEPD a insisté sur la nécessité de respecter les **garanties en matière de protection des données**, surtout dans le contexte des procédures relatives à l'**obligation de vigilance à l'égard de la clientèle**. Il a rappelé que la seule finalité du traitement de données au titre des directives anti-blanchiment doit être la prévention du blanchiment de capitaux et du financement du terrorisme, et que **les données ne doivent pas faire l'objet d'un traitement ultérieur à d'autres fins incompatibles** par des entités assujetties (par exemple, à des fins commerciales ou de marketing) et par des pouvoirs publics.
9. De plus, il a insisté sur la nécessité de respecter les **principes de nécessité et de proportionnalité** quand les droits des personnes viennent à être restreints et lorsque des sanctions administratives sont publiées, et a recommandé d'évaluer d'autres options moins intrusives que l'obligation générale de **publication**. Enfin, il a insisté sur la nécessité de prévoir des **règles déterminant spécifiquement les données d'identification des bénéficiaires effectifs** qui devraient être traitées par les registres centraux des bénéficiaires effectifs. À cet égard, l'article 30, paragraphe 5, de la quatrième directive anti-blanchiment dispose à présent que ces registres traitent au moins les données à caractère personnel suivantes: le nom, le mois et l'année de naissance, la nationalité et le pays de résidence du bénéficiaire effectif, ainsi que la nature et l'étendue des intérêts effectifs détenus.
10. Dans son avis 1/2017, le CEPD a exprimé plusieurs inquiétudes concernant le respect des **principes de limitation des finalités et de proportionnalité** par les modifications introduites par la cinquième directive anti-blanchiment. Il a en particulier signalé des lacunes dans la proposition de législation en lien avec les garanties insuffisantes pour éviter que des données à caractère personnel collectées aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme ne soient utilisées à d'autres fins, comme la lutte contre l'**évasion fiscale** ou l'accroissement de la transparence des entreprises. En outre, il a recommandé de veiller à ce qu'une évaluation adéquate de la **proportionnalité des mesures proposées soit effectuée en fonction de leur finalité**, en particulier au regard de l'application de l'approche fondée sur les risques, de l'accès élargi aux informations sur les transactions financières par les CRF, ainsi que de l'élargissement de l'accès des autorités compétentes et du grand public aux informations sur les bénéficiaires effectifs. Au sujet de ce dernier aspect, le CEPD a recommandé de prévoir un accès limité uniquement pour les services répressifs.

### 3. COMMENTAIRES ET RECOMMANDATIONS

#### 3.1. Premier pilier: veiller à la mise en œuvre effective du cadre de l'UE existant en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

11. Le CEPD est d'accord avec le plan d'action sur le fait que, parmi les initiatives de la Commission visant à lutter contre le blanchiment de capitaux et le financement du terrorisme, la première priorité devrait être de veiller à ce que les règles LBC-FT de l'Union soient effectivement et rigoureusement **mises en œuvre** par les États membres. Cela inclut également le plein respect du cadre de protection des données lors de la mise en œuvre de ces mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme.
12. Parmi les mesures envisagées, **la mise en place de mécanismes centralisés pour les comptes bancaires et de registres des bénéficiaires effectifs** est particulièrement pertinente du point de vue de la protection des données, puisqu'elle vise l'interconnexion de bases de données contenant de nombreuses données à caractère personnel (par exemple, le nom, la date de naissance, la nationalité, le pays de résidence, le numéro de compte bancaire, etc.). Par conséquent, le CEPD se réjouit de l'engagement pris par la Commission de suivre de près la

mise en place de ces registres centraux afin de s'assurer qu'ils sont alimentés avec des données de haute qualité<sup>13</sup> et qu'ils sont le plus à jour possible, car cela est conforme au principe d'exactitude ancré à l'article 5, paragraphe 1, point d), du RGPD.

13. Conformément à la cinquième directive anti-blanchiment, les mécanismes centralisés pour les comptes bancaires doivent être institués au plus tard le 10 septembre 2020<sup>14</sup>. Il s'agit de **mécanismes automatisés centralisés**, tels que des registres centraux ou des systèmes électroniques centraux de recherche de données, permettant l'identification de toute personne physique ou morale qui détient ou contrôle des comptes de paiement et des comptes bancaires, ainsi que des coffres-forts tenus par un établissement de crédit<sup>15</sup>.
14. Le rapport de la Commission au Parlement européen et au Conseil sur l'interconnexion des mécanismes automatisés centralisés nationaux des États membres concernant les comptes bancaires<sup>16</sup> concluait que l'**interconnexion de ces mécanismes** est possible. Le CEPD se félicite que, dans ce rapport, qui évalue différentes solutions informatiques à l'échelle de l'Union qui pourraient servir de modèles pour l'interconnexion des mécanismes centralisés, la Commission tienne compte des principes en matière de protection des données et insiste sur la nécessité de restreindre la portée des informations consultables via la plateforme d'interconnexion au minimum requis (**minimisation des données**) et de maintenir la proportionnalité entre la portée de l'accès aux données à caractère personnel et ce qui est nécessaire pour se conformer aux objectifs de la directive anti-blanchiment (**principe de proportionnalité**)<sup>17</sup>.
15. En outre, le plan d'action mentionne que des travaux sont en cours sur l'interconnexion de **registres centraux de bénéficiaires effectifs** pour les sociétés et autres entités juridiques, qui seront interconnectés par l'intermédiaire de la plate-forme centrale européenne<sup>18</sup> le 10 mars 2021 au plus tard<sup>19</sup>. Le CEPD rappelle que ces registres, auxquels les entités assujetties ont accès dans le cadre de procédures relatives à l'obligation de vigilance à l'égard de la clientèle, traitent au moins les données à caractère personnel des bénéficiaires effectifs suivantes: le nom, le mois et l'année de naissance, la nationalité et le pays de résidence du bénéficiaire effectif, ainsi que la nature et l'étendue des intérêts effectifs détenus<sup>20</sup>. Dès lors, il est particulièrement important que ces registres soient tenus à jour et que toutes les mesures raisonnables soient prises pour que toute donnée à caractère personnel inexacte soit effacée ou rectifiée sans tarder, conformément à l'article 5, paragraphe 1, point d), du RGPD. Cela a également été souligné par le Parlement dans sa dernière résolution sur le plan d'action [2020/2686(RSP)], qui demande à la Commission de réagir face à l'insuffisance et l'inexactitude des données contenues dans les registres nationaux des bénéficiaires effectifs, et exige que des mécanismes de vérification de l'exactitude des données soient mis en place afin de veiller au bon fonctionnement de ces registres et à ce qu'ils donnent au public accès à des données de qualité<sup>21</sup>.
16. Alors que les travaux sur l'interconnexion des mécanismes automatisés centralisés nationaux comme des registres centraux des bénéficiaires effectifs sont toujours en cours, le CEPD se réjouit que le plan d'action souligne l'importance de **suivre les principes en matière de protection des données au regard de l'interconnexion de ces mécanismes**. En effet, comme cette interconnexion permettra aux pouvoirs publics de différente nature, aussi bien les services répressifs que les CRF, d'avoir accès aux registres centralisés, il est important que les travaux relatifs à l'interconnexion s'efforcent d'intégrer aux mécanismes les principes de protection des données dès la conception et de protection des données par défaut conformément à l'article 25 du RGPD, et que des garanties fortes en matière de protection des données soient mises en place, surtout concernant les droits d'accès et l'exactitude des données. À cet égard, le CEPD attire l'attention sur l'avis 5/2018 sur la protection de la vie

