Avis du Contrôleur européen de la protection des données

sur le paquet de mesures de la Commission européenne relatif à l'ouverture des données, qui comprend une proposition de directive modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public (ISP), une communication sur l'ouverture des données et la décision 2011/833/UE de la Commission sur la réutilisation des documents de la Commission

LE CONTROLEUR EUROPEEN DE LA PROTECTION DES DONNEES,

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

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

vu 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[1],

vu le règlement (CE) n° 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[2], et notamment son article 41, paragraphe 2,

A ADOPTE LE PRESENT AVIS:

1. INTRODUCTION

1.1. Contexte

1. Le 12 décembre 2011, la Commission a adopté une proposition de directive modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public (ISP) (ci-après la «proposition»)[3]. La proposition fait partie du paquet de mesures relatif à l'ouverture des données, qui comprend également deux autres documents adoptés le même jour: i) une communication de la Commission intitulée «L'ouverture des données publiques: un moteur pour l'innovation, la croissance et une gouvernance

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.01.2001, p. 1.
[3] COM(2011) 877 final.

Adresse postale: rue Wiertz 60 - B-1047 Brussels
Bureaux: rue Montoyer 63
Courrier électronique: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

transparente» (ci-après la «communication»)[4] et ii) une décision de la Commission sur la réutilisation des documents de la Commission (ci-après la «décision»)[5].

2. Contrairement à ce que prévoit l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, le CEPD n'a pas été consulté. Cela est d'autant plus regrettable que le volume de données à caractère personnel potentiellement concerné est important. Le présent avis est par conséquent basé sur l'article 41, paragraphe 2, dudit règlement. Le CEPD recommande de faire référence au présent avis dans le préambule de l'instrument adopté.

1.2. Objectifs et champ d'application de la proposition et de la décision; thèmes centraux de l'avis du CEPD

3. L'objectif de la proposition est d'actualiser et de modifier le texte existant de la directive 2003/98/CE sur la réutilisation des informations du secteur public (ci-après la «directive ISP»).

4. La directive ISP vise à faciliter la réutilisation des informations du secteur public dans toute l'Union européenne en harmonisant les conditions fondamentales relatives à leur réutilisation et en éliminant les obstacles qui s'y opposent dans le marché intérieur. La directive ISP contient des dispositions relatives à la non-discrimination, à la tarification, aux accords d'exclusivité, à la transparence, aux licences et à des outils pratiques permettant de retrouver et de réutiliser facilement les documents publics[6].

5. Un des principaux objectifs politiques novateurs de la proposition, tels que décrit à la section 5.1 de la Communication, est d'introduire «le principe selon lequel toutes les informations publiques qui ne sont pas explicitement couvertes par une des exceptions sont réutilisables à des fins commerciales ou non commerciales»[7]. En particulier, la modification proposée de l'article 3, paragraphe 1, de la directive ISP fait expressément obligation aux États membres de veiller à ce que les «documents existants» soient «réutilisables à des fins commerciales et non commerciales».

6. D'autres nouvelles dispositions pertinentes de la proposition comprennent, sous réserve de certaines exceptions, la limitation des redevances exigées par le secteur public aux «coûts marginaux de reproduction et de diffusion» (article 6, paragraphe 1, révisé). Par ailleurs, la proposition étend également le champ d'application de la directive ISP aux bibliothèques, archives, musées et bibliothèques universitaires.

7. L'objectif de la décision est d'établir les règles applicables à la Commission pour la réutilisation de ses propres documents.

8. Le présent avis se concentre, aux sections 2 et 3, sur la proposition en tant que telle, tandis que la section 4 commente brièvement la décision. La section 2 donne une vue d'ensemble des problèmes posés par l'ouverture des données au regard de leur

[4] COM(2011) 882 final.
[5] 2011/833/UE.
[6] Voir l'exposé des motifs de la proposition, section 1.
[7] Voir aussi la section 3.2, paragraphe 6, de l'exposé des motifs de la proposition qui recommande des mesures au niveau de l'Union pour «garantir» que «la réutilisation sera autorisée dans tous les États membres pour des données du secteur public fondamentales d'importance primordiale», et la section 5, option «Modifications législatives», point iii), du résumé de l'analyse d'impact, qui appelle à «modifier le principe général pour rendre réutilisables tous les documents accessibles».

protection et aborde les défis et les considérations qui servent de points de référence importants et déterminent, dans une large mesure, l'approche adoptée par le CEPD dans les recommandations plus spécifiques qu'il formule à la section 3.

2. OBSERVATIONS GENERALES

2.1. Application de la législation relative à la protection des données

9. À titre préliminaire, le CEPD souligne que, bien que de nombreuses informations du secteur public ne contiennent aucune donnée à caractère personnel, le secteur public détient également un grand volume de données à caractère personnel dont la nature et le caractère sensible peuvent varier – par exemple, les informations sur les administrateurs et d'autres représentants de sociétés enregistrées dans un registre du commerce, les informations sur les salaires des fonctionnaires ou les dépenses des parlementaires et les dossiers médicaux détenus par un service national de santé.

10. Dans ce contexte, il importe de noter que toute information liée à une personne physique identifiée ou identifiable, qu'elle soit publiquement disponible ou non, constitue une donnée à caractère personnel. En outre, le seul fait que ces données ont été mises à la disposition du public n'entraîne pas de dérogation à la législation relative à la protection des données. La réutilisation de données à caractère personnel publiées par le secteur public reste donc soumise en principe à la législation applicable à la protection des données[8].

