LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Lignes directrices relatives à la protection des données dans la réglementation européenne des services financiers


LE CONTRÔLEUR EUROPÉEN
DE LA PROTECTION DES DONNÉES

Table des matières

Liste des 10 points à vérifier pour l'analyse de la protection des données et du respect de la vie privée

Cette liste de questions, mise au point pour les décideurs et les législateurs dans le domaine de la réglementation des services financiers, est un résumé de la méthodologie en 10 étapes recommandée par le CEPD à la section 3 des présentes lignes directrices.

1. *Les données à caractère personnel, et en particulier les données sensibles, sont-elles susceptibles d'être traitées, c'est-à-dire collectées, analysées ou utilisées d'une quelconque manière? Et si oui, de quelles données s'agit-il?*

2. *Le traitement des données à caractère personnel porte-t-il atteinte au droit de l'individu au respect de sa vie privée et familiale, de son domicile et de sa correspondance?*

3. *Le traitement des données à caractère personnel répond-il à une finalité claire? Les données seront-elles traitées ultérieurement pour d'autres finalités et, si oui, ces finalités sont-elles compatibles avec la finalité d'origine?*

4. *Existe-t-il une base juridique pour le traitement des données à caractère personnel?*

5. *En fonction de l'analyse d'impact, quelle est la période maximale proportionnée pendant laquelle les données à caractère personnel peuvent être stockées ou conservées?*

6. *Qui, au sein de l'UE, a besoin d'accéder aux données pour les finalités déclarées?*

7. *Est-il nécessaire de transférer des données à caractère personnel à des pays tiers? Quelle est la base juridique d'un tel transfert?*

8. *Les personnes concernées ont-elles suffisamment de garanties en ce qui concerne la possibilité d'exercer leurs droits d'accès et de rectification ainsi que d'autres droits pertinents?*

9. *Quelles sont les mesures techniques et organisationnelles appropriées en matière de sécurité, notamment lorsque des bases de données et des systèmes informatiques importants ou complexes sont envisagés?*

10. *Pouvez-vous démontrer à une autorité de contrôle indépendante que le traitement des données à caractère personnel est conforme à la loi sur la protection des données?*

1. La réglementation en matière de protection des données et de services financiers

Pourquoi la protection des données est importante pour la réglementation des services financiers

1. La réglementation des services financiers dans l'UE a pour but de garantir la stabilité financière, l'efficacité du marché unique des services financiers, ainsi que l'intégrité et la confiance des marchés.[1] Les mesures dans ce domaine comprennent notamment les exigences bancaires en matière de fonds propres, les règles sur les marchés des produits dérivés, le secteur de l'assurance, les titres et les fonds de placement, les infrastructures des marchés financiers, les services financiers de détail et les systèmes de paiement. Depuis l'éclatement de la crise financière, en 2008, plus de 40 nouvelles lois, dont beaucoup découlent d'engagements pris par le G20, ont été proposées, et la plupart d'entre elles ont été adoptées. Ce vaste corpus règlementaire prévoit un contrôle étroit du comportement des opérateurs et des investisseurs sur les marchés financiers, à travers l'attribution de pouvoirs accrus aux autorités de surveillance, la transparence à l'égard de tous les participants au marché, le contrôle de la prise de risques et la protection des consommateurs, des investisseurs et des contribuables contre les activités risquées. D'autres mesures, comme les directives sur le blanchiment de capitaux et le financement du terrorisme, ou le règlement sur les règles financières applicables au budget annuel de l'UE, imposent un certain nombre d'obligations aux institutions financières.

2. La plupart de ces mesures concernent les actions des personnes morales. Toutefois, nombre d'entre elles, comme celles relatives à la surveillance, à la conservation et la déclaration d'informations, à l'échange de données, aux pouvoirs des autorités compétentes et aux sanctions pour violation des règles applicables, nécessitent le traitement de données à caractère personnel, c'est-à-dire des données relatives à des personnes physiques directement ou indirectement identifiables. Certaines mesures peuvent également être attentatoires au droit au respect de la vie privée.

3. Le respect des droits des individus à la vie privée et à la protection des données, tels que consacrés par la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»), est une condition essentielle de la validité de la législation de l'UE.[2] Les règles et principes de protection des données consacrés, en particulier, à l'article 8 de la Charte et à l'article 16 du traité sur le fonctionnement de l'Union européenne (le «TFUE»), sont destinés à faciliter la libre circulation des informations au sein du marché intérieur, mais aussi à protéger les droits et intérêts de la personne. La bonne application des règles et des principes de protection des données devrait donc contribuer à renforcer l'efficacité et la qualité de l'élaboration des politiques et de la législation dans le domaine de la réglementation des services financiers.

L'objet des présentes lignes directrices

4. Le CEPD a pour objectif de veiller à ce que les institutions et organes de l'UE soient conscients des obligations relatives à la protection des données et intègrent des normes exigeantes en matière de protection des données dans toutes les nouvelles

[1] COM(2014) 279 final, Un secteur financier réformé pour l'Europe.
[2] Voir affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland Ltd*, arrêt de la CJUE du 8 avril 2014.

législations[3]. Le présent document s'adresse aux décideurs et aux législateurs dans le domaine de la réglementation des services financiers. Il fait partie de la «boîte à outils des politiques» développée par le CEPD à l'intention des institutions de l'UE, afin de faciliter l'élaboration de politiques respectueuses des droits et libertés fondamentaux prévus par la Charte, et en particulier des droits au respect de la vie privée et à la protection des données à caractère personnel.[4] S'appuyant sur le document stratégique publié en juin 2014 («Le CEPD en tant que conseiller des institutions de l'UE à l'égard des politiques et des législations: tirer profit de dix années d'expérience»), sur les avis formulés par le CEPD au cours des dernières années, à la fois en tant que conseiller des institutions de l'UE à l'égard des politiques et des législations et en tant qu'autorité de contrôle, ainsi que sur les enseignements tirés au cours d'un séminaire organisé par la DG MARKT en février 2014, le présent document porte sur les différents types de mesures prises dans le cadre de la réglementation des services financiers qui sont les plus susceptibles d'avoir une incidence sur la protection des données.

Comment utiliser ces lignes directrices?

5. Les lignes directrices sont structurées comme suit:

    - la section 2 résume la nature des droits au respect de la vie privée et à la protection des données à caractère personnel dans le cadre des droits fondamentaux de l'UE;

    - la section 3 décrit les étapes analytiques nécessaires pour évaluer les aspects des mesures proposées liés à la protection des données;[5]

    - la section 4 illustre l'application des règles de protection des données par la mise en place de mesures spécifiques dans la réglementation des services financiers actuelle ou proposée;

    - la section 5 expose la façon dont le CEPD propose de continuer à travailler avec les décideurs et les législateurs dans le domaine de la réglementation des services financiers dans le futur.

6. Ces lignes directrices, qui sont conçues comme des orientations pratiques, point par point, pour accompagner les décideurs dans le processus d'élaboration des politiques, peuvent compléter les lignes directrices de la Commission sur l'analyse d'impact. Elles seront régulièrement réexaminées, et le CEPD vous invite à lui faire part de vos remarques et commentaires concernant leur utilité.

7. La proposition de règlement général sur la protection des données de la Commission prévoit l'obligation, pour les autorités ou organes publics, de réaliser une «analyse d'impact relative à la protection des données» («si celle-ci n'a pas été faite au moment de l'adoption de la loi nationale régissant la mission de l'autorité ou de l'organisme publics concernés ainsi que l'opération ou l'ensemble d'opérations de traitement en

[3] Stratégie 2013-2014 du CEPD pour «Atteindre l'excellence en matière de protection des données», 22 janvier 2013.
[4] Document stratégique du CEPD, «Le CEPD en tant que conseiller des institutions de l'UE à l'égard des politiques et des législations: tirer profit de dix années d'expérience», 4 juin 2014.
[5] Voir le document stratégique du CEPD, section 4.3.

question»).[6] Dès lors, le CEPD recommande aux décideurs de se référer aux dernières normes internationales concernant les analyses d'impact relatives au respect de la vie privée, telles que la norme ISO 22307:2008 Services financiers - Analyse d'impact relative au respect de la vie privée.

2. Aperçu du cadre juridique de l'UE en matière de protection des données

La Charte des droits fondamentaux de l'UE

8. Une mesure de l'UE n'est licite que si elle est conforme à la Charte.[7] Les droits au respect de la vie privée et familiale et à la protection des données à caractère personnel prévus aux articles 7 et 8 de la Charte, sont étroitement liés et se recoupent même partiellement.[8] La protection des données, en tant que droit, tire son origine du droit au respect de la vie privée tel que consacré, en particulier, à l'article 8 de la Convention européenne des droits de l'homme (la «CEDH»). Ces deux droits sont des manifestations récentes des principes universels et éthiques de dignité et d'autonomie, mais aussi du droit de chaque individu de développer sa personnalité et d'exprimer son avis sur les questions ayant un impact direct sur lui. L'objectif commun qui sous-tend ces droits est d'éviter toute ingérence excessive et de permettre aux individus d'exercer un contrôle suffisant sur leur propre vie.

9. En vertu de la Charte, qui, depuis l'entrée en vigueur du Traité de Lisbonne, a valeur de droit primaire dans l'UE, les droits au respect de la vie privée et à la protection des données sont des droits distincts. Aussi n'est-il pas nécessaire, lors de l'analyse du droit à la protection des données, de se référer systématiquement au droit antérieur au respect de la vie privée. La jurisprudence pertinente souligne le défi, pour la Cour de justice de l'Union européenne (CJEU), de mettre en œuvre une approche claire et cohérente concernant l'application de ces droits et libertés distincts consacrés par la Charte, dont les différences revêtent une importance considérable pour la protection de l'individu.