privée dès la conception<sup>22</sup>, qui donne des exemples de **méthodes permettant de recenser les exigences en matière de respect de la vie privée et de protection des données et de les intégrer dans des processus d'ingénierie de la vie privée** en vue d'appliquer les garanties technologiques et organisationnelles appropriées. En outre, le CEPD suggère, dans le cadre des travaux d'interconnexion, de tenir compte des recommandations fournies dans son avis sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 89/666/CEE, 2005/56/CE et 2009/101/CE en ce qui concerne l'interconnexion des registres centraux, du commerce et des sociétés<sup>23</sup>. Il attire en particulier l'attention sur ses recommandations antérieures relatives à la **gouvernance du réseau ainsi qu'aux rôles, aux compétences et aux responsabilités** des parties prenantes concernées, ainsi que sur celles concernant les garanties en matière de protection des données pour les **transferts de données à caractère personnel vers des pays tiers**. Enfin, des orientations précises pour l'établissement d'une gouvernance et d'une gestion informatiques solides de ces bases de données interconnectées sont présentées dans les lignes directrices du CEPD sur la protection des données à caractère personnel pour la gouvernance informatique et la gestion informatique des institutions européennes<sup>24</sup>.

### 3.2. Deuxième pilier: mettre en place un corpus réglementaire renforcé

17. Le CEPD convient que la lutte contre le blanchiment de capitaux profiterait considérablement de l'harmonisation des règles LBC-FT, au moyen de l'adoption d'un règlement garantissant l'application directe des principales règles, ainsi que leur interprétation uniforme par la Cour de justice de l'Union européenne. C'est pourquoi la CEPD saluerait une harmonisation accrue de ces règles au niveau de l'Union européenne, qui non seulement aurait une incidence bénéfique sur la lutte contre le blanchiment de capitaux et le terrorisme, mais qui renforcerait et rationaliserait aussi les garanties en matière de protection des données à l'échelle européenne en la matière.
18. À cette fin, le plan d'action propose plusieurs sujets importants qui pourraient être couverts par un futur règlement, tels que la liste des entités assujetties, les obligations de vigilance à l'égard de la clientèle, les contrôles internes, les obligations déclaratives ainsi que les dispositions relatives aux registres des bénéficiaires effectifs et aux mécanismes centralisés pour les comptes bancaires. Comme susmentionné, il s'agit là de domaines qui ont une incidence significative sur les droits à la protection des données et au respect de la vie privée puisqu'ils supposent le traitement d'une quantité substantielle de données à caractère personnel.
19. Le CEPD se réjouit que la Commission ait l'intention de suivre une **approche fondée sur les risques à l'égard des nouvelles mesures du corpus réglementaire renforcé**, consistant à appliquer des procédures moins intrusives aux situations moins risquées. Cette approche est conforme aux principes en matière de protection des données et, en particulier, à l'impératif d'évaluer la nécessité et la proportionnalité des mesures législatives, à la lumière de l'incidence de ces mesures sur les droits au respect de la vie privée et à la protection des données à caractère personnel. Pour des orientations sur ce sujet, le CEPD recommande de consulter ses **lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel**<sup>25</sup>.
20. Le CEPD a déjà souligné, par le passé, qu'il importe d'instaurer des garanties claires pour assurer le respect du **droit à l'information dans le cadre des procédures relatives à l'obligation de vigilance à l'égard de la clientèle**<sup>26</sup>. Il avait en particulier recommandé des

garanties, qui ont été insérées dans la quatrième directive anti-blanchiment, pour veiller à ce que, lorsque des données sont collectées, le client soit informé de la ou des fins auxquelles ces données sont requises et traitées. Ces garanties sont importantes dès lors que, par exemple, les données nécessaires pour établir la relation d'affaires seront collectées et utilisées parallèlement à des fins commerciales (par exemple, vérification de l'identité du client) et aux fins de l'obligation de vigilance à l'égard de la clientèle (à savoir, lutte contre le blanchiment de capitaux). À cet égard, l'article 41, paragraphe 3, de la quatrième directive anti-blanchiment exige que *«[L]es entités assujetties communiquent aux nouveaux clients les informations requises en vertu de l'article 10 de la directive 95/46/CE avant de nouer une relation d'affaires ou d'exécuter une transaction à titre occasionnel. Ces informations contiennent en particulier un avertissement général concernant les obligations légales des entités assujetties au titre de la présente directive en ce qui concerne le traitement des données à caractère personnel aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme visés à l'article 1<sup>er</sup> de la présente directive»*. Ces recommandations sont toujours valables à l'heure actuelle en vertu du RGPD, et le CEPD encourage la Commission à en tenir compte, également dans le contexte de l'élaboration de futures dispositions.