11. Comme exposé de manière plus détaillée à la section 3.1, la directive IPS, telle qu'elle est proposée, ne précise pas clairement si elle s'applique aussi aux données à caractère personnel et, si tel est le cas, dans quelle mesure et sous quelles conditions.

2.2. Principaux problèmes liés à la protection des données

12. L'établissement d'un principe de réutilisation de toutes les informations du secteur public est susceptible de rendre ces informations beaucoup plus facilement accessibles. Il peut offrir des avantages potentiels, comme une plus grande transparence et une réutilisation innovante des informations du secteur public, et notamment de certaines catégories de données à caractère personnel.

13. Toutefois, une plus grande accessibilité des informations peut également accroître les risques d'usage abusif des données à caractère personnel. Ces risques s'appliquent même si les données à caractère personnel concernées ont déjà été rendues publiques (ou si elles peuvent l'être) en vertu des «règles d'accès» de l'État membre concerné. Tant que des garanties adéquates ne seront pas mises en place et appliquées de manière cohérente et efficace, les informations mises à disposition en vue de leur réutilisation sont susceptibles d'être recueillies illégalement (en Europe et ailleurs)[9], combinées à d'autres informations, vendues et au final utilisées à des fins qui i) n'étaient pas prévues initialement, ii) peuvent être disproportionnées et iii) peuvent être dénuées

[8] Voir l'arrêt de la Cour de justice de l'Union européenne du 16 décembre 2008 dans l'affaire C-73/07, *Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy en Satamedia Oy*, points 38-49. Voir aussi l'avis 7/2003 du groupe de travail «Article 29», section II.2, point 3, cité in extenso à la note de bas de page 11 ci-dessous.

[9] Sur les réutilisations et transferts internationaux des ISP par des organisations situées dans des pays tiers, voir la section 3.4 ci-dessous.

d'une base juridique adéquate. Parmi les menaces pour la vie privée figurent également des activités criminelles telles que l'usurpation d'identité.

14. Ces risques ne sont pas entièrement nouveaux et concernent de nombreux projets à grande échelle, dans le cadre desquels de nombreuses données à caractère personnel, précédemment enregistrées sous format papier dans les bureaux de collectivités locales, sont publiées sur l'internet sous une forme numérique[10].

15. En revanche, les projets d'ouverture des données hissent l'accessibilité des informations à un tout autre niveau. En effet, bon nombre de ces projets supposent i) de rendre accessibles des bases de données entières ii) sous une forme électronique normalisée iii) à toute personne qui en fait la demande sans procédure d'examen iv) et gratuitement, v) et ce pour toute finalité commerciale ou non commerciale en vertu d'une licence ouverte. Cette nouvelle forme d'accessibilité constitue le principal objectif de l'ouverture des données, mais elle n'est pas dépourvue de risques si elle est appliquée sans discernement et sans garanties appropriées. À titre d'illustration, un portail conventionnel d'administration en ligne permettant l'accès du public à des données à caractère personnel particulières d'un registre du commerce peut, s'il est correctement configuré et si des mesures adéquates de sécurité sont mises en place, poser de grandes difficultés à toute tierce partie cherchant à collecter (et donc à utiliser ultérieurement) le contenu de la base de données toute entière. En ouvrant tout simplement la totalité de la base de données à toute partie intéressée en vue de sa réutilisation, l'accessibilité et les risques qu'elle comporte augmentent de manière exponentielle.

2.3. Réutilisation des ISP en vertu du cadre actuel de la protection des données

16. Pour remédier aux problèmes liés à la protection des données, la directive ISP fait référence au cadre général de la protection des données:

    - le considérant 21 énonce que la directive ISP «devrait être mise en œuvre et appliquée dans le respect total des principes relatifs à la protection des données à caractère personnel» et
    - l'article 1er, paragraphe 4, dispose que la directive ISP «laisse intact et n'affecte en rien le niveau de protection des personnes à l'égard du traitement des données à caractère personnel».

17. Toutefois, ni la directive ISP existante, ni la proposition ne prévoient de dispositions spécifiques en matière de protection des données afin de remédier au fait qu'elles rendent obligatoire la réutilisation d'un large volume d'informations du secteur public et qu'elles peuvent avoir d'importantes conséquences pour la protection des données.

18. À cet égard, le groupe de travail «Article 29» sur la protection des données (ci-après «le groupe de travail ''Article 29''») a émis de nouvelles lignes directrices en 2003 concernant l'application du cadre actuel de la protection des données à la réutilisation des ISP lorsque celles-ci comprennent des données à caractère personnel[11]. L'avis du

[10] Voir, par exemple, l'avis du CEPD sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 89/666/CEE, 2005/56/CE et 2009/101/CE en ce qui concerne l'interconnexion des registres centraux, du commerce et des sociétés (JO C 220 du 26.7.2011, p. 1), section III.1.

[11] Voir l'avis 7/2003 du groupe de travail «Article 29» sur la protection des données concernant la réutilisation des informations émanant du secteur public et la protection des données à caractère personnel – Trouver le juste milieu, adopté le 12 décembre 2003 (GT 83). Voir également deux autres avis connexes du groupe de travail

groupe de travail «Article 29» s'est focalisé sur le principe de limitation des finalités[12], tout en abordant d'autres questions telles que la légitimité (base juridique) de la divulgation publique et de la réutilisation des ISP, la protection spéciale accordée aux données sensibles, les transferts vers les pays tiers, la qualité des données et les droits des personnes concernées.