Le droit au respect de la vie privée

10. Le droit au respect de la vie privée et familiale, du domicile et de la correspondance, tel que consacré à l'article 7 de la Charte, protège avant tout l'individu contre toute ingérence dans sa vie privée.[9] Il s'agit d'un droit classique «négatif» qui protège les personnes physiques, en premier lieu, contre toute ingérence de l'État. Toute ingérence doit, conformément à l'article 52, paragraphe 1, de la Charte, être prévue par la loi, respecter le contenu essentiel du droit et être justifiable, «dans le respect du principe de proportionnalité», du fait qu'elle est «nécessaire et répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui». En outre, la notion de vie privée a évolué dans la

[6] Considérant 73 et article 33 de la proposition de règlement général sur la protection des données, COM(2012) 11 final, 25 janvier 2012.
[7] Affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof* et *Österreichischer Rundfunk*, arrêt de la CJUE du 20 mai 2003.
[8] Affaires jointes C-92/09 et C-93/09, *Schecke* et *Eifert*, arrêt de la CJUE du 9 novembre 2010, points 47 à 52.
[9] Ainsi, l'article 7 de la Charte constitue quasiment l'exact pendant de l'article 8 de la CEDH, la seule différence tenant au remplacement du terme «correspondance» dans la CEDH par le terme «communications».

jurisprudence et recouvre désormais les situations intimes, mais aussi les activités purement personnelles, domestiques ou sociales des personnes physiques.[10]

11. Dans la pratique, cela signifie que les mesures attentatoires au droit au respect de la vie privée doivent être fondées sur une appréciation correcte et empirique d'autres mesures moins intrusives.[11] La CJUE a considéré que la publication d'informations sur les rémunérations de dirigeants d'entreprises semi-publiques constituerait une ingérence disproportionnée dans la vie privée.[12] Dans un autre arrêt, la Cour a annulé une mesure de l'UE exigeant la publication d'informations sur les bénéficiaires d'aides agricoles sur un site web, la Cour n'ayant trouvé aucun élément prouvant que le législateur avait envisagé des solutions moins intrusives.[13]

Le droit à la protection des données à caractère personnel

12. Les données à caractère personnel englobent toutes les informations relatives à des personnes identifiées ou identifiables. Dans la CEDH, la protection des données ne fait pas l'objet d'un droit distinct mais découle de l'article 8 de la CEDH sur le droit au respect de la vie privée, comme en témoigne la jurisprudence pertinente. Cela n'est pas le cas dans l'UE en ce qui concerne la Charte des droits fondamentaux. En effet, l'article 8 de la Charte consacre la protection des données à caractère personnel comme un droit distinct et anticipatoire, qui accorde aux personnes physiques le droit que leurs informations ne puissent être traitées (par *quiconque* et pas seulement par l'État) que sous réserve de la satisfaction des conditions essentielles énoncées aux paragraphes 2 et 3 de l'article 8. Selon ces dispositions, le traitement doit être loyal et licite, transparent pour la personne physique (la «personne concernée» en droit européen) et effectué à des fins déterminées. La personne physique a le droit d'accéder aux informations la concernant et de les rectifier, et ses droits doivent faire l'objet d'un contrôle par une autorité indépendante. Ces conditions, qui reposent sur certains des principes (mais pas tous) énoncés dans la directive 95/46/CE (ci-après désignée par la «directive sur la protection des données»), peuvent être considérées comme l'«essence» du droit.[14] Le droit à la protection des données à caractère personnel vise également à protéger d'autres droits et libertés fondamentaux, notamment – mais pas exclusivement – le droit au respect de la vie privée, en ce sens qu'il nécessite d'assurer un équilibre avec les autres intérêts et objectifs de l'UE.[15]

13. L'article 16 du TFUE constitue la base juridique pour l'adoption de règles relatives à la protection des données et à la libre circulation de ces données au sein de l'UE. Ces règles (résumées ci-dessous) prévoient un système de poids et contrepoids avec des droits et obligations, des procédures et des mécanismes de surveillance spécifiques. Elles s'appliquent à tous les traitements de données à caractère personnel, automatisés en tout ou en partie, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier, sauf pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit de l'UE, ou pour

[10] Voir également le document de travail du Groupe de travail «Article 29» sur la protection des données relatif à la surveillance des communications électroniques sur le lieu de travail, WP55, 2002.
[11] *Schecke*, points 81 à 85.
[12] *Rundfunk*, point 74.
[13] *Schecke*, point 81 à 86.
[14] Ainsi que l'a confirmé la CJUE, qui considère un contrôleur de la protection des données indépendant comme un «composant essentiel» de l'article 8; affaire C-14/10 *Commission contre Autriche*, arrêt de la CJUE du 16 octobre 2012; C-288/12, *Commission contre Hongrie*, arrêt de la CJUE du 8 avril 2014.
[15] Avis 4/2007 du Groupe de travail «Article 29» sur les données à caractère personnel, WP 136, 2007, p. 7.

l'exercice d'activités exclusivement personnelles ou domestiques.[16] Chaque État membre est tenu d'appliquer les dispositions nationales qu'il arrête aux traitements effectués «dans le cadre des activités d'un établissement du responsable du traitement sur le territoire» de l'État membre en question, même lorsque l'établissement lui-même est basé dans un autre État membre ou dans un pays tiers.[17] Un ou plusieurs de ces instruments peuvent donc s'appliquer aux mesures prévues dans la réglementation des services financiers.

14. En d'autres termes, le cadre de l'UE n'interdit pas le traitement de données à caractère personnel; au contraire, l'UE encourage le traitement à condition de clarifier les «règles du jeu» pour les citoyens, les entreprises et les autorités.

La protection des données et le respect de la vie privée: des droits distincts

15. La protection des données et le respect de la vie privée sont des droits distincts, tant par leur nature que par leur fonctionnement, qui nécessitent une analyse et une application séparées. Le champ d'application de la protection des données est vaste. Si l'ingérence dans la vie privée doit être déterminée en fonction du contexte, les règles de protection des données s'appliquent à tous les traitements, hormis certaines exceptions.[18] De même, le droit au respect de la vie privée est plus large que le droit à la protection des données. En effet, il concerne le domicile et la famille et recouvre, outre les données à caractère personnel, de nombreux autres aspects.[19] Ainsi, les situations qui relèvent du champ d'application de la législation en matière de protection des données ne sont pas toutes couvertes par le droit au respect de la vie privée, et les situations touchant au droit au respect de la vie privée ne supposent pas forcément le traitement de données à caractère personnel.

16. Certaines mesures impliquent le traitement de données à caractère personnel et doivent, de ce fait, se conformer aux règles en matière de protection des données, même si elles n'ont aucune incidence sur le droit au respect de la vie privée. Ainsi, par exemple, la CJUE a conclu que la mémorisation par un employeur des noms et des données relatives aux rémunérations de ses salariés ne pouvait constituer une ingérence dans la vie privée (bien entendu, dans la mesure où il s'agit d'un traitement de données, une telle mémorisation doit toutefois se conformer aux règles de l'UE concernant la protection des données).[20]

17. Dans d'autres cas, le traitement de données à caractère personnel a une incidence sur le droit au respect de la vie privée. Dans l'arrêt *Rundfunk* précité, la CJUE a estimé que la communication de données relatives aux salariés – qu'elles soient «sensibles» ou non – par l'employeur à un tiers (comme une autorité publique dans l'affaire en question) porterait effectivement atteinte au droit au respect de la vie privée des personnes concernées.[21] Un tel effet est probable lorsque les données en question sont sensibles (comme des données médicales, par exemple), lorsque les données sont utilisées à des fins répressives ou de surveillance, ou lorsque le traitement présente un

[16] Article 3 de la directive 95/46/CE.
[17] Article 4, paragraphe 1, point a), de la directive 95/46/CE. Voir également l'affaire C-131/12, *Google Spain contre Agencia Española de Protección de Datos*, arrêt de la CJUE du 13 mai 2014, point 52.
[18] Voir le point 13 ci-dessus.
[19] Voir, par exemple, l'arrêt de la Cour suprême des États-Unis dans l'affaire *Griswold contre Connecticut* (1965).
[20] *Rundfunk*, point 74.
[21] *Rundfunk*, points 74 et 75.

caractère permanent ou systématique, par exemple lorsque les informations sont conservées et pas seulement collectées et utilisées.

18. Le caractère distinct des deux droits a été reconnu, dans une certaine mesure, dans l'arrêt rendu dans l'affaire *Digital Rights Ireland* concernant la conservation obligatoire de données de communications. Dans cette affaire, la CJUE a considéré qu'il n'était pas suffisant d'appliquer l'article 7 relatif au droit au respect de la vie privée (bien que celui-ci ait retenu l'attention des tribunaux nationaux ayant renvoyé les affaires en question devant la CJUE). En effet, la Cour a estimé que la conservation de données constituait un traitement de données à caractère personnel au sens de l'article 8 et que, partant, elle devait nécessairement satisfaire aux exigences spécifiques découlant de cet article.[22]

19. La compréhension de l'étendue, de la finalité et de la base juridique du traitement de données à caractère personnel permet d'éclairer, comme entendent l'expliquer les présentes lignes directrices, l'examen de la question de savoir si la mesure proposée porte atteinte ou non au droit au respect de la vie privée consacré à l'article 7 de la Charte.

Aperçu du cadre juridique en matière de protection des données

20. Le cadre juridique régissant le traitement des données à caractère personnel dans l'UE se compose actuellement de quatre instruments principaux:

- **La directive 95/46/CE**[23] (ou directive sur la protection des données) est la pierre angulaire de la législation relative à la protection des données à caractère personnel en Europe. Elle fixe des règles générales concernant la licéité des traitements de données à caractère personnel et les droits des personnes physiques dont les données sont traitées (personnes concernées), et elle oblige chaque État membre à veiller à la mise en place d'une autorité de contrôle indépendante chargée du suivi de la mise en œuvre de la directive.

- **Le règlement (CE) nº 45/2001**[24] porte sur le traitement de données à caractère personnel par les institutions et organes de l'UE et instaure le CEPD en tant qu'autorité de contrôle indépendante.

- **La directive 2002/58/CE**[25] concerne le traitement de données à caractère personnel dans le secteur des communications électroniques et fixe des règles qui revêtent une importance particulière pour la confidentialité, les données relatives à la facturation et au trafic, ainsi que les communications commerciales non sollicitées.

[22] *Digital Rights*, point 29.

[23] La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281, 23.11.1995, p. 31 à 50**.** La directive est en cours de révision et sera remplacée par la proposition de règlement général sur la protection des données (note en bas de page 6), laquelle, une fois entrée en vigueur, nécessitera une révision de la directive 2002/58/CE et du règlement (CE) nº 45/2001 afin de s'assurer de l'harmonisation des règles.

[24] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO L 008, 12.01.2001, p. 1 à 22.

[25] Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201, 31.07.2002, p. 37 à 47.