21. Dans son avis de 2013 sur le projet de quatrième directive anti-blanchiment, le CEPD recommandait également que le législateur clarifie le type d'information qui devait être pris en considération dans le cadre de l'obligation de vigilance à l'égard de la clientèle normale mais aussi renforcée (pour les personnes politiquement exposées et les personnes liées) et aux fins de la réalisation d'évaluations des risques en vue de prévenir les décisions arbitraires et les discriminations, ainsi que pour garantir le respect du **principe de minimisation des données**. À cet égard, les procédures relatives à l'obligation de vigilance à l'égard de la clientèle supposent à l'heure actuelle le traitement de données relatives à l'identité du client, aux bénéficiaires effectifs des entités juridiques, à l'objet et à la nature envisagée de la relation d'affaires, ainsi qu'à l'examen des transactions, y compris, si nécessaire, de l'origine des fonds<sup>27</sup>. Pour les personnes politiquement exposées, les membres de leur famille ou les personnes connues pour être étroitement associées aux personnes politiquement exposées, l'obligation de vigilance renforcée à l'égard de la clientèle exige aussi que la relation d'affaires soit autorisée par un membre d'un niveau élevé de la hiérarchie, que les mesures appropriées pour établir l'origine du patrimoine et l'origine des fonds soient prises, et qu'un contrôle renforcé de la relation d'affaires sur une base continue soit assuré<sup>28</sup>. Par conséquent, lorsque les entités assujetties collectent et traitent les données des clients dans le cadre de procédures relatives à l'obligation de vigilance à l'égard de la clientèle, elles devraient s'assurer que toutes les **données à caractère personnel demandées sont adéquates, pertinentes et limitées au strict nécessaire** en lien avec les finalités de l'obligation de vigilance à l'égard de la clientèle.
22. Les procédures relatives à l'obligation de vigilance à l'égard de la clientèle devraient également inclure des garanties en matière de protection des données conformément au RGPD afin de garantir, par exemple, que les personnes physiques relevant de la connaissance clientèle **ne font pas l'objet de décisions fondées sur des données à caractère personnel qui n'auraient pas dû être collectées et/ou qui ne sont pas nécessaires** à l'établissement de la relation d'affaires, ou encore qui ont été **réutilisées à d'autres fins incompatibles**. De plus, les dispositions relatives à l'obligation de vigilance à l'égard de la clientèle devraient également tenir compte des limites de la prise de décision individuelle automatisée, y compris le profilage, fixées à l'article 22 du RGPD, et être alignées sur ces limites, en particulier lorsque ces procédures relatives à l'obligation de vigilance à l'égard de la clientèle pourraient entraîner l'émission d'un rapport relatif à des activités suspectes sur l'activité du client.

23. Le CEPD constate qu'avec le développement de la transition numérique dans tous les domaines de la vie, les procédures relatives à l'obligation de vigilance à l'égard de la clientèle visant à identifier le client et la vérification de l'identité pourraient se dérouler en ligne (à distance) à l'avenir. Dans ce cas, le CEPD souligne que le **passage au numérique de l'obligation de vigilance à l'égard de la clientèle** doit s'accompagner de l'adoption des mesures nécessaires pour garantir la **sécurité des données à caractère personnel**, et en particulier de mesures de lutte contre le traitement non autorisé ou illicite de données à caractère personnel et contre la perte, la destruction ou les dommages accidentels (intégrité et confidentialité). De plus, le passage au numérique des procédures relatives à l'obligation de vigilance à l'égard de la clientèle devrait être sous-tendu par le **principe de protection des données dès la conception**, de manière à ce que celui-ci facilite d'emblée l'exercice des droits relatifs aux données à caractère personnel. Enfin, le CEPD rappelle que, depuis l'entrée en vigueur du RGPD, toutes les entités doivent veiller à être en mesure de démontrer qu'elles respectent les obligations en matière de protection des données (**principe de responsabilité**). Dès lors, les entités assujetties, en leur qualité des responsables du traitement, doivent, dans le cadre des procédures relatives à l'obligation de vigilance à l'égard de la clientèle, tenir un registre des activités de traitement relevant de leur responsabilité et tenir ces informations à disposition de l'autorité de contrôle de la protection des données à la demande de cette dernière.
24. Enfin, le plan d'action prône un élargissement de la portée de la législation européenne relative à la lutte contre le blanchiment de capitaux afin d'aborder les implications de l'innovation technologique et de l'évolution des normes internationales. Le CEPD se félicite de la référence expresse à la nécessité de **nouvelles solutions technologiques qui peuvent faciliter la détection des transactions et activités suspectes respectant les règles en matière de protection des données**, et recommande que ces solutions suivent les principes de protection des données dès la conception et de protection des données par défaut, conformément à son avis 5/2018 sur la protection de la vie privée dès la conception.

### 3.3. Troisième pilier: instaurer une surveillance de niveau européen

25. La Commission envisage, dans le plan d'action, la création d'un **système de surveillance LBC-FT intégré au niveau de l'Union européenne**, qui garantisse une application cohérente et de grande qualité du corpus réglementaire unique relatif à la lutte contre le blanchiment de capitaux et le financement du terrorisme dans l'ensemble de l'Union et favorise une coopération efficace entre toutes les autorités compétentes.
26. Comme proposé dans le plan d'action, les pouvoirs de l'autorité de surveillance LBC-FT de l'Union européenne, qui assume une responsabilité exclusive ou conjointe avec les autorités de surveillance nationales, peuvent impliquer de pouvoir examiner les documents relatifs aux opérations et aux clients, afin de garantir la bonne application des politiques internes par les entités soumises à surveillance<sup>29</sup>. Le CEPD insiste sur le fait qu'il importe que la future proposition législative instituant l'autorité de surveillance LBC-FT de l'Union européenne comprenne une **base juridique claire concernant le traitement des données à caractère personnel** et indiquant les finalités et les limites de ce traitement, conformément à l'article 5, paragraphe 1, du règlement (UE) 2018/1725.
27. Il est également probable que cette surveillance suppose une coopération à deux niveaux: d'une part, une coopération **entre États membres** impliquant le partage d'information au-delà des frontières; d'autre part, une coopération entre **différentes autorités** d'un même État membre ou de plusieurs États membres, y compris entre les autorités de surveillance

financière et prudentielle dans un premier temps, puis entre les autorités chargées de l'enquête et les services répressifs dans un second temps. **Le CEPD recommande que l'instrument juridique** instaurant l'autorité de surveillance LBC-FT de l'Union européenne **prévoit déjà des règles spécifiques sur le partage et la diffusion d'informations qui tiennent compte des garanties nécessaires en matière de protection des données.**