19. L'avis du groupe de travail «Article 29» montre que l'application du cadre juridique actuel de la protection des données à la réutilisation des ISP soulève une série de problèmes.

20. En particulier, il n'est pas aisé d'appliquer effectivement le principe de limitation des finalités dans le cas de la réutilisation des ISP. D'un côté, l'idée même et le moteur de l'innovation qui sous-tendent le concept d'«ouverture des données» et la réutilisation des ISP tiennent à ce que les informations doivent être disponibles afin d'être réutilisées pour des produits et services novateurs, et donc pour des finalités qui n'ont pas été définies au préalable et qui ne peuvent être prévues clairement. De l'autre, la limitation des finalités est un principe clé de la protection des données, qui exige que les données à caractère personnel collectées pour une finalité particulière ne peuvent être utilisées ultérieurement pour une autre finalité incompatible si certaines conditions supplémentaires ne sont pas remplies[13]. Il n'est pas facile de concilier ces deux préoccupations (ouverture et protection des données).

21. La difficulté consiste à définir clairement à l'avance les données à caractère personnel pouvant être rendues publiques ainsi que les garanties appropriées en matière de protection des données qui assurent la sécurité juridique tout en permettant l'innovation et la réutilisation pour n'importe quelle finalité (licite).

22. La proportionnalité est un autre principe clé prévu par la directive 95/46/CE[14]. Il existe plusieurs méthodes, modalités et degrés de détail différents pour rendre les données à caractère personnel publiquement disponibles. Certains d'entre eux peuvent être plus intrusifs que d'autres et présenter davantage de risques. Par conséquent, certains seront considérés comme proportionnés, tandis que d'autres non[15]. Un autre défi de taille consiste donc à garantir la proportionnalité tout en permettant une certaine flexibilité.

23. Dans un contexte similaire – à savoir, celui de l'équilibre entre le droit à la protection des données à caractère personnel et le droit d'accès du public aux documents –, le CEPD a recommandé aux institutions et organes de l'UE d'adopter une «approche proactive» dans ce domaine. Celle-ci implique d'analyser anticipativement et à un

---

«Article 29»: l'avis 3/1999 relatif à la préservation des données concernant l'information émanant du secteur public et la protection des données à caractère personnel, adopté le 3 mai 1999 (GT 20) ainsi que l'avis 5/2001 concernant un rapport spécial du Médiateur européen, adopté le 17 mai 2001.

[12] Voir l'article 6, paragraphe 1, point b), de la directive 95/46/CE.

[13] Ce principe s'applique également aux données à caractère personnel qui sont disponibles publiquement. Le seul fait que des données à caractère personnel sont publiquement disponibles pour une finalité particulière n'implique pas nécessairement que ces données doivent également être mises à disposition en vue de leur réutilisation pour n'importe quelle autre finalité.

[14] Voir l'article 6, paragraphe 1, point c), de la directive 95/46/CE.

[15] Voir, par exemple, l'arrêt de la CJUE du 9 novembre 2010 dans les affaires jointes C-92/09 et C-93/09, *Schecke et Eifert*, et en particulier les points 81, 85 et 86. Dans cette affaire, la CJUE a souligné que les dérogations et les limitations en rapport avec la protection des données à caractère personnel ne doivent s'appliquer que dans la mesure où elles sont strictement nécessaires. La Cour a notamment estimé que les institutions européennes devraient étudier différentes méthodes de publication afin de trouver celle qui serait conforme à l'objectif de la publication tout en étant moins attentatoire au droit des bénéficiaires au respect de leur vie privée et à la protection de leurs données à caractère personnel.

stade précoce la portée d'une divulgation publique de données à caractère personnel et d'informer les personnes concernées en ce sens de manière à les mettre en mesure d'exercer leurs droits[16]. Cette approche aidera à trouver des solutions appropriées au cas par cas et pourra également s'avérer intéressante pour la réutilisation éventuelle d'ISP contenant des données à caractère personnel.

2.4. La proposition doit traiter de manière plus spécifique de la protection des données

24. Bien que la directive 95/46/CE prévoit un cadre juridique solide et que l'avis du groupe de travail «Article 29» apporte d'importants éclaircissements, certaines dispositions de la directive ISP elle-même doivent également être clarifiées et davantage précisées afin de contribuer à un niveau plus élevé et plus cohérent de protection des données dans toute l'Union européenne ainsi qu'à un degré plus élevé de sécurité juridique pour les personnes concernées.

25. Dans l'état actuel de l'harmonisation de la législation européenne, il existe des différences considérables entre les règles et pratiques nationales en ce qui concerne la réutilisation des ISP. En particulier, les attitudes culturelles et, partant, les législations nationales sur l'accès aux documents divergent entre elles. Les lois nationales en matière de protection des données transposant la directive 95/46/CE ne sont pas non plus identiques à cet égard.

26. Malgré ces différences, les personnes concernées doivent avoir l'assurance que leurs données seront systématiquement protégées, même lorsque celles-ci sont transférées vers un autre État membre en vue d'être réutilisées.

27. En outre, il convient d'éviter toute complexité et fragmentation superflues, non seulement pour assurer une protection adéquate aux personnes concernées, mais aussi pour permettre la libre circulation des données à caractère personnel dans toute l'Europe, ce qui constitue un autre objectif clé de la directive 95/46/CE.

28. Le projet de recommandations politiques sur la vie privée élaboré par le réseau thématique LAPSI[17] en décembre 2011 illustre clairement les disparités insatisfaisantes et superflues qui existent dans la manière dont la directive ISP a été transposée dans les États membres pour ce qui est de la protection des données.