- **La décision-cadre 2008/977/JAI du Conseil**[26] concerne la coopération policière et judiciaire en matière pénale et fixe des règles applicables aux échanges de données à caractère personnel, notamment les bases de données nationales et européennes et les transmissions aux autorités compétentes et à des personnes privées 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.

3. Les dix étapes analytiques

21. Comme l'indique la section précédente, le cadre juridique de l'UE est complexe. Aussi le CEPD a-t-il préparé, pour la réglementation des services financiers, une méthodologie en 10 étapes destinée à aider les décideurs à anticiper certaines difficultés qui peuvent se présenter.

1) Identifier les données à caractère personnel à traiter

Définition des données à caractère personnel

22. Toute mesure prévoyant le traitement de données à caractère personnel doit indiquer clairement les catégories de données à caractère personnel, et tout particulièrement les données sensibles, à traiter.

23. Les données à caractère personnel sont définies[27] comme toute information concernant une personne physique identifiée ou identifiable («personne concernée»). Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Il s'agit d'une notion large qui englobe beaucoup plus d'informations que les données permettant d'identifier directement une personne, comme un nom, un numéro national d'enregistrement ou un numéro d'identification fiscal, et qui recouvre également, par exemple, les informations concernant la rémunération, le montant des revenus du travail et du capital et celui des subventions perçues par les personnes physiques, les informations biométriques, les adresses IP, les données relatives au trafic et les données de localisation, les périodes de travail journalières, les périodes de repos ainsi que les interruptions et pauses correspondantes.[28]

[26] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350, 30.12.2008, p. 60 à 71. Cette décision-cadre est également en cours de révision et sera remplacée par une proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données; COM(2012) 10 final, 25 janvier 2012.

[27] Article 2, point a), de la directive 95/46/CE.

[28] Le Groupe de travail «Article 29», dans l'avis 4/2007, analyse les quatre éléments constitutifs de cette notion, à savoir «toute information», «concernant», «identifiée ou identifiable» et «personne physique», chacun de ces éléments devant être évalué afin de déterminer si des «données à caractère personnel» sont en jeu dans une situation donnée. Voir également la section 4.1 du document stratégique du CEPD.

Les données sensibles

24. Les mesures réglementaires dans le secteur financier impliquent souvent le traitement de données relatives à des infractions et des condamnations pénales ou à des soupçons d'infractions pénales: ces données sont qualifiées de «*données sensibles*».[29] Les autres types de données sensibles en vertu du droit de l'UE comprennent les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle. Dans l'UE, le traitement de données sensibles ne peut, en principe, être effectué que s'il respecte des conditions strictes et met en œuvre des garanties de confidentialité et de sécurité appropriées telles que prévues par le droit national.[30]

L'anonymisation

25. Les données à caractère personnel qui ont été rendues anonymes, c'est-à-dire les données qui ont été modifiées d'une manière telle que la personne concernée n'est plus identifiable, ne sont pas soumises aux règles de l'UE en matière de protection des données.[31] Toutefois, la technologie permet de plus en plus de ré-identifier une personne à l'aide de données rendues anonymes, par exemple en recoupant les données avec d'autres sources d'informations éventuellement disponibles, y compris publiquement. Par conséquent, la meilleure façon de garantir la protection de la personne physique n'est pas de rendre les données anonymes, mais plutôt de limiter le traitement des données à caractère personnel au minimum nécessaire.

Définition du traitement et du responsable du traitement

26. «Traitement» est défini comme «toute opération ou ensemble d'opérations, effectuée(s) ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction».[32] Toute mesure impliquant le traitement de données à caractère personnel (qu'elle soit considérée ou non comme une atteinte à la vie privée) doit se conformer à la loi applicable en matière de protection des données.

27. Le «responsable du traitement» est la personne physique ou morale qui détermine les «finalités et les moyens» du traitement et à qui incombe, dans l'UE, la plupart des responsabilités et obligations juridiques en matière de protection des données, comme le fait de veiller à la qualité des données, d'appliquer des mesures de sécurité appropriées et de répondre à toute demande formulée par une personne concernée qui souhaite exercer ses droits. Pour toute mesure impliquant le traitement de données à

[29] L'article 8 de la directive 95/46/CE énumère des «catégories particulières» de données à caractère personnel. L'article 10 du règlement 45/2001 porte sur le traitement de ces catégories par une institution ou un organe de l'UE; l'article 6 de la décision-cadre 2008/977/JAI porte sur le traitement des données par les autorités compétentes en matière répressive.

[30] Article 8, paragraphe 5, de la directive 95/46/CE. Voir les points 59 à 61 ci-dessous sur les mesures relatives à la sécurité des données.

[31] Considérant 26 de la directive 95/46/CE.

[32] Article 2, point b), de la directive 95/46/CE.

caractère personnel, l'identité du responsable du traitement doit être clairement indiquée.

Recommandation

28. Toutes les mesures impliquant le traitement de données à caractère personnel doivent comporter une disposition de fond exigeant que le traitement soit conforme aux règles européennes et nationales en matière de protection des données. Cette disposition devrait être incluse dans l'instrument juridique lui-même et non pas laissée à des actes délégués ou d'exécution de la Commission ou à des mesures de transposition des États membres.[33] La disposition devrait indiquer, le plus précisément possible:

    a) le type de données à traiter, et tout particulièrement s'il y a des données sensibles,

    b) la durée de conservation des données,

    c) qui pourra avoir accès aux données, et

    d) des garanties appropriées pour protéger les droits de la personne physique.

2) Déterminer si le traitement de données constitue une ingérence dans le droit au respect de la vie privée

29. Des analyses séparées sont nécessaires pour déterminer la conformité d'une mesure proposée avec le droit au respect de la vie privée, d'un côté, et avec le droit à la protection des données, de l'autre. Si une atteinte au droit au respect de la vie privée est constatée, l'article 52, paragraphe 1, de la Charte devient pertinent.[34]

Le pouvoir de pénétrer dans des locaux privés dans le règlement relatif aux abus de marché

Le pouvoir de pénétrer dans des locaux privés pour y saisir des documents sous quelque forme que ce soit présente un caractère très intrusif. En temps normal, les contrôles in situ par les autorités compétentes devraient être limités aux locaux commerciaux de l'entreprise en question et exclure l'inspection des locaux privés des salariés, sauf si cela est strictement nécessaire.

Le CEPD a fait valoir, dans son avis sur la proposition de la Commission, qu'un tel pouvoir devrait être soumis à l'obligation générale d'obtenir une autorisation judiciaire préalable. Le règlement tel qu'adopté comporte une disposition prévoyant une autorisation judiciaire préalable, dans le respect du droit national.

Recommandation

30. Les décideurs devraient s'assurer, dans le cadre de l'analyse d'impact, que toute ingérence est proportionnelle à la finalité de la mesure, et vérifier s'il n'existe pas d'autres mesures moins attentatoires au droit fondamental en cause qui permettraient d'obtenir le résultat souhaité.[35] Si aucune mesure alternative n'est disponible, les

[33] Voir, par exemple, l'avis du CEPD sur l'ordonnance européenne de saisie conservatoire des comptes bancaires, 13 octobre 2011, p. 4.
[34] Voir les points 10 et 11 ci-dessus.
[35] Dans les affaires jointes C-92/09 et C-93/09 (*Schecke*), la CJUE a considéré, au point 81, que, lors de l'adoption de mesures imposant la publication obligatoire de certaines informations relatives aux bénéficiaires de fonds de l'UE, les législateurs de l'UE auraient dû prendre en considération des modalités de publication de ces informations qui soient conformes à l'objectif d'une telle publication tout en étant moins attentatoires au

décideurs devraient limiter l'ingérence au strict nécessaire pour atteindre les finalités déclarées.[36] Cet objectif pourrait être réalisé en réduisant la quantité de données à traiter ou en prévoyant des garanties spécifiques concernant les droits des personnes physiques dans l'instrument lui-même.[37]

3) Définir la finalité du traitement des données à caractère personnel

31. Les données à caractère personnel ne peuvent être collectées que pour des finalités «déterminées, explicites et légitimes», et ne doivent pas être «traitées ultérieurement de manière incompatible» avec ces finalités.[38] C'est le principe de la *«limitation de la finalité»*. Dans la réglementation des services financiers, les intérêts publics légitimes comprennent notamment la stabilité du système financier, la transparence, la prévention des abus de marché, le renforcement de l'intégrité du marché et de la protection des investisseurs, ainsi que la lutte contre le blanchiment de capitaux. Les autorités répressives peuvent demander des informations à des tiers, notamment en ce qui concerne la population, la sécurité sociale, les registres fiscaux et les opérateurs de télécommunications, qui comprennent des données à caractère personnel collectées initialement à d'autres fins. Toute mesure prévoyant de telles dispositions devrait appliquer explicitement les exceptions et limitations visées à l'article 13 de la directive sur la protection des données, en vertu duquel les États membres peuvent prendre des mesures législatives nécessaires pour sauvegarder les missions de contrôle, d'inspection ou de réglementation liées à un intérêt économique ou financier d'un État membre ou de l'UE.

32. Aucune information collectée dans le cadre de ces mesures ne devrait être utilisée ultérieurement pour d'autres finalités incompatibles. Le Groupe de travail «Article 29» a fourni des orientations sur les critères sur lesquels l'évaluation de la compatibilité de la finalité devrait se fonder.[39] Un traitement ultérieur pour d'autres finalités susceptibles de porter atteinte aux droits de la personne physique sera probablement incompatible. Ainsi, par exemple, les données collectées, à l'origine, aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, ne devraient pas être traitées ultérieurement pour la lutte contre la fraude et l'évasion fiscales, à moins que l'instrument applicable ne stipule clairement ces finalités.[40]

33. Les règles de l'UE concernant la protection des données prévoient également le principe de la *«minimisation des données»*, selon lequel seules les données qui sont adéquates, pertinentes et non excessives au regard de la finalité définie sont collectées et utilisées.[41] Pour chaque type de données à caractère personnel, les décideurs devraient évaluer la proportionnalité du traitement par rapport aux «objectifs légitimes

---

droit de ces bénéficiaires au respect de leur vie privée, en général, et à la protection de leurs données à caractère personnel, en particulier.

[36] La CJUE a retenu que, compte tenu de l'ampleur de l'ingérence dans les droits fondamentaux des personnes physiques, le pouvoir d'appréciation du législateur était nécessairement réduit (*Digital Rights Ireland*, point 48).