28. Lorsque les fonctions et pouvoirs de la future autorité de surveillance LBC-FT de l'Union européenne prévoient une possible coopération de celle-ci avec des pays tiers ou des organisations internationales, l'acte fondateur devrait aussi introduire des **dispositions plus précises sur les conditions relatives aux transferts internationaux de données opérationnelles à caractère personnel**, en particulier sur les transferts faisant l'objet de garanties appropriées et de dérogations pour des situations particulières<sup>30</sup>. Le CEPD rappelle que ces dispositions doivent respecter les conditions des articles 46 à 51 et de l'article 94 du règlement (UE) 2018/1725, et être soumises à des garanties appropriées en matière de protection des données.

### 3.4. Quatrième pilier: créer un mécanisme de coordination et de soutien pour les CRF

29. Un **mécanisme de coordination solide et efficace entre les CRF**, qui sont considérées comme étant les «pôles du renseignement financier»<sup>31</sup>, est un élément crucial de la lutte contre le blanchiment de capitaux, étant donné que les activités illicites couvrent habituellement des transactions transfrontières et/ou entre différentes institutions. Cependant, peu d'analyses conjointes de ces activités et des facteurs pertinents sont réalisées par les CRF des États membres et les autres pouvoirs publics. En conséquence, dans la pratique, il est possible qu'il existe des lacunes législatives et opérationnelles, dont des acteurs malveillants peuvent tirer parti pour commettre des actes illicites relatifs au blanchiment de capitaux et au financement du terrorisme.
30. La coordination transfrontière exige de recourir à des **outils et procédures adaptés et efficaces** qui facilitent le partage d'informations et la mise en correspondance des données, mais qui sont parallèlement pleinement conformes aux exigences en matière de protection des données. À cet égard, comme signalé précédemment, la protection des données doit être considérée comme faisant partie intégrante du processus analytique complexe de prévention et de détection du blanchiment de capitaux et d'autres activités illicites, et non comme y faisant obstacle.

#### **FIU.net**

31. Depuis près de 20 ans, la coopération entre les CRF et l'Union européenne est facilitée par un réseau d'échange d'informations (appelé «**FIU.net**»<sup>32</sup>). Dans sa communication intitulée «*Vers une meilleure mise en œuvre du cadre réglementaire de l'UE en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme*», la Commission reconnaît qu'il existe, aujourd'hui encore, des problèmes techniques récurrents qui entravent le fonctionnement de l'outil FIU.net, qui compliquent le partage d'informations pour les CRF, et qui ont donc entraîné une réduction de l'échange d'informations et de la mise en correspondance des données entre elles<sup>33</sup>. En outre, le rapport relève le manque de réglementation des échanges d'informations entre les CRF des États membres et les CRF de pays tiers, qui a conduit à une approche non harmonisée de ces échanges. Ces obstacles juridiques et pratiques ont inévitablement une incidence sur l'exactitude et l'information actualisée de FIU.net, et constituent donc un risque pour la protection des droits au respect de la vie privée et à la protection des données à caractère personnel.

32. Pour atténuer ces problèmes, le plan d'action fait écho au besoin urgent d'investir dans le développement de FIU.net et de trouver une solution adaptée pour sa gestion.
33. Concernant l'avenir de FIU.net<sup>34</sup>, la Commission a mentionné la future autorité de surveillance LBC-FT de l'Union européenne comme potentielle **entité d'hébergement du réseau**, ainsi que d'autres solutions possibles, par exemple le **renforcement du mandat** d'Europol en vue de lui conférer une base juridique pour héberger le réseau<sup>35</sup>. Si une solution n'est pas en place d'ici fin 2020, la Commission a fait part de son intention de reprendre provisoirement la gestion de FIU.net, afin d'assurer le fonctionnement continu et ininterrompu du système.
34. Bien que le rôle de la Commission en tant qu'hébergeur de FIU.net reste encore à déterminer du point de vue de la protection des données (c'est-à-dire le responsable du traitement, le responsable conjoint du traitement et le sous-traitant), le CEPD rappelle qu'une base juridique valable est nécessaire pour traiter les données à caractère personnel partagées par l'intermédiaire du réseau. À cet égard, le CEPD relève que l'article 51 de la quatrième directive anti-blanchiment dispose que *«[I]a Commission peut apporter tout le soutien nécessaire pour faciliter la coordination, y compris l'échange d'informations entre les CRF au sein de l'Union»*. Sans préjudice d'une analyse plus approfondie et bien qu'elle ne fasse pas expressément référence au traitement de données à caractère personnel, cette disposition semblerait apporter une certaine base pour la gestion de **FIU.net**, étant donné que le traitement de données à caractère personnel serait normalement jugé nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investie la Commission [voir article 6 du RGPD et article 5 du règlement (UE) 2018/1725].