29. En outre, étant donné que le cadre juridique de la protection des données est actuellement en cours de révision[18], le CEPD considère qu'il serait également approprié, le cas échéant, de tenir compte de concepts nouveaux tels que le respect de la vie privée dès la conception et la responsabilité, et de faire expressément référence à

---

[16] Voir le document du CEPD du 24 mars 2011 sur l'«accès du public aux documents contenant des données à caractère personnel après l'arrêt *Bavarian Lager*», disponible sur le site web du CEPD (http://www.edps.europa.eu), et notamment le chapitre III aux pages 6 à 11.

[17] LAPSI est un réseau thématique européen sur les «aspects juridiques des informations du secteur public», financé par la Commission (voir http://www.lapsi-project.eu/). La dernière mouture du projet de recommandations politiques est disponible à la page http://www.lapsi-project.eu/wiki/index.php/Policy_recommendation_on_privacy.

[18] Voir la proposition de la Commission d'un règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (COM(2012)11 final). Voir également l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données à la page http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package;jsessionid=46ACCFDB9005EB950DF9C7D58BDE5377.

des outils pratiques tels que les analyses d'impact sur la protection des données dans la proposition[19].

30. Pour ces raisons, le CEPD recommande que la proposition ne se borne pas à faire simplement référence aux «principes relatifs à la protection des données» (voir le considérant 21) et qu'elle définisse plus clairement les situations dans lesquelles des informations contenant des données à caractère personnel peuvent être mises à disposition en vue de leur réutilisation, et moyennant quelles garanties, comme exposé de manière plus détaillée à la section 3.

3. RECOMMANDATIONS SPECIFIQUES

3.1. L'applicabilité du principe de réutilisation aux données à caractère personnel doit être clarifiée et soumise à des conditions supplémentaires

Dispositions pertinentes: article 1er, paragraphe 2, point c), et article 1er, paragraphe 3

31. La modification proposée de l'article 3, paragraphe 1, de la directive ISP (lue en parallèle avec l'article 1er, paragraphe 1))[20] fait expressément obligation aux États membres de veiller à ce que les «documents existants» détenus par des organismes du secteur public soient «réutilisables à des fins commerciales et non commerciales».

32. Ni la directive ISP existante, ni la proposition ne contiennent de dérogations spécifiques pour les données à caractère personnel. Cela dit, l'article 1er, paragraphe 2, point c), exclut du champ d'application de la directive ISP les «documents qui sont exclus de l'accès conformément aux règles d'accès en vigueur dans les États membres, y compris pour des motifs de protection de la sécurité nationale (autrement dit, la sûreté de l'État), de défense ou de sécurité publique [ou] de confidentialité des données statistiques ou des informations commerciales».

33. L'article 1er, paragraphe 3, prévoit en outre que la directive ISP «s'appuie sur les règles d'accès en vigueur dans les États membres et ne les affecte en rien» et qu'elle «ne s'applique pas aux cas dans lesquels, conformément aux règles d'accès, les citoyens ou les entreprises doivent démontrer un intérêt particulier pour obtenir l'accès aux documents».

34. Ces dispositions impliquent que les documents contenant des données à caractère personnel ne relèvent de la directive ISP que s'ils sont rendus publiquement accessibles, ou peuvent l'être, en vertu des «règles d'accès en vigueur dans les États membres».

L'article 1er, paragraphe 2, point c), doit faire expressément référence à la protection de la vie privée et des données à caractère personnel comme cause de dérogation aux règles d'accès

35. L'article 1er, paragraphe 2, point c), laisse à chaque État membre toute latitude pour définir ses propres «règles d'accès» et ne cite que quelques exemples de motifs pour

[19] Voir, par exemple, la recommandation de la Commission du 9.3.2012 relative à la préparation de l'introduction des systèmes intelligents de mesure, C(2012) 1342 final.

[20] Sauf indication contraire, les références se rapportent aux articles révisés de la directive ISP telle que proposée.

lesquels un document peut «ne pas être accessible […]». Actuellement, la protection de la vie privée et des données n'est pas expressément citée parmi ces exemples.

36. Dans un souci de clarté et de cohérence par rapport aux règles générales relatives à l'accès du public aux documents, le CEPD recommande de modifier l'article 1er, paragraphe 2, point c), et de mentionner expressément la notion de «protection de la vie privée et des données à caractère personnel» parmi les exemples de causes possibles de dérogation aux règles d'accès.

Évaluation des risques pour la protection des données et garanties pour atténuer ces risques

37. Comme exposé ci-dessus à la section 2.2, les projets d'ouverture des données hissent l'accessibilité des informations à un autre niveau et peuvent induire des risques supplémentaires importants pour la protection des données à caractère personnel.

38. Dans cette perspective, le CEPD recommande que la proposition aborde, à tout le moins de manière générale, la question de savoir comment la réutilisation des informations du secteur public contenant des données à caractère personnel peut être mise en conformité avec les règles relatives à la protection des données.

39. Il est crucial que les organismes du secteur public adoptent une approche proactive[21] lorsqu'ils mettent à disposition des données à caractère personnel en vue de leur réutilisation. Une approche proactive permettrait de rendre les données publiquement disponibles dans le but explicite de leur réutilisation, moyennant certaines conditions et garanties spécifiques conformes aux règles relatives à la protection des données.