[37] Voir les points 50 à 58 ci-dessous. Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, 10 février 2012, points 40 à 42 et 47.

[38] Article 6, paragraphe 1, point b), de la directive 95/46/CE, article 4, paragraphe 1, point b), du règlement 45/2001 et article 3 de la décision-cadre 2008/977/JAI.

[39] Voir l'avis 3/2013 du Groupe de travail «Article 29» sur le principe de la limitation de la finalité, 2013.

[40] Voir l'avis du CEPD sur la lutte contre le blanchiment de capitaux, 4 juillet 2013, p. 8 et 9.

[41] Article 6, paragraphe 1, point c), de la directive 95/46/CE et article 4, paragraphe 1, point c), du règlement 45/2001.

poursuivis» et vérifier si la finalité de la mesure pourrait être atteinte sans traiter les données.[42]

Listes d'initiés

«Informations privilégiées» désigne des informations non publiques concernant des émetteurs d'instruments financiers qui, si elles étaient rendus publiques, pourraient affecter de manière significative les cours de ces instruments financiers ou d'instruments dérivés qui leur sont liés («opérations d'initiés»). Conformément à l'article 18 du règlement sur les abus de marché, les émetteurs d'instruments financiers (ou toute personne agissant en leur nom ou pour leur compte) doivent établir une liste de toutes les personnes qui ont accès aux informations privilégiées, et qui travaillent pour eux en vertu d'un contrat de travail ou exécutent des tâches leur donnant accès à des informations privilégiées, comme les conseillers, les comptables ou les agences de notation de crédit. Ces listes d'initiés permettent aux autorités compétentes d'enquêter sur d'éventuels abus de marché ou opérations d'initiés.

En accord avec la recommandation du CEPD, le règlement sur les abus de marché comprend une référence explicite à la finalité des listes, aux principaux éléments de la liste, aux raisons pour lesquelles des personnes sont inscrites sur la liste, ainsi qu'une référence à l'obligation de consulter le CEPD sur les projets de normes techniques d'exécution à élaborer par l'AEMF, en ce qui concerne le format précis des listes d'initiés et le format de mise à jour de ces listes.

Recommandation

34. La mesure devrait toujours préciser les finalités pour lesquelles les données à caractère personnel seront traitées, et spécifier, autant que possible, les traitements ultérieurs qui peuvent être considérés ou non comme compatibles.

4) Établir une base juridique pour le traitement des données

Les fondements juridiques possibles

35. En vertu de l'article 8, paragraphe 2, de la Charte, les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Ces fondements sont précisés plus avant dans la directive sur la protection des données et dans le règlement 45/2001.[43] La directive énumère ainsi plusieurs fondements possibles pour la légitimation du traitement:

    a) la personne concernée a indubitablement donné son consentement au traitement

    ou celui-ci est nécessaire:

    b) à l'exécution d'un contrat auquel la personne concernée est partie;

    c) au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

    d) à la sauvegarde de l'intérêt vital de la personne concernée;

    e) à l'exécution d'une mission d'intérêt public; ou

[42] Arrêt *Schecke*, point 74.
[43] Article 7 de la directive 95/46/CE et article 5 du règlement 45/2001.

f) à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, sous réserve d'un exercice de mise en balance supplémentaire visant à sauvegarder les droits et intérêts de la personne concernée.[44]

36. Le règlement 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes de l'UE contient un libellé similaire, mais il omet le fondement d'«intérêt légitime». Une base juridique couramment appliquée est la nécessité du traitement en vue de l'exécution d'une mission effectuée dans l'intérêt public sur la base du droit de l'UE.[45]

Le consentement en tant que base juridique

37. Bien que le consentement de la personne concernée soit un fondement juridique évident, il n'est pas toujours approprié en raison des conditions à respecter pour garantir la validité du consentement.[46] Par exemple, en ce qui concerne la transparence du patrimoine des débiteurs, la licéité du traitement de données relatives au patrimoine des débiteurs devrait reposer non pas sur le consentement, mais sur le respect d'une obligation légale ou la réalisation d'un intérêt public.[47] Pour les mesures de lutte contre le blanchiment de capitaux, le CEPD a suggéré comme base juridique appropriée la «nécessité du respect d'une obligation légale».[48] Les mesures visant à augmenter la transparence des marchés financiers devraient prendre en considération l'exécution d'une mission dans l'intérêt public plutôt que le consentement. Toutefois, le consentement peut être approprié dans des situations exceptionnelles *ad hoc* où la personne concernée ne risque pas de faire l'objet de pressions excessives; il peut également servir de «couche de protection» supplémentaire pour des informations particulièrement confidentielles.

Les données sensibles

38. Les données sensibles (c'est-à-dire les données relatives à des infractions, etc.; voir la définition qui en est donnée au point 24 ci-dessus) ne peuvent être traitées que si l'une des exceptions suivantes s'applique:[49]

a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre en dispose autrement;

b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates;

c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

[44] Voir l'avis 06/2014 du Groupe de travail «Article 29» sur la notion d'intérêt légitime du responsable du traitement en vertu de l'article 7 de la directive 95/46/CE.
[45] Article 5, point a), du règlement 45/2001.
[46] Article 2, point h), de la directive 95/46/CE et article 2, point h), du règlement 45/2001.
[47] Voir l'avis du CEPD sur le Livre vert de la Commission intitulé «Exécution effective des décisions judiciaires dans l'Union européenne: la transparence du patrimoine des débiteurs», 22 septembre 2008, points 9 à 12.
[48] Voir l'avis du CEPD sur la lutte contre le blanchiment de capitaux, point 33.
[49] Article 8, paragraphe 2, de la directive 95/46/CE.

d) le traitement est effectué dans le cadre de ses activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées; ou

e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

Recommandation

39. Toute mesure impliquant le traitement de données à caractère personnel devrait être fondée sur une analyse adéquate de la base juridique de ce traitement et préciser, si nécessaire, dans l'instrument lui-même, la base juridique du traitement. Toute mesure envisageant le traitement de données sensibles (telles que définies dans la directive sur la protection des données) doit indiquer clairement lesquelles, parmi les cinq exceptions, s'appliquent à l'interdiction générale.

5) Évaluer et justifier une période de conservation des données appropriée

40. Les données à caractère personnel nécessaires à la réalisation des finalités spécifiées doivent être supprimées dès qu'elles ne sont plus nécessaires à la réalisation de ces finalités, à moins que des règles européennes ou nationales spécifiques ne s'appliquent, comme celles prévoyant la conservation des données pour une période donnée, par exemple à des fins fiscales.[50]

La conservation des données dans le cadre du contrôle des entreprises d'investissement et de l'éventuel blanchiment de capitaux

Des mesures récentes ont adopté des approches divergentes en ce qui concerne la conservation des données à caractère personnel collectées dans le cadre du contrôle de la conformité avec les règles de l'UE.

Le règlement sur les abus de marché exige que les données à caractère personnel traitées dans le cadre d'activités de supervision soient conservées pendant une durée maximale de cinq ans.

Conformément à la directive révisée relative aux marchés d'instruments financiers, les entreprises d'investissement sont tenues de conserver un enregistrement de tout service fourni, de toute activité exercée et de toute transaction effectuée pendant cinq ans, ou «pendant une durée pouvant aller jusqu'à sept ans» si les informations sont demandées par une autorité compétente.

La proposition de la Commission concernant une nouvelle directive relative à la lutte contre le blanchiment de capitaux propose une période de conservation de cinq ans à la suite d'un paiement, période qui peut aller jusqu'à 10 ans – le CEPD a remis en cause cette disposition, la jugeant arbitraire et dépourvue de justification empirique.

[50] Article 6, paragraphe 1, point e), de la directive 95/46/CE et article 4, paragraphe 1, point e), du règlement 45/2001. Voir l'avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 16.

41. Le fait de spécifier la période de conservation des données dans un acte législatif contribue à améliorer la sécurité juridique et est davantage conforme aux meilleures pratiques. Cette période devrait être fixée non pas de manière arbitraire, mais en fonction de critères objectifs et sur la base d'une analyse au cas par cas.

Recommandation

42. Les législateurs devraient procéder à une évaluation approfondie afin de savoir quelle période de conservation des données à caractère personnel à traiter serait suffisante et proportionnée au regard de la finalité déclarée. L'analyse d'impact devrait comprendre une analyse des solutions pertinentes. Les décideurs devraient également envisager la possibilité d'une clause de réexamen prévoyant ou reportant à une date ultérieure l'examen et la révision de la période de conservation initiale. En l'absence d'une durée explicite, l'instrument proposé devrait, tout au moins, exiger que les données soient supprimées dès qu'elles ne sont plus nécessaires.

6) Identifier les parties au sein de l'UE qui peuvent avoir accès aux données à caractère personnel

43. Les échanges de données à caractère personnel entre des organisations privées et/ou des autorités publiques établies au sein de l'UE sont également considérés comme des traitements de données dans le cadre des règles de protection des données. Des règles distinctes s'appliquent aux échanges de données, selon que l'autorité concernée est:[51]

    - une autorité répressive ou judiciaire susceptible de relever du champ d'application de la décision-cadre 2008/977/JAI; ou

    - une autorité administrative chargée du contrôle des établissements de crédit ou financiers susceptible de relever, au niveau national, du champ d'application de la directive sur la protection des données, ou, au niveau européen, du règlement 45/2001.[52]

Recommandation

44. Les propositions devraient indiquer, de la façon la plus précise possible, les autorités compétentes concernées, et notamment:

    - les types de données à échanger;

    - les finalités pour lesquelles les données peuvent être transférées et traitées ultérieurement;[53] et

    - les garanties contre l'accès aux données par d'autres autorités ou des tiers extérieurs ayant un intérêt dans la finalité poursuivie.[54]

[51] Voir l'avis du CEPD sur la lutte contre le blanchiment de capitaux, 4 juillet 2013, p. 7 et 8.
[52] Les articles 7 et 8 du règlement 45/2001 régissent les transferts de données à caractère personnel entre institutions ou organes de l'UE ou en leur sein, ou à d'autres destinataires.
[53] Avis du CEPD sur le règlement financier applicable au budget général des Communautés européennes, 12 décembre 2006, p. 12 à 18, point 22.
[54] Voir notamment l'avis du CEPD sur la lutte contre le blanchiment de capitaux, p. 21 et 22.