### **Le mécanisme de coordination et de soutien pour les CRF**

35. En ce qui concerne le mécanisme de coordination et de soutien pour les CRF plus généralement, **le CEPD fait remarquer que les CRF des différents États membres suivent des modèles institutionnels différents et ont donc des pouvoirs hétérogènes**. Il y a, d'une part, les CRF **administratives**, qui procèdent à l'analyse des rapports relatifs à des activités suspectes et transmettent ces derniers aux services répressifs pour enquête lorsque des indices montrent que la transaction signalée pourrait être constitutive d'une infraction. D'autre part, il y a les CRF **répressives**, qui disposent de compétences d'enquête à l'égard de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Il y a également des CRF qui sont des hybrides de ces deux modèles, et jouissent de pouvoirs différents. Ainsi que la Commission l'a indiqué dans son rapport portant évaluation du cadre pour la coopération entre les CRF<sup>36</sup>, les différences de statut, de pouvoirs et d'organisation des CRF continuent de **nuire à leur capacité à accéder aux informations pertinentes et à les partager**. Du point de vue de la protection des données, de telles distorsions résultant de la nature différente des CRF entraînent un grave risque de non-respect du principe de limitation des finalités dans la gestion et le partage des informations.
36. Par ailleurs, le CEPD rappelle que le considérant 56 de la quatrième directive anti-blanchiment indique qu'il convient d'autoriser **à des fins d'analyse** l'échange entre les CRF d'informations relatives au blanchiment de capitaux ou au financement du terrorisme, **informations qui ne font pas l'objet d'un traitement ni d'une dissémination ultérieure**, sauf si cet échange d'informations est contraire aux principes fondamentaux du droit national. Par conséquent, le CEPD recommande que la proposition législative instituant un mécanisme de coordination et de soutien pour les CRF envisagée par la Commission prévoit déjà des dispositions fixant des **conditions explicites et claires d'accès aux informations sur les**

**transactions financières et de partage de ces dernières par les CRF des États membres.** En outre, comme déjà indiqué dans l’avis 1/2017, le CEPD considère comme plus conforme aux principes de proportionnalité et de limitation des finalités une configuration juridique des pouvoirs des CRF «fondée sur l’enquête» qu’une configuration «fondée sur le renseignement», dans le cadre de laquelle les CRF peuvent demander des informations aux entités assujetties à des fins d’analyse et de renseignement qui lui sont propres, sans déclaration de transaction suspecte établie au préalable<sup>37</sup>. Comme souligné dans ledit avis, cette deuxième optique se rapprocherait davantage de l’exploration de données que d’une enquête ciblée, ce qui a des conséquences sur les droits relatifs aux données à caractère personnel.

### **3.5. Cinquième pilier: faire appliquer les dispositions de droit pénal et les dispositions en matière d’échange d’informations arrêtées au niveau de l’Union européenne**

37. En ce qui concerne l’appel au renforcement de la coordination concernant les questions de renseignement financier entre les services répressifs et les CRF des États membres lancé dans le plan d’action, compte tenu de leur nature et de leurs pouvoirs différents (rôles administratif et pénal/répressif), le CEPD tient à insister sur le fait que **cette coordination et cet échange de données doivent toujours être conformes au cadre de protection des données**. De plus, les moyens technologiques utilisés pour le partage d’informations entre ces autorités devraient inclure des mesures techniques et organisationnelles appropriées, pour protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l’altération ou la divulgation illicite, y compris le chiffrement et l’anonymisation.
38. Dans le plan d’action, la Commission encourage le recours aux partenariats public-privé (PPP) en matière de renseignement financier, essentiellement sous deux formes: 1) les échanges d’informations – des CRF et des services répressifs aux entités assujetties – sur **les typologies et les tendances**; et 2) le partage d’**informations opérationnelles** – des services répressifs aux entités assujetties – **sur les suspects détectés par le renseignement**, aux fins du suivi des transactions effectuées par ces suspects. Cette initiative est conforme à la position adoptée par le Groupe d’action financière (**GAFI**) ces dernières années, défendant un rôle plus actif des PPP dans le renseignement financier afin de préserver l’intégrité du système financier international<sup>38</sup>.
39. En ce qui concerne **le premier type de PPP, le CEPD salue et soutient l’idée d’efforts conjoints des services répressifs, des CRF et du secteur privé** pour structurer les débats sur les politiques et les forums de discussion et à des fins de recherche et d’analyse des typologies et des tendances relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Le CEPD rappelle que les PPP ont été utilisés avec succès dans des domaines similaires, tels que la cybersécurité, le calcul à haute performance, la robotique ou les futures technologies internet<sup>39</sup>, dans lesquels les exigences en matière de protection des données ont structuré les échanges d’information et ont été intégrées aux processus de recherche, sans soulever d’inquiétude particulière quant à leur mise en œuvre.
40. Le CEPD se félicite de la résolution du Parlement sur le plan d’action<sup>40</sup>, dans laquelle il soutient expressément les PPP sous la forme de plateformes tripartites, et il souligne l’obligation pour ce type de PPP de respecter strictement les limites que constituent les règles de protection des données et les droits fondamentaux applicables. En outre, le CEPD se joint à l’appel lancé par le Parlement à la Commission, lui demandant de **proposer un cadre juridique clair pour ces plateformes**, assurant également le respect des règles relatives à l’échange d’informations et à la protection des données.