40. À cet effet, le CEPD recommande de préciser dans la proposition qu'avant de mettre à disposition des données à caractère personnel en vue de leur réutilisation, un organisme du secteur public doit évaluer si ces données peuvent être rendues disponibles. Cette évaluation devrait également établir les conditions et les sauvegardes spécifiques en matière de protection des données permettant la réutilisation des données. Elle serait comparable à l'analyse d'impact sur la protection des données prévue dans la proposition d'un règlement général sur la protection des données[22]. Le CEPD suggère d'inclure les principaux éléments de l'évaluation dans le texte de la proposition de directive.

41. L'évaluation doit garantir qu'il existe une base juridique adéquate pour le transfert et la réutilisation des données en vertu du droit national, que la réutilisation n'est permise que pour une finalité compatible et que les demandeurs se conforment à toutes les autres dispositions de la législation en vigueur relative à la protection des données. L'évaluation peut également déterminer des garanties supplémentaires: elle peut avoir pour effet, par exemple, d'imposer une anonymisation intégrale ou partielle avant que les données soient mises à disposition en vue de leur réutilisation et d'interdire la réidentification des personnes concernées (voir les points 45-46 et 56 ci-dessous).

42. Le cas échéant, il se peut que les demandeurs aient également à remplir certaines conditions supplémentaires spécifiques stipulées dans leurs licences, voire à élaborer

[21] Voir également dans ce contexte le document du CEPD mentionné à la note de bas de page 16.

[22] En ce qui concerne les analyses d'impact sur la protection des données, voir l'article 33 de la proposition de la Commission d'un cadre général pour la protection des données et l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, points 200-205, cité à la note de bas de page 18.

eux-mêmes une analyse d'impact sur la protection des données (voir le point 53 ci-dessous). Dans certains cas, l'organisme du secteur public peut aussi limiter le nombre de licences qu'il est habilité à octroyer et les restreindre aux demandeurs répondant à certains critères dans la perspective de la protection des données (voir le point 52 ci-dessous).

3.2. Anonymisation

Les données partiellement anonymisées et/ou agrégées peuvent également comprendre des données à caractère personnel

43. Il convient de souligner que les données continueront d'être considérées comme des «données à caractère personnel» et qu'elles seront donc soumises à la législation relative à la protection des données tant que les personnes physiques peuvent être identifiées, que ce soit directement ou indirectement. Le fait que certaines «techniques d'anonymisation» aient été utilisées n'implique pas que les données sont nécessairement considérées comme «anonymisées» au sens du considérant 26 de la directive 95/46/CE[23]. Une série de données peut contenir des données à caractère personnel et conduire finalement à l'identification d'une personne physique même après la suppression des identificateurs directs et l'utilisation de diverses techniques d'anonymisation supplémentaires[24].

44. L'anonymisation intégrale n'est pas toujours possible et elle devient de plus en plus difficile à mettre en œuvre du fait de l'évolution de l'informatique moderne et de l'omniprésence des informations. Néanmoins, si une anonymisation intégrale ne peut être complètement garantie, les exigences en matière de protection des données continuent de s'appliquer, telles que, par exemple, la nécessité d'une base juridique appropriée pour le transfert et la réutilisation, le principe de limitation des finalités et la protection particulière accordée aux données sensibles (comme les informations liées à la santé). Par conséquent, le respect de la législation relative à la protection des données doit être garanti chaque fois que les données ne sont pas intégralement anonymisées.

Des niveaux adéquats d'anonymisation doivent être garantis

45. Pour remédier à ces situations, le CEPD recommande de préciser clairement dans la proposition que l'organisme du secteur public doit veiller à ce que les données à caractère personnel concernées ont été anonymisées et mises à disposition en vue de leur réutilisation uniquement sous cette forme anonymisée, à moins que l'évaluation visée aux points 37 à 42 ci-dessus n'établisse, en pleine conformité avec la législation en vigueur en matière de protection des données, que les données à caractère personnel peuvent être mises à disposition d'une manière telle qu'elle permet d'identifier les personnes concernées (par exemple, noms des administrateurs dans un registre du commerce).

---

[23] Voir notamment au considérant 26: «pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne».

[24] Voir l'avis du groupe de travail «Article 29» sur le concept de données à caractère personnel (GT 136), pp. 15-20. Voir également l'arrêt fondamental de la Chambre des Lords du Royaume-Uni du 9 juillet 2008 dans l'affaire *CSA contre SIC*, ainsi que les points pertinents de plusieurs avis du CEPD, notamment l'avis du CEPD du 3 septembre 2010 relatif à un contrôle préalable sur le système de surveillance européen («TESSy»), section 3.1.

46. L'évaluation visée aux points 37 à 42 devrait également déterminer si la législation relative à la protection des données permet de mettre à disposition les données en vue de leur réutilisation après une simple anonymisation partielle ; si tel est le cas, elle devrait déterminer le niveau d'anonymisation requis afin de réduire au minimum le risque de réidentification et d'usage abusif des données à caractère personnel. En principe, l'anonymisation devrait être effectuée dans une mesure appropriée, compte tenu des finalités du traitement, d'une part, et de la nature des données et des conséquences potentielles pour les individus au cas où ils seraient réidentifiés, d'autre part[25].

47. Lorsque l'évaluation révèle que les données à caractère personnel ne peuvent être mises à disposition en vue de leur réutilisation après une anonymisation partielle et qu'une anonymisation intégrale est impossible, le CEPD observe que les ISP contenant des données à caractère personnel ne doivent pas nécessairement et toujours être rendues publiquement disponibles pour qu'elles bénéficient des possibilités de la réutilisation. Les données peuvent, par exemple, être seulement mises à la disposition de certains titulaires d'une licence sélectionnés sur la base de critères spécifiques, en vue de leur réutilisation.