7) Établir une base juridique adéquate pour tout transfert de données à caractère personnel en dehors de l'UE

45. Le transfert de données à caractère personnel vers des pays tiers présente des risques particuliers pour la personne physique, et toute exigence relative à une telle divulgation doit être mise en balance avec les droits de la personne physique.[55] En règle générale, en vertu des articles 25 et 26 de la directive relative à la protection des données et de l'article 9 du règlement 45/2001, les données à caractère personnel ne peuvent être transférées vers un pays tiers que si, sous réserve du respect des autres exigences applicables, la Commission estime que le pays destinataire assure un niveau de protection adéquat.[56] En l'absence d'une décision sur le caractère adéquat du niveau de protection, les données à caractère personnel peuvent être transférées pour autant que le transfert entre dans le champ d'application de l'une des dérogations, et notamment:

    a) la personne concernée a indubitablement donné son consentement au traitement proposé;

    b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;

    c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers;

    d) le transfert est nécessaire ou rendu juridiquement obligatoire pour des motifs d'intérêt public importants ou pour la constatation, l'exercice ou la défense d'un droit en justice.

46. Ces dérogations doivent être interprétées de manière prudente et restrictive, et faire l'objet d'une analyse au cas par cas.[57] En particulier, les motifs d'«intérêt public important» impliquent des intérêts identifiés comme tels par la législation nationale applicable aux responsables du traitement établis dans l'UE; les intérêts de pays tiers, ou les exigences légales établies par ceux-ci, ne sont pas, en eux-mêmes, valides ou

[55] Pour des orientations plus détaillées, voir le document de travail 1/2009 du Groupe de travail «Article 29» sur la communication de pièces préalable dans le cadre de poursuites transfrontalières en matière civile.

[56] Si les données doivent être transférées à une organisation internationale, celle-ci doit assurer un niveau de protection adéquat. Voir les décisions actuelles publiées par la Commission européenne concernant le caractère adéquat de la protection http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (dernier accès le 16 novembre 2014). En vertu de l'article 9 du règlement 45/2001, le responsable du traitement – c'est-à-dire l'institution ou l'organe de l'UE qui est à l'origine du transfert – a également la possibilité de procéder à une appréciation du caractère adéquat du niveau de protection offert par le pays tiers ou l'organisation internationale en question. Voir l'avis du CEPD, «Le transfert de données à caractère personnel à des pays tiers et des organisations internationales par des institutions et des organes de l'UE: document d'orientation», 14 juillet 2014. Si les données doivent être transférées à une organisation internationale, celle-ci doit assurer un niveau de protection adéquat. Voir les décisions actuelles publiées par la Commission européenne concernant le caractère adéquat de la protection http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (dernier accès le 16 novembre 2014).

[57] Voir le document de travail du Groupe de travail «Article 29» relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, p. 7.

suffisants.[58] Certaines mesures liées à la réglementation des services financiers prévoient la possibilité, pour les responsables du traitement, d'aller au-delà de leurs obligations légales spécifiques afin d'aider les autorités répressives ou les acteurs privés à combattre des activités illégales comme le blanchiment de capitaux ou la détection de la fraude. S'il est estimé qu'il existe un intérêt public important en vertu du droit national de l'État membre auquel est soumis le responsable du traitement, cette dérogation pourrait s'appliquer aux transferts de données à caractère personnel aux autorités compétentes de pays tiers, lorsque cela est nécessaire pour le contrôle de sociétés mères situées sur leur territoire et possédant une filiale dans un ou plusieurs États membres. Toutefois, l'«intérêt public» ne saurait être invoqué pour justifier des transferts réguliers, massifs ou structurels de données, ainsi que l'a fait valoir le CEPD à propos de la proposition de transfert massif de données personnelles et sensibles à des pays étrangers à des fins de lutte contre le blanchiment de capitaux.[59]

47. Si aucune dérogation ne s'applique, l'expéditeur des données doit justifier de garanties adéquates permettant de s'assurer que les personnes concernées sont correctement protégées[60] dans un instrument opposable et juridiquement contraignant. Pour les entités privées, ces garanties prennent généralement la forme d'un accord, par le biais de clauses contractuelles types, de règles d'entreprise contraignantes ou d'autres accords *ad hoc* entre l'expéditeur et le destinataire des données. Pour le secteur public, elles peuvent être couvertes par des engagements prévus dans des mémorandums d'accord ou des accords internationaux juridiquement contraignants. Lorsque des garanties adéquates sont invoquées, l'expéditeur des données peut également être tenu, en vertu de la loi applicable, d'informer ou d'obtenir l'autorisation préalable de la (des) autorité(s) compétente(s) en matière de protection des données.[61]

48. L'article 13 de la décision-cadre 2008/977/JAI prévoit un régime spécifique distinct pour les transferts internationaux nécessaires 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.

Recommandation

49. Les mesures prévoyant le transfert de données à caractère personnel vers des pays tiers doivent indiquer clairement la base juridique du transfert et devraient prévoir des décisions au cas par cas, dans le respect du principe de la minimisation des données (voir le point 33 ci-dessus). Il serait peut-être approprié de prévoir des garanties explicites concernant la qualité, la pertinence et la confidentialité des données, ainsi

[58] Document de travail du Groupe de travail «Article 29» sur l'article 26, paragraphe 1, p. 14 et 15. Le Groupe de travail souligne que le considérant 58 de la directive 95/46/CE mentionne les cas dans lesquels des échanges internationaux de données pourraient être nécessaires «entre les administrations fiscales et douanières de différents pays» ou «entre les services compétents en matière de sécurité sociale», ce qui implique que le transfert présente un intérêt pour les autorités d'un État membre de l'UE, et non pas seulement pour les autorités du pays tiers.

[59] Voir l'avis du CEPD sur la lutte contre le blanchiment de capitaux, pp. 11 et 12.

[60] Les garanties doivent assurer une protection adéquate des données par le destinataire par le biais d'engagements détaillés sur des aspects comme le droit des personnes concernées à poursuivre tout manquement aux obligations contractuelles de l'importateur ou de l'exportateur, les obligations de l'exportateur et de l'importateur, la responsabilité, les informations relatives à la médiation et à la juridiction, le droit applicable, la supervision, etc.

[61] En vertu du règlement 45/2001, le CEPD a la possibilité de délivrer une autorisation pour le transfert de données à caractère personnel.

qu'une autorisation préalable expresse de l'autorité compétente en vue du transfert ultérieur des données vers ou par un pays tiers.

8) Prévoir des garanties appropriées pour l'exercice des droits des personnes physiques en matière de protection des données

a) Le droit à l'information

50. Les personnes physiques ont le droit d'être suffisamment informées du traitement des données à caractère personnel les concernant et de leurs droits, que les données aient été collectées directement auprès d'elles ou d'autres sources.[62] Elles devraient obtenir au moins des informations sur l'identité du responsable du traitement, les finalités du traitement, ainsi que toute information supplémentaire qui pourrait s'avérer pertinente.

51. Les mesures devraient prévoir des garanties appropriées concernant le respect de ce droit. Par exemple, dans le contexte des alertes professionnelles,[63] la personne accusée devrait être informée de la nature de l'accusation. Dans le cas des bases de données de l'UE contenant des données à caractère personnel, la Commission ou tout organisme responsable de leur gestion devrait faire en sorte que la politique en matière de respect de la vie privée soit à la disposition du public sur son site web.

[62] Articles 10 et 11 de la directive 95/46/CE, articles 11 et 12 du règlement 45/2001 et article 16 de la décision-cadre 2008/977/JAI.

[63] En général, les dispositifs d'alerte professionnelle encouragent les membres d'une organisation, en échange d'une promesse d'impunité, à signaler les infractions aux règles existantes commises par un associé/collègue (actuel ou ancien) qui pourrait être tenu personnellement responsable en vertu de la loi applicable.

Le droit à l'information dans le contexte des dispositifs d'alerte professionnelle

Le règlement relatif aux abus de marché prévoit l'obligation, pour les autorités compétentes et les employeurs, de mettre en place des procédures pour le signalement d'infractions réelles ou potentielles au règlement.

Toute personne mise en cause dans le rapport d'un dénonciateur devrait en être informée par la personne responsable du dispositif d'alerte professionnelle, dans les plus brefs délais, dès la communication de l'information.

La personne mise en cause devrait être informée:

1) de l'entité responsable du dispositif d'alerte professionnelle,

2) des faits de l'accusation,

3) des départements ou services qui pourraient recevoir le rapport au sein de son entreprise ou dans d'autres entités ou entreprises du groupe dont cette dernière fait partie, et

4) des modalités d'exercice de ses droits d'accès et de rectification.

Toutefois, lorsque et tant qu'il existe un risque substantiel qu'une telle notification compromette la capacité de l'entreprise ou de l'autorité compétente à enquêter efficacement sur l'allégation ou à recueillir les éléments de preuve nécessaires, la personne responsable du dispositif d'alerte professionnelle peut reporter l'information de l'accusé.

Avis 1/2006 du Groupe de travail «Article 29» relatif à l'application des règles européennes de protection des données aux dispositifs internes d'alerte professionnelle («whistleblowing») dans les domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières, p. 13.

b) Les droits d'accès, de rectification et d'effacement

52. Après le début du traitement, les personnes physiques ont le droit d'obtenir du responsable du traitement, sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs, des informations sur les catégories de données traitées, sur la finalité du traitement, sur le destinataire des données et sur la «logique» qui sous-tend tout traitement automatisé des données à caractère personnel les concernant. Les personnes physiques peuvent obtenir l'accès, sous une forme intelligible, aux données à caractère personnel traitées. Ce droit d'accès, qui revêt une importance particulière pour les personnes accusées d'avoir commis un acte répréhensible par des dénonciateurs, est étroitement lié au droit à la bonne administration, et notamment le

droit d'être entendu avant l'adoption d'une décision, le droit à un recours effectif et le droit de la défense de tout accusé.[64]

53. Si le traitement n'est pas conforme aux règles de protection des données, notamment en raison du caractère incomplet ou inexact des données, les personnes physiques peuvent obtenir la rectification, l'effacement ou le verrouillage des données.[65] Cette règle s'applique également lorsque les données à caractère personnel sont «inadéquates, non pertinentes ou excessives au regard des finalités du traitement, (...) qu'elles ne sont pas mises à jour ou (...) qu'elles sont conservées pendant une durée excédant celle nécessaire, à moins que leur conservation ne s'impose à des fins historiques, statistiques ou scientifiques».[66] Enfin, le responsable du traitement peut être tenu de notifier aux tiers auxquels les données ont été communiquées toute rectification ou tout effacement effectué, si cela ne suppose pas un effort disproportionné.[67]

c) Le droit d'opposition

54. Les personnes physiques ont le droit de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à leur situation particulière, à ce que des données les concernant fassent l'objet d'un traitement.[68] En cas d'opposition justifiée, le traitement de ces données devrait cesser.