41. Pour ce qui est de la constitution de PPP pour le partage **d'informations opérationnelles – des services répressifs aux entités assujetties – sur les suspects détectés par le renseignement**, alors que le CEPD n'émet aucun jugement sur le fond des objectifs stratégiques qui les sous-tendent, **il craint que ce choix stratégique n'entraîne un risque élevé pour le droit des personnes physiques au respect de la vie privée** et à la protection des données.
42. Le CEPD rappelle que, dans son avis 1/2017, il a souligné que, d'après le cadre relatif à la lutte contre le blanchiment de capitaux, la détection et la répression des activités criminelles sont réservées aux autorités compétentes. Une personne privée ne se voit en aucun cas, formellement ou informellement, directement ou indirectement, confier un rôle répressif<sup>41</sup>. Dès lors, la création de PPP visant à permettre à des entités privées (à savoir, les entités assujetties) de surveiller des personnes concernées (qui sont également leurs clients) sur la base d'informations opérationnelles à jour faisant toujours l'objet d'une enquête des services répressifs créerait, selon le CEPD, un précédent très risqué du point de vue de la protection des données.
43. Conformément au cadre relatif à la lutte contre le blanchiment de capitaux, le rôle des entités assujetties se limite à la déclaration d'activités suspectes aux CRF au moyen de ce que l'on appelle les «rapports relatifs à des activités suspectes». Ce rôle est unidirectionnel, et les entités assujetties ne reçoivent aucun retour d'information des CRF ou des services répressifs sur l'analyse des informations déclarées et la suite qui leur est donnée. Il s'agit là, du point de vue de la protection des données, d'une garantie pour le respect de la vie privée des personnes physiques, étant donné que les entités assujetties ne participent à aucune opération de traitement concernant des informations sur de possibles infractions découlant des transactions suspectes signalées, qui, du fait de leur nature sensible, devraient se limiter aux seuls pouvoirs publics, compte tenu de leur incidence sur les droits fondamentaux des personnes concernées.
44. Sans préjudice des éléments de preuve qui pourraient être présentés à l'avenir, le CEPD considère qu'il n'existe à l'heure actuelle aucune raison impérieuse justifiant de donner à des personnes privées accès aux données à caractère personnel sensibles de personnes physiques concernant des activités et infractions pénales qui font l'objet d'une enquête, étant donné que celles-ci sont et devraient rester exclusivement aux mains des pouvoirs publics compétents. Par ailleurs, le CEPD rappelle que, pour qu'une mesure respecte le principe de proportionnalité inscrit à l'article 52, paragraphe 1, de la charte, les avantages résultant de cette mesure ne doivent pas être contrebalancés par les inconvénients causés par la mesure au regard de l'exercice des droits fondamentaux. À cet égard, le CEPD considère qu'une mesure qui confère à des entités privées le pouvoir de surveiller des suspects ne pourrait que très difficilement remplir les critères de proportionnalité et de nécessité, et qu'il faudrait d'abord étudier d'autres possibilités moins intrusives d'atteindre le même objectif<sup>42</sup>.
45. Deuxièmement, le partage de données sensibles de «suspects» avec le secteur privé, qui pourrait également avoir ces personnes comme clients, soulève des inquiétudes du point de vue des conflits d'intérêts. En particulier, le CEPD craint que les PPP créés pour le partage **d'informations opérationnelles sur les suspects détectés par le renseignement** ne jouissent pas de l'indépendance et de l'autonomie nécessaires, étant donné que les entités assujetties seraient tenues de surveiller leurs propres clients, à l'égard desquels elles ont un devoir de confidentialité dans le cadre de leur relation d'affaires.
46. Troisièmement, le CEPD craint que la constitution de ce type de PPP ne crée des problèmes en lien avec le **principe de limitation des finalités**, selon lequel les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne

pas être traitées ultérieurement d'une manière incompatible avec ces finalités. En particulier, les entités assujetties participant à des PPP pourraient être tentées d'intégrer les informations partagées par les services répressifs par l'intermédiaire de cette plateforme **dans leurs bases de données globales, de manière à les réutiliser ultérieurement**, dans le cadre de leurs profils client<sup>43</sup>. Cela pourrait entraîner une discrimination à l'encontre de certains clients, par exemple ceux qui sont peu rentables pour la banque et qui présentent un niveau considérable de risque, laquelle pourrait provoquer l'exclusion financière de personnes et communautés vulnérables (ce que l'on appelle le «de-risking» – autrement dit, la diminution des risques – des entités financières, qui consiste à cesser ou limiter les relations avec les clients qui sont susceptibles de représenter un risque)<sup>44</sup>.

47. En effet, la difficile compatibilité et les inquiétudes découlant de la participation de PPP à des missions de renseignement financier sont attestées par les quelques pays au monde qui ont choisi ce modèle<sup>45</sup>, avec un précédent au sein de l'Union européenne, uniquement au sein d'un ancien État membre<sup>46</sup>. En outre, les quelques exemples existants semblent être des partenariats de partage d'informations au niveau national, sans échange transfrontière concernant le renseignement financier et avec un nombre réduit de participants.

### 3.6. Sixième pilier: renforcer le rôle de l'Union européenne sur la scène mondiale

48. Le CEPD salue l'ambition de la Commission de jouer un rôle plus important dans les travaux du GAFI et dans la fixation des normes internationales relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Dans ce contexte, il encourage la Commission à s'efforcer d'intégrer les principes en matière de protection des données de l'Union au sein des processus de mise en conformité LBC-FT, en tant que garantie pour les droits fondamentaux des personnes physiques. À la suite de l'adoption du RGPD, l'Union européenne a démontré sa capacité à influencer les systèmes juridiques de pays tiers et à renforcer leurs normes de protection des données. Le CEPD estime qu'elle devrait continuer sur cette voie, par exemple lorsqu'elle discute des normes internationales LBC-FT ayant trait aux procédures relatives à l'obligation de vigilance à l'égard de la clientèle, à la tenue de registres ou aux rapports relatifs à des activités suspectes, dans le cadre desquels les droits à l'information des personnes physiques dont les données seront traitées et les principes de minimisation des données et d'exactitude revêtent une importance majeure.
49. En outre, le CEPD se félicite de la nouvelle méthode d'évaluation des pays à haut risque [SWD(2020) 99]<sup>47</sup>, qui a été publiée parallèlement au plan d'action. Cette méthode repose sur les critères énumérés à l'article 9 de la quatrième directive anti-blanchiment, et l'évaluation des pays à haut risque devrait être conforme aux éléments mis en lumière dans le présent avis.