48. Par exemple (si toutes les autres exigences en matière de protection des données sont remplies), les microdonnées à granularité fine[26] peuvent, après un certain degré d'anonymisation, être mises à la disposition de chercheurs qualifiés à des fins scientifiques, qui ont été soumis à une procédure d'examen stricte et ont accepté de respecter des conditions de licence strictes, et notamment des obligations de stricte confidentialité[27].

3.3. Octroi de licences

Disposition pertinente: article 8

49. Le projet d'article 8, paragraphe 1, prévoit que «[l]es organismes du secteur public peuvent autoriser la réutilisation sans conditions ou peuvent imposer des conditions, telle qu'une indication de la source, le cas échéant par le biais d'une licence. Ces conditions ne limitent pas indûment les possibilités de réutilisation et ne sont pas utilisées pour restreindre la concurrence».

---

[25] Les dossiers criminels en usage au Royaume-Uni offrent un exemple de données agrégées mises à disposition en vue de leur réutilisation moyennant certaines garanties. Dans ce cas-ci, les créateurs de la série de données à réutiliser ont non seulement supprimé les identificateurs personnels (tels que les noms des auteurs et de leurs victimes) avant de mettre à disposition les données en vue de leur réutilisation, mais aussi les données agrégées de manière à réduire au minimum le risque de réidentification et d'usage abusif des données. Cette mise en balance visait à réduire le plus possible les risques tout en fournissant un degré utile de précision aux personnes souhaitant s'informer sur les taux de criminalité dans certains quartiers.

[26] Les microdonnées sont des «séries de fichiers contenant des informations sur des personnes interrogées ou sur des entités économiques. Autrement dit, les microdonnées sont des informations de base rassemblées dans le cadre d'enquêtes…» (source: Eurostat, à la page http://epp.eurostat.ec.europa.eu/portal/page/portal/research_methodology/statistical_confidentiality/confidential_data/introduction#microdata).
Voir aussi la définition de Wikipedia [*version anglaise*] à la page http://en.wikipedia.org/wiki/Microdata_(statistics): «Dans l'étude de données d'enquêtes et de recensements, les microdonnées sont des informations au niveau des répondants individuels. Par exemple, un recensement national peut collecter l'âge, l'adresse de domicile, le niveau d'éducation, la situation d'emploi et beaucoup d'autres variables, données enregistrées séparément pour chaque répondant: c'est ce que l'on appelle les microdonnées».

[27] Voir, par exemple, l'avis du CEPD du 22 juillet 2010 sur l'analyse empirique des corrélations entre les variables du système de travail et le processus décisionnel.

Clause de protection des données

50. Le CEPD recommande que l'article 8 de la proposition impose clairement que les conditions des licences comprennent une clause spécifique de protection des données chaque fois que des données à caractère personnel sont incluses dans les ISP mises à disposition en vue de leur réutilisation.

51. En ce qui concerne la portée de cette clause, le CEPD souligne que le contenu et la précision de la licence peuvent varier selon les circonstances – comme le risque présenté pour la protection des données, la complexité du cas, la nature des données à caractère personnel concernées et les finalités prévues de la réutilisation. Par conséquent, il ne suffira pas de faire simplement référence à la nécessité de se conformer à la législation en vigueur en matière de protection des données.

52. Le CEPD souhaiterait également que la proposition précise – à l'article 8 ou éventuellement dans un considérant – que l'organisme du secteur public peut soumettre, le cas échéant, la réutilisation des données à caractère personnel à un examen des demandeurs, limiter le nombre de licences qu'il est habilité à octroyer et restreindre l'octroi de la licence aux demandeurs qui apportent la preuve qu'ils satisfont à certains critères spécifiques dans la perspective de la protection des données. Dans tous les cas, la deuxième phrase du projet d'article 8, paragraphe 1, ne doit pas être interprétée de manière à exclure ce pouvoir d'appréciation.

Le demandeur doit rendre compte de la manière dont les risques sont traités

53. Le CEPD recommande par ailleurs – au cas où cela s'avérerait nécessaire compte tenu des risques pour la protection des données à caractère personnel – d'obliger les demandeurs à prouver[28] que les risques pour la protection des données à caractère personnel sont traités de manière adéquate et qu'ils traiteront les données conformément à la législation en vigueur en matière de protection des données.

Finalité de la réutilisation

54. En outre, le CEPD recommande de préciser, dans la proposition, que la réutilisation des ISP contenant des données à caractère personnel peut être subordonnée à la finalité pour laquelle la réutilisation est effectuée, par dérogation à la règle générale autorisant la réutilisation à toute fin commerciale ou non commerciale. Les conditions des licences doivent notamment indiquer les finalités pour lesquelles les données à caractère personnel peuvent être traitées, ou à tout le moins les finalités originales pour lesquelles les données ont été collectées, et imposer que la réutilisation doit être effectuée pour une finalité compatible.

55. Pour ce qui est du concept de «finalité compatible», le CEPD note qu'en vertu de l'article 6, paragraphe 1, point b), de la directive 95/46/CE, «[u]n traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées». Par ailleurs, le considérant 29 énonce que «ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne».

[28] Cela peut se faire, par exemple, en effectuant une analyse d'impact sur la protection des données. Sur ce point, voir la note de bas de page 24 ci-dessus.