55. Les personnes physiques ont également le droit de ne pas être soumises à «une décision produisant des effets juridiques à leur égard ou les affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de leur personnalité, tels que leur rendement professionnel, leur crédit, leur fiabilité, leur comportement, etc.».[69]

---

[64] Articles 41, 47 et 48 de la Charte des droits fondamentaux. Le droit d'une personne physique («personne concernée») d'accéder aux données collectées la concernant est consacré à l'article 8, paragraphe 2, de la Charte. Ce droit est précisé plus en détail à l'article 12, point a), de la directive 95/46/CE, à l'article 13 du règlement 45/2001 et à l'article 17 de la décision-cadre 2008/977/JAI. L'article 13 du règlement 45/2001 précise que: «la personne concernée a le droit d'obtenir, sans contrainte, à tout moment dans un délai de trois mois à partir de la réception de la demande d'information et gratuitement, du responsable du traitement (...)». La CJUE a considéré que le droit d'accès «doit nécessairement concerner le passé. En effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière efficace son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi». Affaire C-553/07, *College van burgemeester en wethouders van Rotterdam contre M.E.E. Rijkeboer*, arrêt de la CJUE du 7 mai 2009, point 54.

[65] Article 12, point b), de la directive 95/46/CE, articles 14 à 16 du règlement 45/2001 et article 17 de la décision-cadre 2008/977/JAI.

[66] Affaire C-131/12, *Google Spain*, point 92. En vertu de l'article 6, paragraphe 1, points c) à e), de la directive 95/46/CE et de l'article 4, paragraphe 1, points c) à e), il incombe au responsable du traitement de veiller à la qualité des données traitées, indépendamment de toute action engagée par les personnes physiques concernées.

[67] Article 12, point c), de la directive 95/46/CE.

[68] Article 14 de la directive 95/46/CE et article 18 du règlement 45/2001.

[69] Article 15 de la directive 95/46/CE, article 19 du règlement 45/2001 et article 7 de la décision-cadre 2008/977/JAI. Il peut être dérogé à ce droit si la décision a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime; ou b) est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

d) La limitation des droits des personnes concernées

56. La limitation des droits des personnes concernées peut être justifiée par des objectifs d'intérêt général, et notamment la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées, un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal, ainsi qu'une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique.[70] En cas de limitation des droits, il pourrait être nécessaire que la mesure prévoie des garanties supplémentaires, telles que la durée et les circonstances dans lesquelles la limitation s'appliquerait.[71]

57. Ces limitations doivent être exceptionnelles et respecter les conditions visées à l'article 52, paragraphe 1, de la Charte. La mesure limitant les droits doit cesser de s'appliquer dès qu'elle n'est plus nécessaire. En ce qui concerne la proposition de révision de la directive relative à la lutte contre le blanchiment de capitaux, le CEPD a recommandé, d'une part, que la mesure prévoie un délai au terme duquel la limitation du droit d'accès cesserait de s'appliquer, et, d'autre part, que cette limitation ne concerne pas les cas qui sont ensuite considérés comme non fondés ou non pertinents.[72]

Recommandation

58. Les mesures qui, à la lumière de ces étapes analytiques, semblent particulièrement intrusives, devraient prévoir, de la façon la plus explicite possible, des garanties permettant de s'assurer que les personnes physiques dont les données à caractère personnel doivent être traitées peuvent exercer leurs droits. Toute limitation de ces droits devrait être explicitement prévue et motivée dans la mesure et être limitée dans le temps, conformément à l'article 52, paragraphe 1, de la Charte.

9) Envisager des mesures appropriées en matière de sécurité des données

59. La réglementation des services financiers s'appuie sur des bases de données importantes et des systèmes informatiques complexes exploités par des établissements financiers ou des autorités réglementaires. Conformément aux règles européennes en matière de protection des données, les responsables du traitement doivent mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Cela implique la nécessité, pour le responsable du traitement, d'identifier, d'évaluer, de prioriser et de traiter les risques de sécurité de manière appropriée en fonction du traitement concerné. Le traitement de données sensibles, en particulier, exige un niveau de sécurité plus élevé.

[70] Article 13 de la directive 95/46/CE et article 20 du règlement 45/2001.

[71] En vertu de l'article 20 du règlement 45/2001, la personne concernée devrait être informée des principales raisons qui motivent la limitation ainsi que de son droit de saisir le contrôleur européen de la protection des données. La personne concernée a également le droit d'accéder indirectement à ses données par l'intermédiaire du CEPD, qui lui fait savoir si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées. Voir les lignes directrices du CEPD sur les droits des personnes physiques à l'égard du traitement des données à caractère personnel, 25 février 2014, p. 26 à 34. Voir, par exemple, l'avis du CEPD sur la lutte contre le blanchiment de capitaux, p. 15 et 16.

[72] Voir l'avis du CEPD sur la lutte contre le blanchiment de capitaux, p. 15 et 16.

60. Des mesures techniques et organisationnelles appropriées pour la gestion des risques identifiés pourraient se traduire par des missions visant à renforcer la conformité globale de la mesure avec les règles de protection des données. Ces mesures permettraient de faciliter le droit des personnes physiques d'accéder aux données, de les vérifier et de s'assurer de leur qualité, ainsi que de garantir des traces d'audit pour l'accès aux données, les transferts, la modification ou la suppression des données au terme de la période de conservation. Des mesures spécifiques pourraient notamment comprendre:

- le cryptage aux fins de la confidentialité et de l'intégrité des données;
- des connexions sécurisées et des mesures destinées à définir et à protéger des périmètres de sécurité logiques, tels que des pare-feux ou des systèmes de prévention et de détection des intrusions;
- la prévention de l'accès physique non autorisé aux infrastructures informatiques et aux locaux sécurisés;
- des procédures d'autorisation et d'authentification des systèmes informatiques;
- la sélection des employés et la séparation des tâches; et
- des mesures organisationnelles destinées à garantir une réaction appropriée aux incidents de sécurité, notamment les violations de données à caractère personnel.[73]

61. La proposition de règlement général sur la protection des données de la Commission introduit la notion de *respect de la vie privée dès la conception*, selon laquelle la protection des données et le respect de la vie privée sont intégrés dans les nouveaux produits, services et procédures dès la phase de conception et pendant toute leur durée de vie, et la notion de *respect de la vie privée par défaut*, selon laquelle les paramètres par défaut sont respectueux de la vie privée. Le CEPD peut fournir des conseils pratiques sur la manière d'intégrer ces notions dans des normes appropriées de «niveau 2»[74] pour le traitement de données dans des bases de données, des systèmes d'alerte précoce ou d'autres systèmes informatiques.

Recommandation

62. Les mesures impliquant un traitement de données à l'aide de systèmes informatiques importants devraient être fondées sur une évaluation minutieuse de leur nécessité. Elles devraient prévoir des garanties techniques et organisationnelles appropriées pour la protection de données personnelles, souvent sensibles, ainsi que la consultation du

[73] L'article 4, paragraphe 3, de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques prévoit l'obligation, pour les fournisseurs de services de communications électroniques accessibles au public, de mettre en œuvre des exigences spécifiques en matière de confidentialité et de sécurité. Cette directive les oblige également à signaler les violations de données, et le règlement général relatif à la protection des données prévoit cette même obligation pour tous les responsables du traitement. Ces obligations, qui sont généralement considérées comme de bonnes pratiques, peuvent également être imposées par des instruments sectoriels spécifiques ou en vertu du droit civil général en matière de responsabilité.

[74] Le niveau 2 de «l'approche Lamfalussy» à quatre niveaux, suivie par l'UE concernant la législation relative aux services financiers, se rapporte aux mesures d'exécution adoptées par la Commission sur la base de projets ou de conseils des autorités de supervision financière européennes. Voir http://ec.europa.eu/internal_market/securities/lamfalussy/index_fr.htm (dernier accès le 16 novembre 2014).

CEPD sur le développement de normes techniques par le biais d'actes délégués et d'exécution.

10) Prévoir des procédures spécifiques pour le contrôle des traitements de données

63. Le traitement de données à caractère personnel est contrôlé par les autorités nationales chargées de la protection des données, et en ce qui concerne les institutions et organes de l'UE, tels que les autorités de supervision financière européennes, par le CEPD.[75] Ainsi, en vertu du règlement (CE) nº 1060/2009 sur les agences de notation de crédit, lorsque les autorités compétentes peuvent échanger des informations avec l'Autorité européenne des marchés financiers (l'ESMA), le traitement par les autorités nationales compétentes au niveau national est supervisé par les autorités chargées de la protection des données, tandis que le traitement par l'ESMA est soumis au contrôle du CEPD. Les responsables du traitement doivent informer l'autorité compétente en matière de protection des données de tout traitement susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées avant le début du traitement.[76] Les traitements risqués susceptibles d'exiger un tel «examen préalable» par le CEPD[77], comprennent notamment:

    a) le traitement de données relatives aux soupçons d'infractions, aux infractions, aux condamnations pénales ou aux mesures de sûreté, comme dans les dispositifs d'alerte professionnelle;

    b) les traitements destinés à évaluer certains aspects de la personnalité de la personne concernée, tels que ses compétences, son efficacité et son comportement; et

    c) les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, par exemple dans l'évaluation du crédit des consommateurs.[78]

Recommandation

64. Les mesures qui envisagent des traitements présentant des risques particuliers au regard des droits des personnes physiques devraient spécifier les procédures à suivre pour l'envoi de notifications aux autorités compétentes en matière de protection des données en vue d'un contrôle préalable des traitements de données à caractère personnel.