## 4. CONCLUSIONS

À la lumière des considérations qui précèdent, le CEPD émet les recommandations suivantes:

- il invite la Commission à ménager, dans ses travaux législatifs, un équilibre entre, d'une part, les mesures qui sont nécessaires pour effectivement atteindre les objectifs d'intérêt général en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et, de l'autre, l'atteinte portée par ceux-ci aux droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel;
- il recommande à la Commission de suivre la mise en œuvre du cadre LBC-FT existant, tout en garantissant le respect du RGPD et du cadre de protection des données;

- il recommande que les travaux relatifs à l'interconnexion des mécanismes centralisés pour les comptes bancaires et des registres des bénéficiaires effectifs respectent, en particulier, les principes de minimisation des données, d'exactitude et de protection des données dès la conception et par défaut;
- il suggère à la Commission de maintenir une approche fondée sur les risques à l'égard des nouvelles mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme du corpus réglementaire renforcé, en appliquant des procédures moins intrusives aux situations moins risquées, car cela est également conforme aux principes en matière de protection des données;
- il recommande, en ce qui concerne l'obligation de vigilance à l'égard de la clientèle, que des garanties soient maintenues dans la proposition de législation afin de garantir le droit des clients d'être informés lorsque leurs données sont collectées, ainsi que d'être informés de la ou des finalité(s) pour lesquelles les données sont requises et seront traitées, et d'assurer le respect des principes de minimisation des données, de limitation des finalités et de protection des données dès la conception, ainsi que des limites de la prise de décision individuelle automatisée;
- il recommande à la Commission de prévoir, dans sa proposition à venir établissant une autorité de surveillance LBC-FT de l'Union européenne, une base juridique pour le traitement des données à caractère personnel ainsi que les garanties nécessaires en matière de protection des données conformément au RGPD et au règlement (UE) 2018/1725, en particulier concernant le partage d'informations et les transferts internationaux de données;
- il recommande à la Commission de clarifier, dans la proposition de mécanisme de coordination et de soutien pour les CRF, les conditions d'accès aux informations sur les transactions financières et de partage de ces informations par les CRF;
- il soutient la création de PPP pour la recherche et l'analyse des typologies et des tendances relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, dans le respect des limites du RGPD;
- il encourage la Commission à intégrer les principes de la protection des données lorsqu'elle fixe des normes internationales au sein du Groupe d'action financière.

Bruxelles, le 23 juillet 2020

Wojciech WIEWIÓROWSKI  
(signature électronique)

---

## NOTES

<sup>1</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016).

<sup>2</sup> Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018).

<sup>3</sup> <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering/public-consultation>

<sup>4</sup> Affaire Digital Rights Ireland (2014).

<sup>5</sup> [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf)

<sup>6</sup> [https://edps.europa.eu/sites/edp/files/publication/19-12-19\\_edps\\_proportionality\\_guidelines2\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_fr.pdf)

<sup>7</sup> Directive (UE) 2018/1673 du Parlement européen et du Conseil du 23 octobre 2018

visant à lutter contre le blanchiment de capitaux au moyen du droit pénal.

<sup>8</sup> Les États membres sont tenus de transposer la sixième directive anti-blanchiment en droit national au plus tard le 3 décembre 2020; ensuite, les entreprises au sein des États membres devront mettre en œuvre la réglementation pertinente au plus tard le 3 juin 2021.

<sup>9</sup> Les considérants 22 et 23 de la quatrième directive anti-blanchiment disposent: «*Le risque de blanchiment de capitaux et de financement du terrorisme n'est pas toujours le même dans chaque cas. Il conviendrait, en conséquence, d'appliquer une approche fondée sur les risques qui soit globale. L'approche fondée sur les risques ne constitue pas une option indûment permissive pour les États membres et les entités assujetties. Elle suppose le recours à la prise de décisions fondées sur des preuves, de façon à cibler de façon plus effective les risques de blanchiment de capitaux et de financement du terrorisme menaçant l'Union et les acteurs qui opèrent en son sein. À la base de l'approche fondée sur les risques se trouve la nécessité pour les États membres et l'Union d'identifier, de comprendre et d'atténuer les risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont exposés. [...]*»

<sup>10</sup> Voir considérant 19 de la sixième directive anti-blanchiment.

<sup>11</sup> [https://edps.europa.eu/sites/edp/files/publication/13-07-04\\_money\\_laundering\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/13-07-04_money_laundering_fr.pdf)

<sup>12</sup> [https://edps.europa.eu/sites/edp/files/publication/17-02-02\\_opinion\\_aml\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/17-02-02_opinion_aml_fr.pdf)

<sup>13</sup> Voir plan d'action, page 4.

<sup>14</sup> Voir considérant 53 de la cinquième directive anti-blanchiment.

<sup>15</sup> Voir article 1<sup>er</sup>, point 19, de la cinquième directive anti-blanchiment, qui insère les articles 32 *bis* et 32 *ter* dans la quatrième directive anti-blanchiment.

<sup>16</sup> Disponible à l'adresse suivante:

[https://ec.europa.eu/info/sites/info/files/report\\_assessing\\_the\\_conditions\\_and\\_the\\_technical\\_specifications\\_and\\_procedures\\_for\\_ensuring\\_secure\\_and\\_efficient\\_interconnection\\_of\\_central\\_bank\\_account\\_registers\\_and\\_data\\_retrieval\\_systems.pdf](https://ec.europa.eu/info/sites/info/files/report_assessing_the_conditions_and_the_technical_specifications_and_procedures_for_ensuring_secure_and_efficient_interconnection_of_central_bank_account_registers_and_data_retrieval_systems.pdf).

<sup>17</sup> Voir page 6 du rapport.

<sup>18</sup> Article 30, paragraphe 10, de la quatrième directive anti-blanchiment, tel que modifié par la cinquième directive anti-blanchiment

<sup>19</sup> Considérant 53 de la cinquième directive anti-blanchiment

<sup>20</sup> Article 30, paragraphe 5, de la quatrième directive anti-blanchiment

<sup>21</sup> Résolution sur une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme – plan d'action de la Commission et autres évolutions récentes [2020/2686(RSP)], disponible à l'adresse suivante: [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204\\_FR.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204_FR.html)