56. Lorsque cela s'avère approprié à la lumière de l'évaluation visée aux points 37 à 42 ci-dessus (par exemple, mais pas seulement, lorsque des données statistiques partiellement anonymisées sont rendues publiquement disponibles à des fins de recherche scientifique), le CEPD recommande d'imposer dans la proposition que les conditions des licences prévoient que les réutilisateurs ne tenteront pas d'identifier les personnes concernées ou d'utiliser les données à l'appui de mesures ou de décisions concernant ces personnes. Ils ne pourront pas non plus autoriser des tiers à le faire ni leur faciliter la tâche en ce sens.

3.4. Réutilisation par des organisations en dehors de l'Union européenne

57. L'article 26, paragraphe 1, point f), de la directive 95/46/CE prévoit une dérogation aux exigences générales régissant les transferts internationaux de données dans les cas où le «transfert [intervient] au départ d'un registre public».

58. Toutefois, cette dérogation ne saurait être interprétée comme fournissant en soi une base juridique pour les transferts d'informations, en vue de leur réutilisation, au départ de bases de données entières vers un pays qui n'assurerait pas un niveau adéquat de protection. Comme le groupe de travail «Article 29» et le CEPD l'ont déjà affirmé dans plusieurs avis[29], les dérogations aux exigences relatives aux transferts s'appliquent au cas par cas et ne peuvent permettre des transferts fréquents, massifs ou structurels.

59. Il y a une grande différence entre le fait de transférer des données publiquement disponibles au cas par cas, en vertu de l'article 26, paragraphe 1, point f), à un pays tiers qui ne garantit pas un niveau adéquat de protection, d'une part, et le fait d'autoriser l'accès à une base de données entière (ou à de larges pans de celles-ci) et la pleine réutilisation de ces données à un pays qui ne garantit pas des niveaux adéquats de protection des données à caractère personnel, d'autre part. De même, il y a une différence entre le fait de permettre à un ressortissant d'un pays tiers de télécharger, éventuellement moyennant le paiement d'un droit, une liste sélective des administrateurs d'une société, d'une part, et le fait de permettre que l'ensemble des données du registre des sociétés d'un État membre, en ce compris les adresses personnelles et des spécimens de la signature écrite de tous les représentants de ses sociétés enregistrées, soient mises à disposition afin d'être réutilisées dans un pays tiers.

60. Par conséquent, le CEPD recommande que la directive ISP remédie spécifiquement au problème des transferts internationaux de données en imposant un niveau adéquat de protection ou une autre base juridique adéquate pour les transferts vers des pays tiers à des fins de réutilisation. Le CEPD recommande également de préciser, dans la proposition, que les conditions des licences doivent également refléter cette exigence et, si nécessaire, contenir des clauses contractuelles appropriées. Il ne suffit pas de se baser sur l'article 26, paragraphe 1, point f), de la directive.

3.5. Coûts de l'anonymisation

Disposition pertinente: article 6

[29] Voir le document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (GT 114) et l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, point 224.

61. La proposition suggère de modifier l'article 6 et d'imposer que «[l]orsque la réutilisation de documents est soumise à des redevances, le montant total exigé par les organismes du secteur public ne dépasse pas les coûts marginaux de reproduction et de diffusion».

62. Cette interdiction générale des droits dépassant les coûts marginaux de reproduction et de diffusion est suivie par un certain nombre d'exceptions, notamment pour les bibliothèques, les musées et les archives, ainsi que pour certains organismes du secteur public exploitant des droits de propriété intellectuelle. Aucune exception spécifique n'est prévue pour les informations du secteur public contenant des données à caractère personnel.

Exception pour les coûts de l'anonymisation

63. L'anonymisation de documents existants détenus par des organismes du secteur public peut, dans certains cas, être une tâche complexe, de longue haleine et onéreuse, nécessitant une expertise spécifique dont tous les organismes du secteur public ne disposent pas. Cependant, cette anonymisation peut souvent s'avérer nécessaire étant donné les risques encourus, mais aussi constituer un investissement intéressant vu la valeur des informations du secteur public partiellement ou intégralement anonymisées, qui peuvent ainsi être mises à disposition en vue de leur réutilisation. Le fait d'autoriser les organismes du secteur public à compenser leurs coûts peut contribuer à garantir que la tâche de l'anonymisation sera effectuée minutieusement et donc donner lieu à un degré plus élevé de protection des données tout en contribuant dans le même temps à un niveau plus élevé de transparence et de disponibilité à des fins de réutilisation.

64. Pour ces raisons, une autre exception à l'article 6, paragraphe 1, pourrait être envisagée afin de permettre à l'organisme du secteur public de faire payer au titulaire de la licence au moins les dépenses raisonnables qu'il a encourues pour prétraiter (par exemple, numériser), agréger et/ou anonymiser (partiellement ou intégralement) les données à caractère personnel offertes à la réutilisation, lorsque l'utilisation de ces techniques se justifie à la lumière des risques accrus découlant de la mise à disposition de ces données en vue de leur réutilisation.

65. Le fait de faire payer la réutilisation ne doit pas, bien sûr, être confondu avec le fait de faire payer l'accès aux documents en vertu de la législation en la matière. Pour réduire le plus possible tout conflit potentiel à cet égard, il pourrait être utile de préciser dans la proposition (par exemple, dans un considérant) que cette dérogation ne préjuge pas de la législation nationale relative à l'accès aux documents, qui peut prévoir que l'accès aux documents doit être fourni gratuitement ou à un prix n'excédant pas, par exemple, «les coûts marginaux de reproduction et de diffusion».