4. Appliquer la méthodologie aux mesures prises dans le cadre de la réglementation des services financiers

Cette section applique, à titre d'illustration, la méthodologie en 10 étapes susmentionnée à trois dispositions types contenues dans des instruments récemment adoptés dans le domaine de la réglementation des services financiers, et ayant une incidence sur les droits au respect de la vie privée et à la protection des données à caractère personnel:

a. la transparence et la publication des sanctions;

[75] Article 28 de la directive 95/46/CE et article 41 du règlement 45/2001.
[76] Article 20 de la directive 95/46/CE et article 27 du règlement 45/2001.
[77] Article 27, paragraphe 2, du règlement 45/2001.
[78] Voir l'avis du CEPD sur les contrats de crédit relatifs aux biens immobiliers à usage résidentiel, 25 juillet 2011.

b. les dispositifs d'alerte professionnelle; et

c. l'enregistrement de télécommunications et les pouvoirs de demander des données téléphoniques et de trafic.

Les mesures de transparence et la publication des sanctions

1ère étape: Identifier les données à caractère personnel à traiter

Plusieurs mesures, telles que la directive 2014/65/UE relative aux marchés d'instruments financiers et la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, envisagent la publication des sanctions pour violation de la réglementation des services financiers, y compris l'identification de la personne à l'origine de l'infraction. Le contrôle des activités des entreprises pour veiller à l'intégrité du marché est également susceptible de donner lieu à des obligations de déclaration. Les entreprises peuvent ainsi être tenues de communiquer des données à caractère personnel relatives à leurs salariés et/ou à leurs clients.

2e étape: Déterminer si le traitement de données constitue une ingérence dans le droit au respect de la vie privée

La publication des noms des personnes soupçonnées d'avoir enfreint les règles constitue une ingérence dans leur droit au respect de la vie privée. Cette ingérence pourrait être minimisée de plusieurs façons:

a) Elle ne devrait pas être automatique et devrait être évitée si la finalité peut être réalisée par des moyens moins intrusifs. L'autorité devrait être en mesure d'exercer son pouvoir discrétionnaire au cas par cas, afin d'éviter la publication en cas de violations moins graves, lorsque la violation n'a pas causé de préjudice considérable ou lorsque la partie s'est montrée coopérative. La publication devrait être justifiée par la gravité de l'infraction et les pertes causées à des tiers, le degré de responsabilité de la personne en cause et les infractions commises précédemment, ainsi que toutes autres circonstances particulières.[79]

b) Toute publication devrait être retardée jusqu'à ce que la dernière instance d'une procédure judiciaire soit épuisée, et elle ne devrait jamais avoir lieu dans des situations où la décision fait l'objet d'un recours ou est finalement annulée par un tribunal.[80]

c) Avant la publication de la décision, l'entreprise concernée devrait être invitée à indiquer quelles informations devraient être considérées comme confidentielles et ne devraient donc pas être publiées.

d) Les noms des personnes physiques (salariés ou autres) devraient être supprimés des décisions publiées, et les fonctions des personnes physiques qui sont mentionnées dans ces décisions ou d'autres documents devraient être supprimées et remplacées par des fonctions plus générales (par ex. «directeur»).

[79] Avis du CEPD sur les opérations d'initiés et les manipulations de marché, 10 février 2012, point 45; avis du CEPD sur l'activité des établissements de crédit et la surveillance prudentielle, 10 février 2012, point 21; avis du CEPD sur les agences de notation de crédit, 10 février 2012, point 47.

[80] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 61.

3e étape: Définir la finalité du traitement de données

La transparence vise à éviter de futures infractions et à informer les opérateurs de marché des éventuelles infractions commises. Bien que l'objectif de transparence ait une incidence sur le droit au respect de la vie privée et qu'il doive tenir compte des exigences fixées par la CJUE,[81] il peut être légitimement poursuivi à condition que les exigences de confidentialité soient respectées.

4e étape: Établir une base juridique pour le traitement de données

Une base juridique appropriée pour la publication serait l'exécution d'une mission d'intérêt public ou le respect d'une obligation légale imposée au responsable du traitement, plutôt que le consentement de la personne concernée.

5e étape: Évaluer et justifier une période de conservation appropriée

Les données à caractère personnel devraient être conservées par l'entreprise et/ou l'autorité de contrôle pendant une durée n'excédant pas celle nécessaire et être rendues anonymes dès qu'elles ne sont plus pertinentes pour l'application du règlement de l'UE en question. Étant donné que, dans la plupart des cas, la publication sera effectuée sur l'internet, les États membres devraient être obligés de s'assurer que les données à caractère personnel sont maintenues en ligne pendant une période raisonnable à l'issue de laquelle elles devraient être systématiquement effacées.[82]

6e étape: Identifier les parties au sein de l'UE qui peuvent avoir accès aux données à caractère personnel

Les personnes physiques ne devraient être autorisées à accéder aux données à caractère personnel que sur la base du besoin d'en connaître, et elles ne devraient traiter les données que sur instruction du responsable du traitement.

Des mesures techniques et organisationnelles appropriées doivent être mises en place pour protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération et la communication non autorisée, par exemple en sensibilisant les salariés. Lorsque l'accès sur demande de tiers, tels que des autorités répressives, est envisagé, il convient de préciser quelles autorités peuvent traiter ultérieurement les données à caractère personnel et pour quelle finalité celles-ci peuvent être traitées.

7e étape: Établir une base juridique adéquate pour tout transfert de données à caractère personnel en dehors de l'UE

La coopération entre les autorités compétentes de l'UE et celles de pays tiers implique généralement l'échange de données relatives au commerce transfrontalier et aux sociétés mères d'un État membre qui possèdent une filiale dans un autre État membre.

Lorsque cet échange implique un transfert de données à caractère personnel vers un pays tiers dont la Commission estime qu'il n'assure pas un niveau de protection adéquat, un motif d'intérêt public reconnu dans le droit national pourrait être approprié. Les transferts ne devraient pas être effectués automatiquement, mais basés sur une évaluation au cas par cas de

[81] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers**,** point 51; affaires conjointes C-92/09 et C-93/09, *Schecke*, points 56 à 64.

[82] Avis du CEPD sur les opérations d'initiés et les manipulations de marché, points 49 et 50*;* avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 64.

la nécessité et du caractère proportionné du transfert. Des conditions devraient être appliquées à tout transfert ultérieur vers un autre pays tiers, comme le fait d'exiger l'autorisation écrite expresse de l'autorité de l'État membre.[83]

8e étape: Prévoir des garanties appropriées pour l'exercice des droits des personnes physiques en matière de protection des données

Les autorités compétentes devraient prendre l'initiative d'informer les personnes concernées avant la publication de toute décision de sanction prise à leur encontre, et confirmer leur droit de s'opposer pour des raisons prépondérantes et légitimes.[84]

9e étape: Envisager des mesures appropriées en matière de sécurité des données

Toute mesure visant à renforcer la transparence devrait prévoir l'obligation, pour le personnel des autorités compétentes, d'être tenu au secret professionnel, et devrait interdire la divulgation d'informations confidentielles.[85]

Les dispositifs d'alerte professionnelle

1ère étape: Identifier les données à caractère personnel à traiter

Les procédures mises en place pour le signalement d'infractions ou la dénonciation d'irrégularités ont une incidence sur la protection des données à caractère personnel du dénonciateur et de la personne accusée d'avoir commis un acte répréhensible.[86] Les personnes responsables des dispositifs d'alerte professionnelle devraient évaluer attentivement s'il peut être proportionné et approprié de limiter le nombre de personnes autorisées à dénoncer les fautes présumées, les catégories de personnes susceptibles d'être incriminées et les infractions pour lesquelles elles peuvent être mises en cause.

2e étape: Déterminer si le traitement de données constitue une ingérence dans le droit au respect de la vie privée

La confidentialité de l'identité des dénonciateurs devrait être garantie à tous les stades de la procédure, à moins que sa communication ne soit requise par le droit national dans le contexte d'enquêtes ou de procédures judiciaires ultérieures.[87]

5e étape: Évaluer et justifier une période de conservation appropriée

Les délais de conservation des données à caractère personnel collectées dans le cadre de l'enquête sur un rapport devraient être limités au minimum. En principe, il ne devrait pas être nécessaire de conserver les données pendant plus de deux mois après la clôture de l'enquête,

[83] Avis du CEPD concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, p. 14 à 16. Un exemple de cette disposition est fourni par l'article 29 du règlement sur les abus de marché.

[84] Article 14 de la directive 95/46/CE. Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 62; avis du CEPD sur les opérations d'initiés et les manipulations de marché, point 48.

[85] Avis du CEPD concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, points 17 et 18.

[86] Avis 1/2006 du Groupe de travail «Article 29» relatif à l'application des règles européennes de protection des données aux dispositifs internes d'alerte professionnelle («whistleblowing») dans les domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières.

[87] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 67; avis du CEPD sur les propositions relatives aux opérations d'initiés et les manipulations de marché, point 54; lignes directrices du CEPD sur les droits des personnes physiques à l'égard du traitement des données à caractère personnel, p. 32.

à moins que des procédures légales ou des mesures disciplinaires ne soient engagées contre la personne mise en cause ou, en cas de déclaration fausse ou diffamatoire, le dénonciateur.

8e étape: Prévoir des garanties appropriées pour l'exercice des droits des personnes physiques en matière de protection des données

Les personnes accusées d'avoir commis un acte répréhensible doivent pouvoir bénéficier des droits de la défense, du droit d'être entendues avant l'adoption d'une décision les concernant, ainsi que du droit d'introduire un recours juridictionnel effectif contre toute mesure ou décision rendue à leur égard.[88] Les dénonciateurs devraient être encouragés à présenter des rapports identifiés et confidentiels plutôt que des rapports anonymes, et les personnes responsables du dispositif devraient communiquer l'identité des dénonciateurs lorsque l'accusation s'avère malveillante.[89]

10e étape: Prévoir des procédures spécifiques pour le contrôle du traitement de données

Tout dispositif d'alerte professionnelle implique le traitement de données à caractère personnel concernant les soupçons d'infractions et, de ce fait, présente des risques particuliers pour la personne signalant les actes répréhensibles présumés comme pour l'accusé. Le dispositif devrait donc être notifié à l'autorité compétente en matière de protection des données en vue d'un contrôle préalable.