- 
- <sup>22</sup> Voir [https://edps.europa.eu/sites/edp/files/publication/18-05-31\\_preliminary\\_opinion\\_on\\_privacy\\_by\\_design\\_en\\_0.pdf](https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf).
- <sup>23</sup> [https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C\\_.2011.220.01.0001.01.FRA&toc=OJ:C:2011:220:TOC](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2011.220.01.0001.01.FRA&toc=OJ:C:2011:220:TOC)
- <sup>24</sup> [https://edps.europa.eu/sites/edp/files/publication/it\\_governance\\_management\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/it_governance_management_fr.pdf)
- <sup>25</sup> Voir note de fin de document 6.
- <sup>26</sup> Voir avis du CEPD de 2013 sur le projet de quatrième directive anti-blanchiment, point 13.
- <sup>27</sup> Voir article 13 de la quatrième directive anti-blanchiment
- <sup>28</sup> Voir articles 20-23 de la quatrième directive anti-blanchiment
- <sup>29</sup> Voir page 8 du plan d'action.
- <sup>30</sup> Voir article 94 du règlement (UE) 2018/1725.
- <sup>31</sup> Voir rapport du Parlement européen intitulé «Anti-money laundering - reinforcing the supervisory and regulatory framework».
- <sup>32</sup> FIU.net est un réseau informatique décentralisé et sophistiqué qui aide les cellules de renseignement financier (CRF) de l'Union européenne dans leur lutte contre le blanchiment de capitaux et le financement du terrorisme. Il est devenu opérationnel en 2002 (en vertu de la décision 2000/642/JAI du Conseil du 17 octobre 2000), puis a été mentionné dans la directive 2005/60/CE (la troisième directive anti-blanchiment) et dans l'actuelle quatrième directive anti-blanchiment en tant qu'instrument d'échange d'informations entre les CRF. Depuis janvier 2016, FIU.net est intégré au sein d'Europol.
- <sup>33</sup> Voir communication de la Commission au Parlement européen et au Conseil intitulée «Vers une meilleure mise en œuvre du cadre réglementaire de l'UE en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme». [COM(2019) 360 final].
- <sup>34</sup> En décembre 2019, le CEPD a considéré que l'intégration de FIU.net dans les systèmes d'Europol (SIENA) était contraire aux dispositions régissant le traitement des données à caractère personnel en raison des restrictions imposées par le règlement Europol aux catégories de personnes au sujet desquelles Europol peut traiter des données à caractère personnel. En particulier, pour respecter les règles, les personnes physiques impliquées dans des transactions suspectes devraient être considérées comme étant des suspects, ce qui ne pourrait pas être systématiquement garanti par Europol, compte tenu de tous les types d'informations et de données à caractère personnel partagées par l'intermédiaire de FIU.net. Dans son avis, le CEPD a conclu que l'administration technique de FIU.net par Europol violait le règlement Europol. Toutefois, compte tenu de l'importance de FIU.net dans la lutte contre le blanchiment de capitaux et le financement du terrorisme au niveau de l'Union européenne, le CEPD a suspendu l'interdiction jusqu'au 19 décembre 2020, afin de permettre un transfert en douceur de l'administration technique de FIU.net vers une autre entité.
- <sup>35</sup> Voir point 33 du programme de travail remanié de la Commission, disponible à l'adresse suivante: [https://ec.europa.eu/info/sites/info/files/cwp-2020-adjusted-annexes\\_en.pdf](https://ec.europa.eu/info/sites/info/files/cwp-2020-adjusted-annexes_en.pdf).
- <sup>36</sup> [https://ec.europa.eu/info/sites/info/files/report\\_assessing\\_the\\_framework\\_for\\_financial\\_intelligence\\_units\\_fius\\_cooperation\\_with\\_third\\_countries\\_and\\_obstacles\\_and\\_opportunities\\_to\\_enhance\\_cooperation\\_between\\_financial\\_intelligence\\_units\\_with.pdf](https://ec.europa.eu/info/sites/info/files/report_assessing_the_framework_for_financial_intelligence_units_fius_cooperation_with_third_countries_and_obstacles_and_opportunities_to_enhance_cooperation_between_financial_intelligence_units_with.pdf)
- <sup>37</sup> Voir avis 1/2017 du CEPD, point 52.
- <sup>38</sup> Voir <https://www.fatf-gafi.org/fr/publications/gafiengeneral/documents/public-private-sector-partnership.html>.
- <sup>39</sup> <https://ec.europa.eu/digital-single-market/en/public-private-partnerships>
- <sup>40</sup> Voir note de fin de document 19.
- <sup>41</sup> Voir avis 1/2017, point 16.
- <sup>42</sup> Voir guide sur la nécessité du CEPD, disponible à l'adresse: [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_fr.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf).
- <sup>43</sup> Tsingou, E., «Global financial governance and the developing anti-money laundering regime: What lessons for International Political Economy?», *International Politics* 47, 617–637 (2010). <https://doi.org/10.1057/ip.2010.32>
- <sup>44</sup> Voir <https://www.fatf-gafi.org/fr/publications/gafiengeneral/documents/public-private-sector-partnership.html>.
- <sup>45</sup> [https://rusi.org/sites/default/files/201710\\_rusi\\_the\\_role\\_of\\_fisps\\_in\\_the\\_disruption\\_of\\_crime\\_maxwell\\_aringstall\\_web\\_4.2.pdf](https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_aringstall_web_4.2.pdf)

---

<sup>46</sup> L'expérience des PPP en matière de renseignement financier au sein de l'Union européenne s'est limitée à la task-force conjointe britannique sur le renseignement relatif au blanchiment de capitaux (Joint Money Laundering Intelligence Taskforce – JMLIT). La JMLIT se structure en trois volets: 1) un groupe opérationnel pour le partage d'informations sur les activités au niveau opérationnel entre le secteur financier, les services répressifs et l'autorité de conduite financière; 2) divers groupes de travail composés d'experts qui recensent et évaluent les menaces nouvelles et émergentes de blanchiment de capitaux et de financement du terrorisme et qui fournissent des produits de la connaissance, tels que des typologies et des indicateurs d'alerte; et 3) un service d'alerte destiné à diffuser plus largement les évaluations et les typologies, qui est assuré par UK Finance.

<sup>47</sup> [https://ec.europa.eu/info/sites/info/files/business\\_economy\\_euro/banking\\_and\\_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology\\_en.pdf](https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology_en.pdf)