3.6. Lignes directrices supplémentaires sur l'anonymisation et l'octroi des licences; consultation du groupe de travail «Article 29»

66. Le CEPD recommande à la Commission d'élaborer, dans un document de la Commission (recommandation, acte d'exécution ou document de travail de la Commission), des lignes directrices supplémentaires sur les aspects de la réutilisation des ISP liés à la protection des données, et en particulier sur l'anonymisation et l'octroi des licences. Dans ce contexte, il pourrait s'avérer particulièrement utile d'élaborer un modèle de clauses adéquates en matière de protection des données à

intégrer dans les licences. Le CEPD recommande par ailleurs de faire expressément référence, dans la proposition, à ces lignes directrices supplémentaires et de spécifier la forme sous laquelle celles-ci seront fournies (par exemple, dans des actes d'exécution).

67. En outre, le CEPD note que le groupe de travail «Article 29» pourrait continuer à jouer un rôle utile en fournissant des avis spécialisés et en favorisant une plus grande cohérence dans ce domaine, notamment en recueillant les meilleures pratiques des États membres et en élaborant des approches harmonisées basées sur les enseignements tirés des expériences nationales. Comme indiqué au point 18, la question de la réutilisation des ISP a été abordée par le groupe de travail «Article 29» en 2003. À la lumière de la révision actuelle de la directive ISP et de l'expérience acquise entre-temps, ainsi que de la révision actuelle du cadre de l'UE relatif à la protection des données, une mise à jour pourrait notamment consister à régler de manière plus détaillée les questions d'anonymisation et d'octroi des licences.

4. ANALYSE DE LA DECISION DE LA COMMISSION

68. Le CEPD regrette de ne pas avoir été consulté sur le projet de décision avant son adoption. La décision ayant déjà été adoptée, il se bornera à mettre brièvement en exergue certains points qui mériteraient d'être améliorés. Il suggère de tenir compte, pour l'heure, de ses observations, au moins pour ce qui est de l'interprétation des dispositions de la décision. Dans un deuxième temps, lorsque la décision sera réévaluée, il conviendra d'envisager sa modification.

69. Le CEPD recommande tout d'abord de définir plus clairement l'expression «données publiques» à l'article 2, point a), compte tenu de la législation de l'UE en vigueur relative à l'accès aux documents et à la protection des données, ainsi que de la jurisprudence des juridictions européennes.

70. Le CEPD recommande par ailleurs d'indiquer clairement si la décision s'applique également aux données à caractère personnel autres que celles pouvant être divulguées en vertu de la législation de l'UE relative à l'accès aux documents. L'article 2, point c), semble l'exclure, mais dans un souci de sécurité juridique, il serait utile de le préciser.

71. Enfin, les observations formulées à l'égard de la proposition sur l'anonymisation (section 3.2), l'octroi des licences (section 3.3), les transferts internationaux (section 3.4) et les coûts de l'anonymisation et de l'agrégation (section 3.5) s'appliquent également *mutatis mutandis* à la décision.

5. CONCLUSIONS

72. La réutilisation des ISP contenant des données à caractère personnel peut apporter des avantages significatifs, mais aussi faire planer des risques considérables sur la protection des données à caractère personnel. À la lumière de ces risques, le CEPD recommande de définir plus clairement, dans la proposition, les situations dans lesquelles des informations contenant des données à caractère personnel peuvent être mises à disposition en vue de leur réutilisation, et moyennant quelles garanties. En particulier, la proposition devrait:

- établir plus clairement le champ d'application de la directive ISP aux données à caractère personnel (section 3.1);
- imposer qu'une évaluation soit effectuée par l'organisme du secteur public concerné avant que toute ISP contenant des données à caractère personnel puisse être mise à disposition en vue de sa réutilisation (section 3.1);
- le cas échéant, imposer que les données soient intégralement ou partiellement anonymisées et que les conditions des licences interdisent expressément la réidentification des personnes physiques et la réutilisation des données à caractère personnel pour des finalités susceptibles d'affecter individuellement les personnes concernées (sections 3.2 et 3.3);
- imposer que les conditions des licences de réutilisation des ISP contiennent une clause de protection des données, chaque fois que des données à caractère personnel sont traitées (section 3.3);
- lorsque cela s'avère nécessaire au vu des risques pour la protection des données à caractère personnel, imposer aux demandeurs de prouver (par une analyse d'impact sur la protection des données ou autrement) que tout risque pour la protection des données à caractère personnel est géré de manière adéquate et qu'ils traiteront les données conformément à la législation en vigueur en matière de protection des données (section 3.3);
- préciser que la réutilisation peut être subordonnée à la finalité pour laquelle elle est effectuée, par dérogation à la règle générale permettant la réutilisation à toute fin commerciale et non commerciale (section 3.3).

73. En outre, le CEPD suggère:
- d'envisager d'autoriser que les coûts de prétraitement (comme la numérisation), d'anonymisation et d'agrégation soient facturés aux titulaires des licences lorsque cela s'avère approprié (section 3.5) et
- que la Commission élabore des lignes directrices supplémentaires, centrées sur l'anonymisation et l'octroi des licences, et qu'elle consulte le groupe de travail «Article 29» à ce sujet (section 3.6).

Fait à Bruxelles, le 18 avril 2012

(**signé**)

Peter HUSTINX
Contrôleur européen de la protection des données