L'enregistrement de télécommunications et les pouvoirs de demander des données téléphoniques et de trafic

1ère étape: Identifier les données à caractère personnel à traiter

Les catégories de données relatives aux communications à traiter devraient être clairement définies.[90] Les «données relatives au trafic» sont définies dans le droit de l'UE comme «toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation».[91] Ces données comprennent généralement des données à caractère personnel, comme l'identité des personnes émettant et recevant l'appel, l'heure et la durée de l'appel, le réseau utilisé et, dans le cas d'appareils portables, la situation géographique de l'utilisateur. Certaines données relatives au trafic pour l'utilisation de l'internet et des communications électroniques (la liste des sites visités, par exemple) peuvent en outre révéler des détails importants du contenu de la communication.[92] En ce qui concerne les données relatives aux communications, il convient d'établir une distinction claire entre les «données relatives au trafic» et les données relatives au contenu de la communication (la «conversation»).

2e étape: Déterminer si le traitement de données constitue une ingérence dans le droit au respect de la vie privée

Les entreprises du secteur des services financiers enregistrent souvent le contenu des conversations concernant les transactions.[93] Même lorsque les conversations en cause portent

[88] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 68.
[89] Voir les lignes directrices du CEPD sur les droits des personnes physiques à l'égard du traitement des données à caractère personnel, p. 32.
[90] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 34.
[91] Directive 2002/58/CE, article 2.
[92] Avis du CEPD sur les propositions relatives aux opérations d'initiés et les manipulations de marché, point 24. Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 44.
[93] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 20.

entièrement ou essentiellement sur des transactions financières ou des activités professionnelles, les enregistrements de ces communications comprennent des données à caractère personnel, et l'accès à ces données par les autorités compétentes constitue une ingérence significative dans le droit au respect de la vie privée. À moins que cela ne soit strictement nécessaire, la mesure devrait explicitement exclure l'accès par les autorités compétentes au contenu des communications.[94] L'accès aux données relatives aux communications par l'autorité compétente devrait être conditionné à l'obtention d'une autorisation judiciaire préalable, dans l'intérêt d'une application harmonisée de la législation de l'UE dans tous les État membres.[95]

3e étape: Définir la finalité du traitement de données

Les informations sur les communications téléphoniques et électroniques impliquant des salariés d'une entreprise peuvent être utiles pour la conduite d'enquêtes sur les actes répréhensibles ou les manquements aux obligations d'une entreprise. Toute mesure permettant l'accès à ces données devrait définir précisément la finalité de ce traitement, conformément à l'article 6, paragraphe 1, de la directive relative à la protection des données.[96] Les pouvoirs de demander des données relatives au trafic devraient être clairement définis et limités aux cas où il existe un soupçon raisonnable que de tels enregistrements sont susceptibles de démontrer un manquement aux obligations de l'entreprise.

5e étape: Évaluer et justifier une période de conservation appropriée

La mesure devrait stipuler un délai maximal approprié pour la conservation des données, qui soit applicable aussi bien aux entreprises qu'aux autorités compétentes en charge de la surveillance du marché financier/de l'activité en question.[97]

8e étape: Prévoir des garanties appropriées pour l'exercice des droits des personnes physiques en matière de protection des données

La mesure devrait prévoir le droit du destinataire de faire réexaminer par les tribunaux la décision relative à l'accès aux données de communications rendue par l'autorité compétente.[98] La mesure devrait veiller à ce que la personne concernée soit informée du droit de rectifier les données la concernant et du droit de saisir le CEPD.[99]

5. Travailler avec le CEPD

65. Conformément à l'article 28, paragraphe 2, du règlement 45/2001, la Commission est tenue de consulter le CEPD lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

[94] Avis du CEPD sur les opérations d'initiés et les manipulations de marché, points 25, 32 et 34. Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 32.
[95] Avis du CEPD sur les opérations d'initiés et les manipulations de marché, point 27; avis du CEPD sur les agences de notation de crédit, point 18.
[96] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 28.
[97] Avis du CEPD sur les propositions relatives aux marchés d'instruments financiers, point 38.
[98] Avis du CEPD sur les opérations d'initiés et les manipulations de marché, point 28.
[99] Avis du CEPD sur une notification en vue d'un contrôle préalable reçue du délégué à la protection des données de la Banque centrale européenne concernant l'enregistrement, le stockage et l'écoute des conversations téléphoniques au sein de la DG-M et de la DG-P, Bruxelles, 5 mai 2006 (affaire 2005-376), p. 11 à 13.

66. Dans la pratique, le CEPD a décidé d'intervenir en amont en donnant des conseils à toutes les étapes de l'élaboration des politiques et de la procédure législative, non seulement à la Commission, mais aussi au Parlement et au Conseil.[100] En outre, à la suite de discussions avec la Commission, il a été convenu et stipulé dans une note du Secrétaire général de décembre 2006, que les services de la Commission devraient consulter le CEPD de manière informelle avant l'adoption d'une proposition ayant une incidence sur la protection des données, et que, lorsque la Commission est elle-même le législateur (directives ou règlements de la Commission, décisions de «comitologie» ou autres, mandat de négociation…) ou pour des documents non législatifs, une consultation formelle devrait avoir lieu avant l'adoption de l'acte par le Collège, sans préjudice d'une consultation informelle au cours de la phase de préparation. Le CEPD souhaite poursuivre et élargir ce dispositif.

67. De plus en plus fréquemment, les mesures d'exécution et les actes délégués sont élaborés par les autorités de supervision financière de l'UE, le plus souvent après une consultation publique, puis soumis à la Commission qui, de fait, dispose d'une marge de manœuvre limitée pour modifier les projets qui lui sont soumis. Le CEPD se réserve le droit de formuler des commentaires sur ces projets par le biais d'un avis public, mais il serait plus approprié, dans la plupart des cas, de transmettre les commentaires directement à la Commission, de manière informelle avant l'adoption de l'instrument, et de manière formelle après celle-ci. Pour que ces conseils soient utiles, la Commission devrait accorder au CEPD un délai raisonnable pour examiner les documents.

68. Le CEPD vous invite à lui faire part de vos remarques concernant les présentes lignes directrices, dont il entend examiner l'efficacité et la pertinence d'ici 2019 au plus tard.

Bruxelles, le 26 novembre 2014

[100] Voir la section 3.2 du document stratégique du CEPD.

Annexe: Les avis du CEPD dans le contexte de la réglementation des services financiers de l'UE

(Sur la création de la base de données du système d'alerte précoce) Avis du CEPD sur la proposition modifiée de règlement du Conseil modifiant le règlement (CE, Euratom) nº 1605/2002 portant règlement financier applicable au budget général des Communautés européennes (COM(2006) 213 final) et sur la proposition de règlement (CE, Euratom) de la Commission modifiant le règlement (CE, Euratom) nº 2342/2002 établissant les modalités d'exécution du règlement (CE, Euratom) nº 1605/2002 du Conseil portant règlement financier applicable au budget général des Communautés européennes, adopté le 12 décembre 2006, JO C 94, 28 avril 2007.

Avis du CEPD sur le Livre vert de la Commission intitulé «Exécution effective des décisions judiciaires dans l'Union européenne: la transparence du patrimoine des débiteurs», adopté le 22 septembre 2008, JO C 20, 27 janvier 2009.

Avis du CEPD sur la proposition de directive du Parlement européen et du Conseil relative aux systèmes de garantie des dépôts (refonte), adopté le 9 septembre 2010, JO C 323, 30 novembre 2010.

Avis du CEPD sur la proposition de règlement du Parlement européen et du Conseil sur les produits dérivés négociés de gré à gré, les contreparties centrales et les référentiels centraux, adopté le 19 avril 2011, JO C 216/04, 22 juillet 2011.

Avis du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des exigences techniques pour les virements et les prélèvements en euros et modifiant le règlement (CE) nº 924/2009, adopté le 23 juin 2011, JO C 284/01, 28 septembre 2011.

(Sur la consultation de bases de données nationales sur le crédit afin d'évaluer la solvabilité des consommateurs) Avis du CEPD sur la proposition de directive du Parlement européen et du Conseil concernant les contrats de crédit relatifs aux biens immobiliers à usage résidentiel, adopté le 25 juillet 2011, JO C 377/02, 23 décembre 2011.

Avis du CEPD sur une proposition de règlement du Parlement européen et du Conseil portant création d'une ordonnance européenne de saisie conservatoire des comptes bancaires, destinée à faciliter le recouvrement transfrontalier de créances en matière civile et commerciale, adopté le 13 octobre 2011, JO C 373/03, 21 décembre 2011.

Avis du CEPD sur les propositions de la Commission relatives à une directive du Parlement européen et du Conseil concernant les marchés d'instruments financiers abrogeant la directive 2004/39/CE du Parlement européen et du Conseil et à un règlement du Parlement européen et du Conseil concernant les marchés d'instruments financiers modifiant le règlement sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux, adopté le 10 février 2012, JO C 147, 25 mai 2012.

Avis du CEPD sur les propositions de la Commission de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché, et de directive du Parlement européen et du Conseil relative aux sanctions pénales applicables aux opérations d'initiés et aux manipulations de marché, adopté le 10 février 2012, JO C 177, 20 juin 2012.

Avis du CEPD sur les propositions de la Commission concernant une directive concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, et un règlement concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement, adopté le 10 février 2012, JO C 175, 19 juin 2012.

Avis du CEPD sur la proposition de la Commission de règlement du Parlement européen et du Conseil modifiant le règlement (CE) nº 1060/2009 sur les agences de notation de crédit, adopté le 10 février 2012, JO C 139/02, 15 mai 2012.

Avis du CEPD relatif à la proposition de règlement sur les fonds européens de capital-risque et à la proposition de règlement sur les fonds d'entrepreneuriat social européens, adopté le 14 juin 2012, JO C 335, 1er novembre 2012.

Avis du CEPD sur une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et une proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les virements de fonds, adopté le 4 juillet 2013, JO C 32, 4 février 2014.

Avis du CEPD sur la proposition de la Commission de règlement du Parlement européen et du Conseil concernant l'amélioration du règlement des opérations sur titres dans l'Union européenne et les dépositaires centraux de titres (DCT) et modifiant la directive 98/26/CE, adopté le 9 juillet 2012, JO C 336, 6 novembre 2012.

Avis du CEPD sur une proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2006/48/CE et 2009/110/CE et abrogeant la directive 2007/64/CE, ainsi qu'une proposition de règlement du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, adopté le 5 décembre 2013, JO C 38, 8 février 2014.